Dipartimento di Giurisprudenza

Cattedra di Diritto Internazionale

La compatiblità delle operazioni di mass surveillance con il diritto alla privacy

RELATORE

Prof. Palombino

CORRELATORE

Prof. Pustorino

CANDIDATO:

Chiara Sparacino
Matr. 152183

ANNO ACCADEMICO 2021/2022

A Lillo e Lilli

INDICE

CAPITOLO TERZO

IL CASO SNOWDEN

INTRODUZIONE

Il lavoro che segue si pone come obiettivo l'analisi del quadro giuridico internazionale relativo al diritto alla privacy, alla luce dell'avvento di nuove forme di sorveglianza di massa.

Lo sviluppo di nuove e potenti tecnologie ha certamente contribuito ad un intenso monitoraggio da parte delle autorità nazionali ed internazionali nei confronti degli individui, non distinguendo, però, coloro che effettivamente necessitano di particolari attenzioni in virtù di potenziali minacce alla sicurezza nazionale da coloro che possono al più essere considerati mere vittime di un sistema di sorveglianza eccessivamente ingerente.

Per tali ragioni, l'elaborato si propone di studiare entrambi i lati della medaglia rappresentata dal diritto di sorveglianza degli Stati, prevedendo, dunque, un focus sull'ingerenza arbitraria ed indiscriminata esercitata nei confronti dei singoli e della loro vita privata, con consequenziale lesione del diritto alla privacy, ormai oggetto di tutela che trova riconoscimento in molteplici fonti di diritto internazionale e regionale di seguito trattate.

Lo scritto si presenta suddiviso in tre sezioni: il Primo Capitolo ha ad oggetto la nascita del diritto alla sorveglianza dei singoli Stati ed il suo mutamento alla luce dei fenomeni terroristici che hanno segnato lo scenario internazionale.

L'attacco alle Torri Gemelle, rivendicato da Al-Qaeda nel 2001 durante l'amministrazione Bush, è stato determinante per la scelta di operare una netta riforma relativa al *modus operandi* ed alla struttura dei servizi d'intelligence statunitensi e del loro approccio alla collaborazione internazionale per la lotta al terrorismo, incentivata da una comune ed omogenea volontà di garantire la sicurezza interna ed internazionale.

Al fine di perseguire tale scopo, i governi si sono dotati di strumenti progressivamente più innovativi e potenzialmente più rischiosi per l'integrità della privacy dei cittadini.

L'avvento dei social media, come si vedrà in questa prima fase, si è rivelato cruciale per il monitoraggio degli utenti, permettendo alle autorità di trasformare le piattaforme *social* in veri e propri strumenti di sorveglianza di massa: *Facebook*,

Twitter, Yahoo! e svariati altri colossi della Silicon Valley sono un prezioso pozzo da cui attingere ingenti *database*, utili per gli scambi di informazioni interni ed intergovernativi.

L'esercizio del diritto di sorveglianza ha assunto ancora maggiore arbitrarietà a seguito dell'emergenza pandemica da Covid-19, durante la quale si è reso necessario controllare i cittadini ed i loro movimenti per monitorare la situazione sanitaria mondiale. Si è trattato di operazioni internazionalmente riconosciute e giustificate in virtù dei Regolamenti Sanitari Internazionali adottati dall'Organizzazione Mondiale della Sanità.

Nel Secondo Capitolo si analizza l'interesse, diritto e necessità, che per eccellenza si contrappone all'esercizio del diritto di sorveglianza: il diritto alla privacy.

È ormai agevole rintracciare fonti del diritto alla privacy, sia di rango internazionale, che regionale, sempre più complete e meno lacunose, anche grazie alla prassi che ha accompagnato contestualmente la nascita di questa nuova tutela.

A questo proposito, e per assicurare una completa analisi del diritto in materia, si è resa necessaria un'analisi in chiave comparativa delle legislazioni europee e statunitensi, prevedendo queste ultime regolamentazioni differenti, anche dovute al diverso scenario storico.

Se, sul versante americano, è già possibile rintracciare la previsione di una tutela alla riservatezza nel 1974, con l'emanazione del Privacy Act, è tuttavia da ricordare che la privacy di cui si preoccupò il legislatore americano è di natura prettamente economica, interessandosi esclusivamente ai diritti di riservatezza del singolo ricollegabili alla figura del consumatore; dunque, si intende qui tutelare il singolo in termini di correttezza delle pratiche commerciali.

Al contrario, analizzando l'iter legislativo comunitario, è facilmente riconoscibile l'intento dell'Unione Europea di garantire una tutela al cittadino comunitario, soffermandosi sul diritto alla privacy, quale diritto umano fondamentale.

Il Regolamento Europeo per la Protezione dei Dati Personali, meglio noto come GDPR, è il frutto di un laborioso tentativo ben riuscito di coprire ogni possibile ramificazione del diritto alla privacy ed assicurare un accesso giudiziario per le relative controversie.

A coronare questo nuovo e totalizzante quadro garantista, vi è stata l'istituzione di un'autorità indipendente adibita al controllo del rispetto del diritto alla protezione dei dati personali, dotata di poteri d'inchiesta e sanzionatori: il Garante Europeo della Protezione dei Dati, al quale spetta competenza su tutto il territorio comunitario.

Terminato lo studio della dottrina domestica ed internazionale, si è reso utile lo studio della giurisprudenza più emblematica della necessità di una tutela della riservatezza. Dunque, di cruciale importanza è stata la rassegna delle pronunce che hanno marcato i punti cardine fondamentali per tentare di identificare la linea di confine della liceità del diritto di sorveglianza.

Anche nella prassi si ravvisano emblematiche differenze tra i ricorsi giudiziari nel quadro europeo e nel quadro statunitense.

E ciò trova le proprie spiegazioni nelle vicende che dal 2010 in poi, hanno segnato il destino della regolamentazione relativa alla tutela della privacy.

Si giunge, in terza ed ultima istanza, ad analizzare il caso da cui è nata una lunga controversia, risoltasi soltanto due anni fa, con una sentenza di condanna emanata dalla corte d'appello americana nei confronti dei propri servizi di intelligence: il caso Snowden.

Edward Snowden ha ottenuto il titolo di *whistleblower* per aver diffuso informazioni circa le operazioni della National Security Agency, denunciando l'abuso di poter esercitato dai servizi segreti americani finalizzato allo spionaggio della corrispondenza telematica scambiata tra i cittadini americani e tra questi ultimi ed utenti localizzati al di fuori del territorio statunitense.

Tutto ciò veniva realizzato bypassando il consenso degli utenti, servendosi di programmi appositamente creati per intercettare, archiviare e trasferire dati personali illegittimamente raccolti: primo fra tutti vi fu PRISM, con cui i dipendenti dell'NSA riuscivano ad accedere ad ogni dispositivo mobile, trasformandolo in uno strumento di sorveglianza di massa persino a distanza.

Il caso Snowden è stato poi responsabile di ingenti conseguenze internazionali, giacché l'intelligence statunitense non si era limitata ad intercettare le comunicazioni dei cittadini, ma si era spinta ad esercitare un effettivo spionaggio nei confronti di altri governi, persino quelli alleati.

Ciò ha implicato l'incrinatura delle relazioni diplomatiche e, consequenzialmente, anche di quelle commerciali, con particolare riferimento al caso della cancelliera tedesca Merkel, anch'ella vittima di spionaggio e dalla quale provennero nuove importanti proposte legislative per reagire attivamente alle offese ricevute.

Il panorama internazionale ha risposto al caso Snowden sollevando un importante dibattito circa la liceità dell'esercizio di spionaggio reciproco da parte dei servizi segreti di ogni governo.

A tal proposito, l'elaborato si conclude con un'analisi della questione storico-giuridica concernente il regime di spionaggio nel diritto internazionale, studiando le diverse posizioni assunte dai Paesi interessati: seppur contrastanti, non permettono di giungere ad altra conclusione se non la configurazione del diritto di spionaggio come un'area grigia del diritto internazionale e che, in quanto tale, segue il cosiddetto principio *Lotus* pacificamente riconosciuto.

CAPITOLO PRIMO

IL DIRITTO DI SORVEGLIANZA DEGLI STATI

"Il re prende nota di tutte le loro intenzioni,
Con mezzi che nemmeno possono immaginare"

William Shakespeare, Enrico V

1.1 Premessa

In questo capitolo si analizzerà il diritto in capo agli Stati di sorvegliare i propri cittadini, esercitato tanto per assicurare e tutelare la sicurezza nazionale e la pace internazionale, quanto- da quanto si vedrà- per intervenire spesso abusivamente nella vita privata dei singoli, ledendo diritti umani e libertà costituzionalmente garantite. Lo scopo di quanto segue, dunque, è cercare di ravvisare una linea di confine tra scopo garantistico della sorveglianza statale e mera ingerenza nella privacy personale.

1.2 Genesi e fonti del diritto di sorveglianza

La sorveglianza è un fenomeno sociale e politico che da sempre ha interessato la collettività e gli individui, che si distinguono-spesso non scientemente- in due opposte fazioni: i sorveglianti ed i sorvegliati.

Prima di passare in rassegna cronologicamente le varie forme di sorveglianza susseguitesi negli anni, è necessario precisare che l'oggetto di questo genere di controllo, seppur non mutando la propria natura, ha mutato funzione, soggettività ed importanza nel panorama nazionale e, ancor di più, nel panorama del diritto internazionale: gli individui. In un primo momento questi ultimi non erano altro che mera popolazione, oggetto essenziale, requisito fondamentale per il riconoscimento di uno Stato, ma pur sempre dall'altro lato dello *schermo statale*[1], dunque lontano dal raggiungimento della soggettività internazionale.

Questa posizione fu superata con l'emanazione di un Parere fondamentale della CPI sui reclami pecuniari degli impiegati delle ferrovie di Danzica, risalente al 3 marzo 1928[2].

Successivamente, la CIG ha riconosciuto per la prima volta la nascita e lo sviluppo di veri e propri diritti individuali, invocabili dinanzi alla stessa Corte da parte dello Stato a cui appartiene l'individuo interessato[3] .

Ciò che urge specificare, però, è l'entità delle norme che danno vita a diritti individuali, quale sia, dunque, il riferimento legislativo che legittimi una soggettività internazionale degli individui in quanto tali. Tre sarebbero le branche del diritto in virtù delle quali si potrebbe configurare l'individuo come destinatario diretto delle stesse: il diritto internazionale dei diritti umani, il diritto internazionale penale ed il diritto internazionale degli investimenti.[4] Rispettivamente, già nella Convenzione europea dei diritti dell'uomo, è ravvisabile un diritto attribuito all'individuo non già sostanziale, bensì di natura procedurale.

---

[1] Carreau Q., Marrella F., *Diritto internazionale*, Giuffrè Editore S.P.A Milano, 2018 (pg.472).
[2] Carreau Q., Marrella F., *Diritto internazionale*, Giuffrè Editore S.P.A Milano, 2018 (pg.471).
[3] Carreau Q., Marrella F., *Diritto internazionale*, Giuffrè Editore S.P.A Milano, 2018 (pg.472).
[4] Palombino F.M., *Introduzione al diritto internazionale*, GLF Editori Laterza, 2019 (pg.138).

All'Articolo 34, la Carta così sancisce:

"The Court may receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto. The High Contracting Parties undertake not to hinder in any way the effective exercise of this right [5]."

In seconda istanza, è il diritto internazionale penale ad occuparsi della punizione di crimini internazionali individuali, configurandosi-anche qui- un destinatario ben definito[6].

Quest'ultima branca del diritto, così come il diritto internazionale di diritti dell'uomo, possono permettersi la configurazione di destinatari specifici in virtù della loro autonomia concettuale, come sostenuto dalla dottrina di Cannizzaro[7].

Infine, il diritto internazionale degli investimenti si occupa nello specifico di scindere diritti e doveri degli investitori stranieri: se, da un lato, i diritti materiali vengono disciplinati perlopiù da trattati bilaterali tra Stati, dall'altro, i diritti procedurali- circoscrivendo la loro applicazione al solo arbitrato ICSID- vengono disciplinati da clausole arbitrali contenute in appositi contratti ovvero in un ordinamento interno che preveda tutele per gli investitori stranieri, garantendo loro il diritto di iniziare arbitrati per eventuali violazioni dei principi che vigilano sui rapporti tra investitore straniero e Stato ospitante[8].

Una corrente di pensiero differente viene prospettata da Cannizzaro, che scandisce nettamente la posizione degli individui, quali meri beneficiari materiali di tali regole, che, invece, producono posizioni soggettive internazionali nei soli confronti degli Stati: da qui la differenza tra titolare di posizione soggettiva ed il beneficiario materiale di essa, che non coincidono.

---

[5] European Convention on Human Rights, ECHR, formalmente "The Convention for the Protection of Human Rights and Fundamental Freedoms", firmata il 4 novembre 1950 ed entrata in vigore il 3 settembre 1953; ratificata da 47 Stati e pubblicata nelle lingue ufficili inglese e francese.

[6] Palombino F.M., *Introduzione al diritto internazionale*, GLF Editori Laterza, 2019 (pg. 142)

[7] Cannizzaro E., *Diritto Internazionale*, G. Giappichelli Editore- Torino, 2012 (pg. 319)

[8] Palombino F.M., *Introduzione al diritto internazionale*, GLF Editori Laterza, 2019 (pg. 142)

Per l'appunto, una norma potrebbe garantire un certo trattamento a favore di un individuo, senza però stabilire e generare un vero e proprio diritto a favore di quest'ultimo.

Un esempio di questa teoria viene fornito lampantemente dalle norme sul trattamento degli stranieri: ogni Stato deve assicurare sul proprio territorio un certo trattamento ai cittadini di un altro Stato; dunque, si instaura una concreta relazione soggettiva fra due Stati: quello territoriale, titolare dell'obbligo di trattamento e quello di cittadinanza, titolare dello speculare diritto[9].

Ad accreditare questa tesi, contribuisce anche lo studioso Antonio Cassese, secondo cui, nella *traditional law*, gli esseri umani intesi quali individui, acquisivano rilevanza internazionale solo in quanto beneficiari di trattati di commercio o navigazione o se coinvolti in affari internazionali[10], restando però controversa la questione della *piracy*[11], fenomeno fin troppo diffuso ai tempi della *traditional law* e che faceva dubitare circa la soggettività internazionale degli individui.

Tuttavia, Cassese scinde il diritto internazionale della *modern law* da quello tradizionale: adesso non vige più il monopolio degli Stati sugli individui.

Quattro sarebbero i filoni della dottrina di Cassese che confermerebbero- anzi accentuerebbero- la soggettività internazionale degli individui: le regole consuetudinarie che impongono obblighi agli individui[12], la simmetrica titolarità di

[9] Cannizzaro E., *Diritto Internazionale*, G. Giappichelli Editore- Torino, 2012 (pg. 317)

[10] Secondo lo stesso Cassese, il diritto internazionale prese una prima vera e propria posizione in relazione alla figura degli individui nel 1928 con un Advisory Opinion della PCIJ, secondo cui- riferendosi al Beamtenabkommen, un trattato tra Germania e Polonia- un accordo non potrebbe generare diritti ovvero obblighi in capo ai singoli privati; d'altro canto, non è opinabile che siano essi stessi oggetto di un accordo internazionale. Dunque, la soluzione sarebbe lasciare alle Parti Contraenti la definizione di norme che definiscano i diritti e gli obblighi sorgenti in capo ai privati, rimettendo la competenza alle corti interne.

[11] Alcuni filosofi, tra cui Kelsen e Westlake sostenevano che la pirateria, già a partire dal diciassettesimo secolo, fosse una condotta reprimibile con sanzioni dirette a specifici individui con obblighi negativi che avevano per destinatari proprio i singoli privati.

[12] I singoli individui- ai sensi del pensiero Cassesiano- sono destinatari delle regole vigenti nel diritto internazionale circa I crimini di guerra, di aggressione, genocidio e contro l'umanità.

diritti in capo agli stessi[13], ed infine il contenuto di trattati internazionali che conferisce diritti agli individui[14].

Specularmente ai diritti, sorgono obblighi in capo agli individui, in virtù-perlopiù- di regole di genesi consuetudinaria, che hanno ad oggetto crimini internazionalizzati e conseguenti sanzioni penali in capo ai soggetti che se ne rendano responsabili[15].

Accanto a queste figure, merita un accenno anche la dottrina francese promanata da Dominique Carreau, secondo cui si giunge finalmente a *la fin de l'ignorance traditionelle des individus*[16], ciò comportando ciò uno slittamento della figura dell'individui da mero oggetto del diritto internazionale a soggetto dello stesso, seppur con soggettività limitata[17].

In conclusione, la figura dell'individuo non è del tutto delineata né in dottrina, né tantomeno in giurisprudenza; data l'incertezza della sua posizione, si può asserire che la soggettività internazionale degli individui sia un principio *sui generis*: seppur non sia possibile considerarlo un mero oggetto del diritto internazionale, non sarebbe neppure corretto credere che si tratti di una soggettività piena[18].

Tuttavia, da sempre gli individui, intesi nella loro singolarità, sono stati oggetto di controllo quasi sempre onnicomprensivo e totalizzante da parte degli Stati, in forme

[13] La titolarità di diritti include, secondo questa dottrina, una sfera procedurale oltre che sostanziale relativa ai diritti umani. Gli stessi privati hanno la possibilità, adesso, di citare in giudizio e ricorrere alle Corti Internazionali, contribuendo-anche se indirettamente- alla formazione ed evoluzione del diritto.

[14] In relazione a questo filone, però, nasce una controversia circa la dimensione e sfera d'applicazione di questi substantive rights citati dagli accordi, discutendo sull'applicabilità degli stessi all'interno degli Stati Contraenti ovvero in una sfera internazionale generale e più ampia.

[15] Agli art.2, 3, 4 e 5 dello Statuto del Tribunale penale internazionale si ravvisa la competenza dello stesso Tribunale relativa rispettivamente ai crimini di guerra, genocidio e contro l'umanità. All'art. 5 dello Statuto della Corte penale internazionale, tribunale sorto a seguito della Convenzione di Roma del 17 luglio 1998, si ravvisa la giurisdizione della Corte a perseguire crimini di genocidio, di guerra, contro l'umanità ed eventualmente-come statuito da Cannizzaro- anche il crimine di aggressione.

[16] Carreau D., *Droit International*, Pedone, 2009.

[17] La dottrina francese citata poggia le basi sul cambiamento avvenuto a partire dalla Prima guerra mondiale, con particolar riferimento alla necessità di proteggere le minoranze, a partire dal 1919 in poi, con la nascita di Convenzioni fondamentali, quali la Convenzione europea dei diritti dell'uomo ed il Trattato di Roma.

[18] Palombino F.M., *Introduzione al diritto internazionale*, GLF Editori Laterza, 2019 (pg. 143)

e gradi differenti, dipendentemente dalla storia, politica, posizione geografica ed entità statali.

La prima e più antica forma di sorveglianza è ravvisabile negli anni dell'Antico Romano Impero: il censimento[19].

Quest'ultimo era appunto finalizzato a stilare un elenco comprensivo di ogni proprietà, del numero di abitanti, della quantità di prole di ogni cittadino, così da poter controllare persino la potenziale mole di singoli idonei a far parte dell'esercito, pronti al combattimento[20].

Un'innovazione della sorveglianza si ebbe con l'introduzione del pensiero di un filosofo inglese Jeremy Bentham[21] (1748-1832), che nel 1791 ideò un modello alternativo di carcere, sostitutivo della usuale deportazione dei condannati in isole coloniali: il *Panopticon*[22].

Il nuovo modello prospettato dal filosofo presentava una peculiare architettura mai vista prima: vi era un unico e solo sorvegliante che, posto all'interno di una torre centrale, poteva osservare e controllare tutti i carcerati, con la differenza asimmetrica che questi ultimi non potevano fare altrettanto, neppure nei confronti di altri carcerati.

La funzionalità di questa struttura circolare si basava su un particolare e strategico gioco di ombre e contro luci che oscurava del tutto il sorvegliante. Da qui l'origine semantica del progetto: dal greco παν e ὀπτικός, appunto colui che tutto vede[23].

In un primo momento, il sorvegliante aveva anche la possibilità di ascoltare i carcerati grazie ad un sistema che sfruttava l'eco derivante da tubi di metallo; sistema che, tuttavia, fu debellato per la scarsa garanzia di unidirezionalità d'ascolto.

[19] Demografia di Roma, sezioni: urbanizzazione, da Romanoimpero.com

[20] I tre censimenti di Augusto e la nascita di Gesù, redazione de Gli scritti, Andrea Leonardo, 12/06/2013, da Gliscritti.it

[21] Stanford Encyclopedia of Philosophy, prima pubblicazione 17/3/2015.

[22] Bahmueller, C. F., 1981, *The National Charity Company: Jeremy Bentham's Silent Revolution*, Berkeley, CA: University of California Press.

[23] Da pan- (παν-) = "tutto", "interamente" + opticon (ὀπτικός) = "visivo"

La struttura *panottica*[24] si prestava perlopiù a carceri e centri per malati psichiatrici[25], ma il filosofo pensò più in grande, immaginando un'applicazione universale a tutti gli edifici pubblici che necessitassero di un controllo interno[26].
Il modello ideato alla fine del diciottesimo secolo, purtroppo o per fortuna-dipende dall'ottica con la quale si guarda ai benefici e rischi che ne derivano-non incontrò successo, se non negli ultimi anni[27] dell'Ottocento in Olanda e nel Novecento negli Stati Uniti d'America[28].
È chiaramente un progetto obsoleto e superato dall'evoluzione tecnologica, che ha permesso la sorveglianza ininterrotta grazie alla dotazione di telecamere onnivedenti.
Ciò che viene ideato da Bentham trovò un'applicazione connotata dall'avvento tecnologico nel primo riferimento al diritto di sorveglianza nella letteratura intesa *strictu sensu* rintracciabile nella storia[29]: la prospettazione distopica orwelliana[30].
Già nel 1948 veniva anticipata la possibilità di una completa sottomissione della riservatezza ad un potere, seppur nel romanzo in forma astratta[31].
Anche qui, uno ed un solo sorvegliante, il Grande Fratello[32], aveva accesso ad una visione onnicomprensiva della vita di tutti i cittadini, servendosi stavolta di uno schermo piuttosto che di una torre. I sorvegliati sapevano di poter essere sotto diretto controllo dell'occhio onnivedente[33], ma non sapevano quando ciò sarebbe potuto accadere.

---

[24] Harrison, R., 1983, *Bentham, London: Routledge and Kegan Paul*.
[25] Semple, J., 1993, *Bentham's Prison: A Study of the Panopticon Penitentiary*, Oxford: Clarendon Press.
[26] Peonidis, F., 2009, *"Bentham and the Greek Revolution: New evidence"*, Journal of Bentham Studies.
[27] Rosenblum, N., 1978, *Bentham's Theory of the Modern State, Cambridge*, MA: Harvard University Press.
[28] In particolare, il riferimento storico va fatto in relazione all' Olanda: Breda, Haarlem e Arnheim e nel Novecento: Stateville in Usa.
[29] Hart, H. L. A., 1982, *Essays on Bentham: Studies on Jurisprudence and Political Theory*, Oxford: Clarendon.
[30] Steinhoff W.R, *George Orwell and the Origins of 1984*, LCCC Library Category, 01/01/1975.
[31] Orwell G., 1984, *Foreward by Thomas Pynchon*, Afterword by Erich Fromm, 1948, Mondadori.
[32] Si tratta delle forze di polizia che avevano accesso ad ogni schermo, non permettendo ai destinatari di sapere se e quando saranno controllati, ma obbligandoli ad assistere ad ogni forma di propaganda.
[33] Meyers J., *Orwell*, EBSCO E-Book, 2010

Ciò che in *1984*[34], con The Big Brother[35], viene scongiurato, non è altro che l'anticipazione di un regime totalitaristico creatosi in alcune regioni del mondo e l'anticamera parallela dell'esercizio della sorveglianza posto in essere dalle regioni mancanti[36].

È sicuramente un'iperbole non lontana dalla realtà[37], ma che non avrebbe potuto aderire lisciamente a quest'ultima, non potendo previamente fare i conti con l'avvento della rivoluzione tecnologica, dello slittamento della vita sociale su piattaforme mediatiche e del progressivo utilizzo di mezzi tecnologici in ogni area in fase di sviluppo: medicina, servizi pubblici, trasporti, musica, ingegneria, ecc.

È fuori dubbio il contributo decisivo che la tecnologia ha apportato nel settore della ricerca e delle telecomunicazioni. Tuttavia, non si è anticipatamente valutato il rischio che quest'ingerenza tecnologica avrebbe comportato nella vita degli *users.*

1984 non è però l'ultimo riferimento al Panopticon rintracciabile nella storia: se ne occupò qualche anno più tardi (1975) Michel Foucault[38] con la pubblicazione di *Sorvegliare e Punire.*

Il fulcro del pensiero del francese[39] sul modello architettonico circolare si può capire appieno da quanto segue, estratto dal suo scritto*:*

"De là, l'effet majeur du Panoptique: induire chez le détenu un état conscient et permanent de visibilité qui assure le fonctionnement automatique du pouvoir. Faire que la surveillance soit permanente dans ses effets, même si elle est discontinue dans son action; que la perfection du pouvoir tende à rendre inutile l'actualité de son exercice; que cet appareil architectural soit une machine à créer et à soutenir un rapport de pouvoir indépendant de celui qui l'exerce […].

Si tratta di un testo che ha influenzato e scardinato l'interesse di filosofi, sociologi e criminologi[40].

---

[34] G. Orwell, 1984 (1949), Mondadori, IBS, Feltrinelli.

[35] Rodden J., *The Cambridge Companion to George Orwell*, Cambridge, UK; New York: Cambridge University Press, 2007.

[36] Gottlieb E., *The Orwell Conundrum*, LCCC Library Catalog, 1992.

[37] Moss J., Wilson G., *"1984" in Literature and Its Times*, GVRL E-book, 1997.

[38] Brunon-Ernst, A. (ed.), 2012, Beyond Foucault: New Perspectives on Bentham's Panopticon, Farnham: Ashgate.

[39] Rorty, R., Moral identity and private autonomy: The case of Foucault, in Essays on Heidegger and others. Cambridge: Cambridge University Press, 1991.

[40] Champs, E. de., 2015, Enlightenment and Utility: Bentham in French, Bentham in France, Cambridge: Cambridge University Press.

Lo scrittore francese introdusse il passaggio ad una c.d. "società disciplinata"[41], e lo fece servendosi di un semplice ma non banale esempio: un regolamento risalente al diciassettesimo secolo da adottare in caso di epidemia da peste in città[42].

Le precauzioni illustrate dal regolamento comprendono la suddivisione degli spazi, una registrazione permanente, introducendo una netta divisione sociale tra chi doveva essere controllato e chi controllasse.

Nel suo *Sorvegliare e Punire*[43], Foucault statuisce:

"L'esercizio della disciplina presuppone un dispositivo che costringe facendo giocare il controllo; un apparato in cui le tecniche che permettono di vedere inducono effetti di potere, e dove, in cambio, i mezzi di coercizione rendono chiaramente visibili coloro sui quali si applicano. Lentamente, nel corso dell'età classica, vediamo strutturarsi quegli «osservatori» della molteplicità umana ai quali la storia delle scienze ha riservato così poche lodi. A fianco della grande tecnologia dei cannocchiali, delle lenti, dei fasci luminosi che ha fatto corpo con la fondazione della nuova fisica e della nuova cosmologia, ci furono le piccole tecniche delle sorveglianze multiple e incrociate, degli sguardi che devono vedere senza essere visti; un'arte oscura della luce e del visibile ha preparato in sordina un nuovo sapere sull'uomo, attraverso tecniche per assoggettarlo e procedimenti per utilizzarlo[44] [45]."

[41] Miller J., *The passion of Michel Foucault*. New York: Doubleday, 1993.

[42] Fonio C., *"Oltre il Panopticon? Foucault e la videosorveglianza"*, Jstor.

[43] Foucault M., *Sorvegliare e punire. Nascita della prigione*, traduzione di Alcesti Tarchetti, Collana Paperbacks, Torino, Einaudi, 1976, (pg. 340).

[44] Michel Foucault, *Sorvegliare e Punire*, Parte seconda, La gerarchia della sorveglianza: "Nel campo perfetto, tutto il potere viene esercitato col solo gioco di una sorveglianza precisa, e ogni sguardo sarà una tessera nel funzionamento globale del potere. Il vecchio e tradizionale schema quadrato viene considerevolmente affinato secondo innumerevoli variazioni. Si definiscono esattamente la geometria delle strade, il numero e la distribuzione delle tende, l'orientazione dei loro ingressi, la disposizione delle file e delle righe; si disegna la rete degli sguardi che si controllano l'un l'altro".

[45] Habermas J., T*he critique of reason as an unmasking of the human sciences: Michel Foucault* (F. Lawrence, Trans.) in the philosophical discouse of modernity: Twelve lectures (pg. 238-265), Cambridge, MA: MIT Press, (originariamente pubblicato nel 1985), 1987.

Si crea così un tessuto sociale che darà vita ad una struttura cognitiva asimmetrica ancora oggi vivente[46] [47].

[46] Marika Surace, *Dalla sorveglianza moderna alla New Surveillance: il ruolo delle tecnologie informatiche nei nuovi metodi di controllo sociale* in ADIR-L'altro diritto (2005).

[47] McCarthy T., *The critique of impure reason: Foucault and the Frankfurt School*. In Ideals and illusions: On reconstruction and deconstruction in contemporary critical theory (pp. 43-75), Cambridge, MA: MIT Press., 1991.

1.3 Mutamento delle modalità d'esercizio del diritto di sorveglianza come conseguenza dello sviluppo tecnologico: l'utilizzo dei dati e metadati

L'avvento della rivoluzione tecnologica ha traslato sul piano digitale ogni forma di vigilanza e sorveglianza; all'occhio umano si sostituisce la fotocamera, alla corrispondenza epistolare si sostituisce la messaggistica online in qualunque momento intercettabile.

Questa traslazione ha comportato una dicotomia del controllo[48] così come era inteso sin lì: vi è un primo controllo c.d. "scopico*",* che si concretizza con la diffusione ramificata di videocamere su scala internazionale, nazionale, regionale e locale, avendo così la possibilità di geo localizzare la gran parte della popolazione servendosi di satelliti; fulcro centrale di questa sorveglianza è appunto la visibilità. La seconda tipologia di controllo, di stampo quantitativo, mira alla raccolta e collezione di dati sensibili, prelevati dall'anagrafe, dagli istituti di intermediazione finanziaria, seguendo transazioni bancarie, configurando una sorveglianza di gran lunga più pericolosa per la privacy del singolo se non mitigata da un'apposita legislazione in materia; fulcro, invece, di questa nuova sorveglianza è la tracciabilità[49] [50].

Il passaggio dalla sorveglianza del Diciannovesimo secolo alla sorveglianza contemporanea[51] [52] è stato ermeticamente ma efficacemente sintetizzato da un assunto di Gary T. Marx che indica cosa si intenda per *New Surveillance*:

"Grazie alla tecnologia informatica sta crollando una delle ultime barriere che ci separano dal controllo totale".

---

[48] Il Panopticon, da mediastudies.com.

[49] Rodotà S., Tecnopolitica. La democrazia e le nuove tecnologie dell'informazione, IIa edizione Bari-Roma, Laterza, 2004.

[50] Lyon D., *L'occhio elettronico. Privacy e filosofia della sorveglianza*, Milano, Feltrinelli, 1997.

[51] Cavicchioli S., Pezzini I., *La Tv verità. Da finestra sul mondo a "Panopticon"*, Collana Rai-VQPT n. 118, Torino, Nuova Eri, 1993.

[52] Lyon D., *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, con prefazione di Stefano Rodotà, Milano, Feltrinelli, 2002.

Così affermando, il sociologo americano vuole porre l'accento sul mutamento degli agenti di ogni tipo di controllo[53]: nell'era postmoderna, l'accesso al potere di sorveglianza era strettamente riservato allo Stato che ne usufruiva al solo scopo di assicurare una migliore amministrazione pubblica; in un secondo momento, dunque nel corrente secolo, la cerchia di soggetti che possono definirsi sorveglianti si è largamente- ed in modo eccessivamente semplice- ampliata: assicuratori, istituti di credito, piattaforme digitali, aziende ed organizzazioni che, distaccandosi dallo scopo di un'ottimale amministrazione statale, puntano all'acquisizione di preferenze personali, propensioni commerciali per pilotare le scelte future dei cosiddetti *costumers*[54].

Non vi è dubbio che vi sia un lato positivo derivante da una simile sorveglianza: lo Stato potrà raccogliere i dati necessari per conoscere e identificare gli individui che necessitano di qualsivoglia tipo di assistenza, così come il riconoscimento dei più svariati diritti, quali ad esempio il diritto di voto ovvero il diritto all'uguaglianza così come espressamente tutelato dall'art. 2 della Costituzione Italiana[55].

Importante è la collezione di dati e metadati[56]: la differenza tra questi risiede nel fatto che i metadati sono dati su dati, che comprendono un oggetto, un destinatario, un agente, un contenuto identificativo. La finalità della raccolta di metadati è strettamente connessa allo scopo della tracciabilità della sorveglianza, puntando appunto alla ricostruzione della vita di cittadini per studiarne il comportamento, le attitudini, preferenze, spese, così da tracciarle sotto ogni punto di vista e predirne lo sviluppo.

---

[53] Bogard, B., *The Simulation of Surveillance: Hyper Control in Telematic Societies*, New York: Cambridge University Press, 1996.

[54] Giudici G., *Dalla sorveglianza moderna alla New Surveillance. Il ruolo delle tecnologie informatiche nei nuovi metodi di controllo sociale*, tratto dal Centro di documentazione su carcere, devianza, marginalità dell'Università degli Studi di Firenze, da gabriellagiudici.it, 10 ottobre 2013.

[55] Carta Fondamentale della Repubblica Italiana, entrata in vigore il 1° gennaio 1948. All'art. 2 essa così sancisce: "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."

[56] I metadati: che cosa sono?, sezione: Amministrazione digitale, da archivibiblioteche.it, 7/04/2019.

Esistono poi diverse tipologie di metadata: metadata descrittivi, metadata amministrativi e gestionali ed infine metadata strutturali[57]. Ciò che li differenzia è la funzione che svolgono[58]: i primi sono volti alla descrizione, appunto, di documenti archiviati ben precisi, comprendendo in realtà ogni aggregazione presente in un archivio; i secondi sono volti alla gestione degli stessi, con funzione prettamente tecnico-organizzativo, disponendo le procedure di creazione ed archiviazione dei dati; i terzi, infine, sono volti a descrivere e fornire le informazioni utili allo scopo di agevolare le relazioni interne tra ogni singolo oggetto dei metadata.

Dati e metadati vengono poi raccolti nel c.d. "database", il quale archivia tutte le informazioni contenute nei dati e metadati e li memorizza consentendone il recupero in qualsiasi momento, godendo di memoria estremamente espansa.

L'alta concentrazione di dati che connota il database implicherebbe un'esigenza di segretezza che non vi ammetterebbe l'accesso facilmente: tuttavia, ciò non sempre rispecchia la realtà, anzi.

In proposito, Roger Clarke, scrittore e filosofo, ha coniato il termine *dataveillance*[59], per quest'ultimo intendendo:

"l'uso sistematico di insiemi di dati personali allo scopo di controllo e monitoraggio delle azioni e comunicazioni di una o più persone".

C'è da dire che molteplici database possono essere- e perlopiù delle volte lo sono- comunicanti fra di loro. Il pericolo che comporta questo genere di comunicazioni, implicante la diffusione di particolari informazioni, consente alle aziende di profilare ogni individuo, ricostruendo un quadro completo, basandosi su ogni *traccia* lasciata seppur in siti di matrice profondamente differente. Questa intercomunicazione fra database viene definita *computer matching*[60] ed opera con

[57] I metadati: che cosa sono?, sezione: Amministrazione digitale, da archivibiblioteche.it, 7/04/2019.

[58] Differenza tra dati e metadati, sezione: Tecnologia, da fondoperlaterra.org, 2022.

[59] Marika Surace, *Dalla sorveglianza moderna alla New Surveillance: il ruolo delle tecnologie informatiche nei nuovi metodi di controllo sociale* in ADIR-L'altro diritto (2005).

[60] Uno dei primi casi di controllo incrociato tra computer è avvenuto circa vent'anni fa, negli Stati Uniti: i responsabili dei sistemi informatici degli allora ministeri di sanità, istruzione e previdenza sociale sperimentarono la fusione dei dati. (101) In piena violazione del Quarto Emendamento della Costituzione, si tentò una retata di proporzioni

il c.d. metodo "front and verification", che consente di incrociare ed intrecciare i tessuti dei diversi archivi digitali, facendoli confluire in un unico database, evidenziando l'invisibilità del potere introdotta dal modello panottico e la non verificabilità dello stesso da parte del singolo che-nel contempo- diventa sempre più trasparente e limpido sotto il profilo della privacy.

La *data surveillance* può anche essere adoperata collettivamente e comportare il c.d. "sospetto categoriale", concetto partorito dal sopra richiamato Gary T.Marx, per quest'ultimo intendendo il sospetto ad esempio diffuso nell'ambiente delle forze dell'ordine, di condurre le indagini essendo guidati e tristemente influenzati da pregiudizi settoriali legati alla razza, etnia, religione, orientamento politico ovvero sessuale; il che, ad esempio, indirizza la polizia a rintracciare il colpevole in un ragazzo proveniente da un ghetto di periferia, piuttosto che in un benestante di un'alta classe sociale[61].

L'influenza che il nuovo assetto socio-tecnologico può comportare, viene descritta da David Lyon[62] che, per la prima volta parla di *modernità liquida*, proprio perché trattasi di un tipo di controllo che può infilarsi ovunque, non essendo più il destinatario in grado di scansarsene.

Lo scrittore, così, interviene nello scenario digitale potenzialmente- e realmente-pericoloso venutosi a creare:

"Non ci sarà più luogo dove rifugiarsi per non essere spiati. Per nessuno. La sorveglianza è una dimensione chiave del nostro mondo: "siamo costantemente

mastodontiche nei confronti di persone verso le quali non c'era stato nessun tipo di denuncia, né l'apertura di un procedimento legale.

[61] "Nella sua analisi svolta sui metodi di individuazione ed arresto dei criminali della polizia statunitense, Marx evidenzia molti esempi in cui è il sospetto categoriale a determinare in che direzione svolgere le indagini o su chi indirizzare la ricerca dei colpevoli. L'appartenere ad un'etnia considerata ad alto tasso di criminalità, l'abitare in una zona della città da cui provengono molti delinquenti comuni, l'avere effettuato spese straordinarie rispetto al proprio consueto stile di vita, divengono dati profondamente a rischio, dati che implicano un sospetto aprioristico su interi gruppi di cittadini. D'altra parte, è chiaro che è impossibile fare a meno di queste risorse, soprattutto quando si parla di controllo governativo.", Marika Surace, *Dalla sorveglianza moderna alla New Surveillance: il ruolo delle tecnologie informatiche nei nuovi metodi di controllo sociale* in ADIR-L'altro diritto (2005).

[62] David Lyon è uno scrittore scozzese, docente di Sociologia nell'Ontario e dirige il Surveillance Studies Center; è stato protagonista del docufilm *The Social Dilemma* (2020).

controllati, messi alla prova, valutati, giudicati nei più piccoli dettagli della vita quotidiana[63].”

Un’influenza particolare ha avuto la pubblicazione de “Il potere socievole” [64]di Fausto Colombo-a sua volta influenzato da Michel Foucault e dal suo scritto “Sorvegliare e punire”[65] - che ha sviluppato una vera e propria mappa concettuale, attraverso la quale è riuscito a raffigurare in modo semplice ma diretto, la transizione della Sorveglianza sociale adoperata per mano dei Mass Media, ad una società sorvegliata dai Social Media; di questi ultimi ci occuperemo successivamente. Innanzitutto, pone in primo piano la differenza tra sorveglianza verticale, sulla quale ci soffermiamo, e quella orizzontale, propria dei Social Media. La prima vede come legittimato attivo il potere, sotto forma di istituzioni politiche e come soggetti passivi i *corpi*- nonché individui[66]. Su questi ultimi viene operata una forte repressione, concretizzata rispettando un progetto disciplinare appositamente progettato nei minimi dettagli, che si basa sugli assunti Foucaultiani[67] ormai consolidati, quali il controllo dell’attività sociale, la gerarchizzazione e l’utilizzo della delinquenza ed infine il modello Panottico. Con riferimento al primo, è corretto asserire che si sostanzi in una scansione dei tempi di preghiera, di marcia, di lavoro, di studio; il secondo si rifà a *Supplizi e Pene* del filosofo francese; il terzo alla struttura che permette di vedere senza essere visti.
Si è già precisato che la sorveglianza verticale si distingue da quella orizzontale, per l’utilizzo dei Mass Media: questo avviene poiché gli stessi sono connotati dalla unidirezionalità, che consente il controllo a senso unico (si pensi alla radio, alla tv, ai giornali: sono tutte fonti e mezzi di comunicazione che non permettono uno scambio di interazioni con i destinatari)[68].

---

[63] David Lyon, Zygmunt Bauma, *Sesto Potere: La sorveglianza nella società liquida (2014), Gius.Laterza & Figli Spa.*
[64] Recensione di Franco Mattarella del libro Il potere socievole di Fausto Colombo, da pensierocritico.eu, ottobre 2013.
[65] Foucault M., Sorvegliare e punire. Nascita della prigione, traduzione di Alcesti Tarchetti, Collana Paperbacks, Torino, Einaudi, 1976, pg.340.
[66] Fausto Colombo, *Il potere socievole*, Bruno Mondadori Editore, (2013).
[67] Foucault M., Sorvegliare e punire. Nascita della prigione, traduzione di Alcesti Tarchetti, Collana Paperbacks, Torino, Einaudi, 1976.
[68] Paccagnella L., Sociologia della Comunicazione, Bologna, Il Mulino, 2010, p. 84.

I Mass Media godono di un importante potere influente[69], conquistato guadagnando la credibilità da parte degli interlocutori con la continuità delle notizie e l'attendibilità delle stesse negli anni[70].

La credibilità di una fonte fa sì che l'ascoltatore ovvero spettatore si serva dello stesso media tutte le volte che dovrà usufruire di una fonte per acquisire una notizia. I mass media hanno poi la capacità di fungere da interlocutori nell'intero settore dell'industria culturale; basti pensare alla rete di contatti consolidata tra giornalisti, scrittori, autori televisivi ecc.[71]

Caratteristica fondamentale che indistintamente riguarda tutti i media è l'incapacità di selezionare una cerchia di interlocutori ovvero di escluderne qualcuno: il c.d. "broadcasting", grazie al quale in realtà si assicura una tutela contro ogni genere di discriminazione, senza poter controllare i riceventi[72].

Tuttavia, i mass media non sono l'unico strumento di cui si serve la sorveglianza verticale: altro mezzo fondamentale sono le tecniche propagandistiche. Utilizzando la c.d. "agenda setting"[73], la quale prevede impostazioni mirate a controllare il *mainstream*[74]: distaccandosi dall'accezione volgarmente diffusa, qui il termine sta ad indicare ciò che riguarda la massa[75], qualcosa di convenzionale, ben prospettato nel panorama collettivo; dunque, ciò che viene pubblicato ed attenzionato dalla *massa*.

---

[69] Reese S.D., The Framing Project: A Bridging Model for Media Research Revisited, in Journal of Communication, 57, 2007, pp. 148-154.

[70] Katz E., *Mass Media Effects. In International Encyclopedia of Communications*, vol. 2. New York, Oxford University Press, 1989, pp. 492-497.

[71] Smith K. A., *Mass Media and Children: Concerns about Harmful Effects Increased with Each New Medium.* In History of Mass Media in the United States: An Encyclopedia, 1998, pp. 349-350.

[72] La sfida educativa, Comitato per il Progetto culturale della Cei, capitolo 8:mass media, Editori Laterza, Bari 2009.

[73] Dearing, J; Rogers E., "Agenda-setting research: Where has it been, where is it going?". Communication Yearbook. 11: 555–594, 1988.

[74] Treccani: Espressione usata prevalentemente in ambito artistico (musica, cinema, letteratura, ecc.), per indicare la corrente più tradizionale e anche più seguita dal grande pubblico. In contrapposizione a prodotti artistici d'autore, o legati alla cultura underground e giovanile, il termine può anche avere una connotazione dispregiativa, per indicare quegli artisti che sono spinti da motivazioni puramente commerciali.

[75] Rösler, Patrick, "Agenda-Setting: History and Research Tradition". The International Encyclopedia of Media Events, 2017.

Sarebbe un errore ipotizzare che questo tipo di attenzione nasca solo per perseguire fini comunicativi ed ottimizzare le informazioni da trasmettere. È una chiara forma di sorveglianza seppur velata dalla maschera di fonte di informazioni, fin troppo spesso sottovalutata, ma che contribuisce ingentemente all'acquisizione di dati dai quali si evinceranno interessi, preferenze e persino debolezze degli utenti.[76]

Le tecniche propagandistiche sfruttano poi, la cronaca nera, che legittima controlli giudiziari, delle forze dell'ordine ad esempio nel corso delle indagini[77].

Ai mass media, la rivoluzione tecnologica ha affiancato l'intelligenza artificiale, (AI, *Artificial Intelligence*) in costante e pericoloso sviluppo in ogni settore. L'invasività della sorveglianza degli stati è stata profondamente incrementata con la possibilità di servirsi di apparecchi in grado di controllare a distanza a qualsiasi ora del giorno e della notte da qualsiasi parte del mondo[78] [79].

Con l'intelligenza artificiale, nasce il c.d. "cyber spazio"[80]-termine coniato da William Gibson[81] nel suo *Neuromante*[82]- il primo luogo accessibile a tutti, raggiungibile da qualsiasi punto della terra, permettendo la comunicazione tra gli utenti diversamente dislocati. Nel 2010 il Pentagono[83] ha riconosciuto il cyber spazio come il quinto spazio: si è aggiunto a terra, aria, mare e spazio[84].

Un riconoscimento che qualche anno dopo verrà ribadito dagli Stati Uniti in concerto con la NATO. Con la nascita di un nuovo mondo, nasce simultaneamente la problematica relativa ad ogni stato e alla volontà di possederne il dominio: è così

[76] Qui un importante esempio di utilizzo di metadati: I mass media, prelevando informazioni apparentemente banali, quali gli ascolti di un programma o le letture di un articolo, sono in grado di profilare I soggetti e condizionarli con suggerimenti ed offerte, molto spesso- ma non necessariamente- a scopo di lucro.

[77] Walgrave, S; Van Aelst, P., "The contingency of the mass media's political agenda setting power: Toward a preliminary theory". Journal of Communication, 2006.

[78] Crevier D., *AI: The Tumultuous Search for Artificial Intelligence*. New York, NY: BasicBooks, 1993.

[79] McCorduck P.,Machines ,Who Think (2nd ed.), Natick, MA: A. K. Peters, Ltd, 2004.

[80] Dal greco *kyber*, "timone", che permette la navigabilità in internet avendo accesso ad infinite quantità di dati.

[81] Manuel Enrico, *William Gibson: l'uomo che inventò lo Sprawl*, 17/03/2021, da tomshw.com.

[82] Gibson W., *Neuromante* (Neuromancer, 1984), Milano, Editrice Nord, 1986.

[83] The Pentagon, è la sede del Dipartimento di Sicurezza degli Stati Uniti d'America, situato in Virginia.

[84] Raffaele Marchetti, Roberta Mulas, *Cyber Security Hacker, terroristi, spie e le nuove minacce del web*, 2017, Luiss University Press.

che il cyber spazio diventa oggetto di giurisdizione, che a fatica si riesce a collocare e che difficilmente permette di stabilire a chi appartenga il dominio in caso di controversie.

L'unica soluzione plausibile al problema è la creazione di un quadro normativo in grado di regolare ogni diramazione del cyber spazio, di ogni possibile minaccia che ne deriva.

Le minacce ed i pericoli legati a questo mondo non sono poche, primo fra tutti il fenomeno di *hacking*[85]-in italiano, letteralmente *hackeraggio*- la cui prima manifestazione si è avuta con la creazione del primo malware, ideato da Morris Worm.

Fu soltanto il primo di centinaia di migliaia di episodi della stessa natura, spianando la strada ai futuri *hacker*[86], spesso esperti di informatica con le competenze idonee per mettere in atto ogni tipo di condotta lesiva delle libertà altrui (si pensi alla sottrazione di dati bancari, al furto d'identità, all'acquisizione illegittima di dati sensibili ecc.).

All'introduzione dell'intelligenza artificiale si è affiancata quella di *machine learning*[87]-letteralmente apprendimento automatico.

Quest'ultimo, in realtà, affonda le radici in un periodo storico di gran lunga precedente all'intelligenza artificiale così come la si intende oggi. Già negli anni della Seconda guerra mondiale, Alan Turing[88] ideò la macchina alla quale venne affibbiato il suo nome- macchina di Turing o MdT[89]- in grado di generare

[85] Letteralmente "intaccare", facendo riferimento all'attività di compromissione di ogni tipo di dispositivi digitali.

[86] Colui che si serve delle competenze informatiche per hackerare dispositivi altrui.

[87] Machine Learning, Intelligenza Artificiale, powered by WordPress, da intelligenzaartificiale.it.

[88] Alan Turing era un matematico, logico e crittografo della Gran Bretagna, ideatore dell'omonima macchina, grazie alla quale si abbreviò di anni la Seconda guerra mondiale. Turing, padre dell'informatica, venne arrestato per atti osceni quando la polizia britannica venne a conoscenza della sua omosessualità; venne costretto all'assunzione di potenti farmaci per portare a termine la castrazione chimica al quale fu costretto pur di evitare la carcerazione. Si suicidò qualche anno più tardi.

[89] Si tratta di una macchina ideale finalizzata alla manipolazione di dati "contenuti su un nastro di lunghezza potenzialmente infinita, secondo un insieme prefissato di regole ben definite".

algoritmi[90], cruciali nel periodo bellico per decodificare il contenuto di messaggi criptati ed anticipare gli attacchi della Germania.

[90] Gli algoritmi implementabili da una MdT vengono definiti "algoritmi Turing-computabili".

1.4 Il ruolo delle Nazioni Unite: la richiesta di moratoria sulle vendite di tecnologie di sorveglianza

Il 24 ottobre 1945 fu fondata l'Organizzazione delle Nazioni Unite, a cui parteciparono, inizialmente, 51 paesi, oggi divenuti 193[91].

Lo scopo dell'ONU era ed è quello di proteggere e tutelare la pace e sicurezza internazionale[92]; ciò viene assicurato attraverso l'espletamento di funzioni più o meno incisive nel panorama internazionale ed esercitate dai diversi organi che costituiscono la struttura delle Nazioni Unite.

Queste ultime vantano una composizione di sei organi principali: l'Assemblea Generale, il Consiglio di Sicurezza, il Segretariato Generale, il Consiglio di amministrazione fiduciaria, il Consiglio economico sociale e la Corte Internazionale di Giustizia[93].

Gli organi principali possono essere affiancati da organi c.d. sussidiari, creati ad hoc per portare al termine specifiche missioni per le quali sono richieste competenze tecniche ben precise.

A completare il quadro dei soggetti delle Nazioni Unite, vi sono poi le agenzie specializzate: si tratta di istituti distinti ed autonomi rispetto all'ONU, ma sotto il potenziale controllo di quest'ultima[94].

"Non c'è materia, sia essa attinente alla politica oppure all'economia, ai rapporti sociali, culturali ecc., che non possa rientrare nel campo d'azione dell'ONU[95]."

È così che il testo di Conforti e Focarelli sintetizza l'onnicomprensività dei poteri delle Nazioni Unite.

Tuttavia, il carattere dell'onnipotenza subisce importanti deroghe, limitandosi a poter essere definita tale solo parzialmente.

---

[91] Nazioni Unite, Centro Regionale di Informazione delle Nazioni Unite, 25 ottobre 2019.
[92] Nazioni Unite, Centro Regionale di Informazione delle Nazioni Unite, 25 ottobre 2019.
[93] Orizzonti Politici, Organizzazione delle Nazioni Unite (ONU), Eleonora Ferrari, 16 luglio 2020.
[94] Orizzonti Politici, Organizzazione delle Nazioni Unite (ONU), Eleonora Ferrari, 16 luglio 2020.
[95] Le Nazioni Unite, Benedetto Conforti, Carlo Focarelli, Wolters Klumer, CEDAM, dodicesima edizione, 2020 (pg. 178).

La competenza dell'ONU, infatti, viene in un primo momento limitata alla c.d. *rationae personae,* in relazione agli affari appartenenti Stati non membri[96]; limite, quest'ultimo, già superato da quanto dimostra la prassi dell'Organizzazione stessa. La competenza è poi circoscritta secondo il criterio c.d. *rationae materiae*[97] ovvero meglio conosciuto come *domestic jurisdiction*[98]. La ratio di questa nozione è porre un limite ai poteri esterni: riguarda, per l'appunto, questioni di competenza essenzialmente rimessa all'ordinamento interno dei singoli Stati, membri e non.
Proprio la Carta dell'ONU, all'Articolo 2 paragrafo 7 statuisce il dovere delle Nazioni Unite di rispettare il limite del dominio riservato:

"*Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter Vll*[99]*."*
In ultima istanza, dunque, si può convenire con l'assunto che la funzione primaria che dà vita all'Organizzazione delle Nazioni Unite è certamente il mantenimento della pace e sicurezza internazionale, ma che nel suo espletamento ravvisa infinite ramificazioni di ulteriori difficoltose problematiche e tematiche che ricomprendono un'immensa gamma di settori, fra cui quello della sorveglianza di massa[100].
Alla diffusione dei c.d. "spyware"- peculiari tipologie di *malware*- si è affiancata una complementare ed ingente violazione di numerosi diritti umani. Consistendo gli *spyware*[101], per l'appunto, in software quasi sempre scaricati inconsapevolmente dall'utente all'interno del proprio dispositivo nel corso della navigazione in Internet, è immediata la finalità degli stessi: la loro capacità di insediarsi senza il

[96] Conforti B., Focarelli C., *Le Nazioni Unite*, Wolters Klumer, CEDAM, dodicesima edizione, 2020, (pg.178).
[97] Claudia Pividori, *Competenza Rationae Materiae, Dossier: la Corte Penale Internazionale*, Centro di Ateneo per I Diritti Umani "Antonio Papisca", Universita degli Studi di Padova.
[98] Cannizzaro E., *Diritto Internazionale*, G. Giappichelli Editore- Torino, 2012.
[99] United Nations Charter, entrata in vigore il 24 ottobre 1945.
[100] Conforti B., Focarelli C., *Le Nazioni Unite*, Wolters Klumer, CEDAM, dodicesima edizione, 2020.
[101] Joseph Regan, *Cosa si intende per spyware?* In AVG, (2020).

consenso dell'interessato è volta al solo scopo di captare e sottrarre informazioni, dati sensibili, spesso persino dati bancari per registrarli ovvero trasmetterli a terzi ed usufruirne in modo illecito.

A metà dello scorso agosto, le Nazioni Unite sono intervenute nel panorama internazionale, rappresentate da otto esperti qualificati dell'Ufficio dell'Alto Commissario delle Nazioni Unite[102] per la protezione dei diritti umani.

Ciò è avvenuto allo scopo di richiedere alla NSO Group[103] (acronimo che sta per Niv, Shalev e Omri, fondatori della società israeliana) se e in che misura, servendosi dello spyware *Pegasus* di cui è proprietaria, avesse riscontrato condotte di *due diligence*[104] nell'espletamento delle proprie funzioni, con particolar riguardo alla tutela dei diritti umani e con la precisa raccomandazione di "*dare the register*", espressione volta ad intendere la richiesta dei risultati a cui la società sarebbe pervenuta durante le proprie ricerche.

È stata proprio Michelle Bachelet, in qualità di alto commissario ONU, a sollevare l'importanza del problema proponendo l'imposta di una moratoria sulle tecnologie che-servendosi dell'intelligenza artificiale- rischiano di commettere ingenti violazioni ai danni di molteplici libertà personali e diritti umani.

La società vanta da anni una vasta gamma di clienti, dislocati in circa quaranta Paesi, che utilizzano il malware per molteplici fini: la stessa NSO[105] ha dichiarato che la vendita di questa tecnologia è prevalentemente finalizzata a garantire quanto più possibile la sicurezza nazionale; tuttavia, non mancano- a detta della società israeliana- governi che si servono di *Pegasus*[106] al solo scopo di sorvegliare i cittadini ed entrare in possesso di dati sensibili, non altrimenti collezionabili.

Complementarmente all'azione delle Nazioni Unite, che richiedevano la creazione di un quadro normativo idoneo a garantire un utilizzo lecito di queste tecnologie di

[102] (F.P.), *Scandalo spyware: Onu, gli esperti chiedono una moratoria sulla vendita di tecnologie di sorveglianza* in SIR Agenzia d'Informazione, (2021).

[103] NSO Group, Cyber intelligence for global security and stability, About Us, da nsogroup.com.

[104] La Due diligence, Studio Previti Associazione Professionale, 27/11/2020, da previti.it.

[105] Patrizia Licata, Spyware e tecnologie di sorveglianza, l'Onu: "Stop alla vendita, servono regole", 12/08/2021, da corrierecomunicazioni.it.

[106] Arianna Rigoni, *Pegasus Spyware, il virus che infetta sistemi iOS e Android, Cyberment*, da cyberment.it.

sorveglianza, è stata aperta una nuova indagine, il cosiddetto *Progetto Pegasus*[107], condotta da diversi media, coordinati dalla ONG Amnesty International[108] e da Forbidden Stories[109], per l'accertamento di violazioni circa le modalità di utilizzo dello spyware in questione: lo stesso veniva utilizzato per intercettare cittadini e non solo. Fra i soggetti interessati dall'illecito vi erano poi importanti entità politiche, giornalistiche (es. Cnn, New York Times) e figure di attivisti dediti alla lotta dei diritti umani. L'ammontare dei numeri telefonici sorvegliati superava i 50 mila utenti[110].

Non è questo, però, l'unico scandalo che ha riguardato la NSO Group, che aveva già in precedenza bloccato e sospeso temporaneamente l'utilizzo del software ad alcuni clienti, a seguito di importanti segnalazioni sull'utilizzo che questi ultimi ne facevano. A differenza del *Progetto Pegasus*[111], in questo caso il ruolo centrale è stato giocato dal NPR, una testata giornalistica americana che, grazie a fonti anonime interne alla società israeliana, è riuscita a divulgare informazioni circa l'indagine interna alla NSO.

Alcune indiscrezioni giornalistiche, tra cui il Washington Post, avrebbero addirittura identificato i clienti colpevoli delle condotte lesive di diritti umani: vi rientrerebbero l'Arabia Saudita, l'Ungheria, e ancora Marocco, Ruanda, Kazakistan, Azerbaijan, Bahrain, agenzie del Messico ed il governo di Dubai.

Attualmente, la proprietaria di *Pegasus* non ha ancora inibito la sospensione prevista per alcuni clienti dall'utilizzo del software[112].

Ciò che è certo, comunque, è la persistenza da parte della NSO Group nel tentare di non compromettere la propria immagine, nonostante le aperte ammissioni della

---

[107] Tommaso Meo, *L'azienda Nso ha impedito ad alcuni clienti di usare il suo spyware Pegasus in WIRED, (2021).*

[108] Amnesty International, ONG nata nel 1961, fondata da Peter Benenson, allo scopo di tutelare I diritti umani e prevenire la loro violazione su scala globale.

[109] Forbiddden Stories, nata nel 2017, fondata da Laurent Richard a aParigi, è un'organizzazione senza scopo di lucro, con lo scopo di portare avanti e pubblicare lavori ed operati di giornalisti e scrittori condannati a morte, tortura o alla detenzione.

[110] Tommaso Meo, *Lo spyware Pegasus ha spiato giornalisti e attivisti in tutto il mondo*, Wired, (2021).

[111] Pegasus: What you need to know about Israeli spyware, Aljazeera, 8/02/2022.

[112] Kevin Carboni, *L'azienda che ha sviluppato lo spyware Pegasus è finita nella lista nera degli Stati Uniti*,Wired, 2021.

vendita del software ad agenzie di intelligence, per la presunta lotta al terrorismo e per la prevenzione dei crimini contro la sicurezza nazionale[113].

La società israeliana non ha del tutto fornito spiegazioni esaustive anche in merito alla stessa indagine interna, continuando a restare su posizioni contraddittorie e poco convergenti con il resto delle indagini effettuate da altre istituzioni e persino con la richiesta delle Nazioni Unite di moratoria sulla vendita delle tecnologie come *Pegasus* per combattere il fenomeno della violazione di privacy ed altri diritti umani, quali la libertà e segretezza della corrispondenza, nonostante l'assenza di un assetto normativo idoneo a prevenire future ripetute condotte come quella qui sopra descritta[114].

Anche l'Unione Europea ha fatto sentire la propria voce, grazie al commissario europeo per la Giustizia, Didier Reynders, incoraggiando ad approfondire l'indagine sulla gestione, vendita, utilizzo di Pegasus, sottolineando la necessità urgente di un quadro legislativo chiaro che tuteli la privacy degli individui[115]; l'unica eccezione ammessa, a sfavore della privacy del singolo, è l'ipotesi di contrasto al terrorismo, che acconsentirebbe acché i governi degli stati membri possano ledere la segretezza della corrispondenza degli utenti sorvegliati.

Lo stesso Reynders ha posto particolare attenzione al caso dell'Ungheria e- soprattutto- all'ordinamento legislativo di quest'ultima, molto meno garantista sotto il punto di vista della privacy rispetto agli altri stati membri dell'Unione: sarebbe l'unico Paese nel quale non si rende necessaria un'autorizzazione giudiziaria per poter procedere ad una vera e propria violazione di diritti umani a scapito dei cittadini e dunque intromettersi senza consenso nei dispositivi interessati al fine di captarne i dati d'interesse; tutto ciò, però, sarebbe permesso solo ed esclusivamente nelle ipotesi di minaccia alla sicurezza del Paese[116].

---

[113] Pegasus, lo spyware di NSO Group usato per attacchi a funzionari di stato americani, 3/12/2021, da hdblog.it

[114] Luca Zaninello, Pegasus: lo spyware che sorveglia politici, giornalisti e attivisti dal 2016, 19/07/2021, da tomshw.it.

[115] Luigi Mastrodonato, *Contro gli spyware qualcosa si muove in Europa e all'Onu* in WIRED, (2021).

[116] Luigi Mastrodonato, *Contro gli spyware qualcosa si muove in Europa e all'Onu* in WIRED, (2021).

Lo stesso governatore ungherese Viktor Orbàn[117] si sarebbe servito del famoso spyware per sorvegliare più di cinquanta giornalisti ovvero esponenti dell'opposizioni, come Gyorgy Gemési.

È da precisare, comunque, che il background storico dell'agenzia israeliana complice, non depone di certo a proprio favore: gravi episodi avevano già compromesso l'integrità nella NSO nei due anni precedenti.

Nel 2019 la NSO è stata parte in causa citata in giudizio da Whatsapp per la violazione della privacy dei suoi utenti, servendosi dello spyware *Pegasus*[118].

Nel 2020 la Citizen Lab, riconosciuta organizzazione di ricerca, aveva inoltre scoperto l'hackeraggio di trentasei telefoni cellulari appartenenti a membri del news network Al Jazeera, ancora una volta utilizzando Pegasus[119].

[117] Viktor Orbán using NSO spyware in assault on media, data suggests, Shaun Walker in Budapest, 18/07/2021. The Guardian.

[118] Tommaso Meo, *Uno spyware per Android e iPhone è collegato ad attacchi terroristici e omicidi?* da wired.it (2021).

[119] Tommaso Meo, Uno spyware per Android e iPhone è collegato ad attacchi terroristici e omicidi? da wired.it (2021).

1.5 Le operazioni di *mass surveillance* per la lotta al terrorismo: l'operato dell'intelligence all'indomani dell'attacco terroristico dell'11 settembre

L'avvento del fenomeno terroristico con sempre più progressiva frequenza, condusse l'Assemblea Generale delle Nazioni Unite prima, e l'Unione Europea poi, ad emanare rispettivamente *Reports* e Direttive vincolanti, allo scopo di contenere, prevenire e contrastare i reati terroristici in tutto il mondo.

La più importante tra le emanazioni comunitarie è costituita dalla Direttiva UE 2017/541[120] sulla lotta contro il terrorismo, la cui trasposizione negli ordinamenti interni sarebbe dovuta avvenire entro l'anno successivo.

Lo scopo della Direttiva era quello di ampliare il raggio di criminalizzazione e conseguente sanzione di molteplici condotte che avessero a che fare con il fenomeno terroristico: reati di terrorismo, direzione e partecipazione a un gruppo terroristico, reclutamento a fini terroristici, organizzazione o agevolazione di viaggi a fini terroristici, il finanziamento e la fornitura di addestramento a fini terroristici, reati connessi di provocazione pubblica del terrorismo, i viaggi a fini terroristici, concorso, istigazione e tentativo.[121] Il contenuto della Direttiva ricalca l'operato del Consiglio d'Europa del maggio 2005[122], riunitosi per la firma di una Convenzione sulla prevenzione del terrorismo: un testo di 32 articoli che mira a rendere omogenea una disciplina penale a livello comunitario[123].

Il Consiglio, spinto dall'aumento di casi di matrice terroristica, condannava i reati terroristici, escludendo ogni causa di giustificazione di natura alcuna e "*recalling*

[120] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.

[121] La lotta al terrorismo e i diritti umani nei tribunali, Indicazioni per giudici, pubblici ministeri e avvocati sull'applicazione della Direttiva UE 2017/541 sulla lotta al terrorismo, International Commission of Jurists, Geneva, Switzerland, 2020.

[122] Commission Delegated Regulation (EU) 2022/486 of 21 January 2022 amending Annexes I and III to Delegated Regulation (EU) No 906/2014 supplementing Regulation (EU) No 1306/2013 of the European Parliament and of the Council as regards the calculation methods of public intervention expenditure.

[123] Si basa, altresì, sul UN Security Council Resolution 2178 e sull'Additional Protocol to the Council of Europe's Convention on the Prevention of Terrorism.

the obligation of all Parties to prevent such offences and, if not prevented, to prosecute and ensure that they are punishable by penalties which take into account their grave nature[124] [125];"

Questo implicava, per l'appunto, l'introduzione di un obbligo alla criminalizzazione internazionale dei reati terroristici, sottolineando la vincolatività del dettato della Convenzione per i destinatari, nonché gli Stati Membri. Il vincolo, tuttavia, non ha mai intaccato i diritti d'espressione e libertà di pensiero delle legislazioni interne, preoccupandosi anzi, di prevedere una sufficiente forma di tutela dei diritti umani, nel bilanciamento con la necessità di contrasto alle organizzazioni terroristiche.

Prima di passare in rassegna le singole condotte penalmente sanzionate, la Convenzione si occupa- nei primi 4 articoli- di identificare una terminologia ed uno scopo, di individuare le politiche nazionali di prevenzione e di cooperazione internazionale in materia di prevenzione. Rispettivamente così l'operato del Consiglio d'Europa recita[126]:

Article 1: *Terminology*

1. For the purposes of this Convention, 'terrorist offence' means any of the offences within the scope of and as defined in one of the treaties listed in the Appendix.

2. On depositing its instrument of ratification, acceptance, approval or accession, a State or the European Community which is not a party to a treaty listed in the Appendix may declare that, in the application of this Convention to the Party concerned, that treaty shall be deemed not to be included in the Appendix. This declaration shall cease to have effect as soon as the treaty enters into force for the Party having made such a declaration, which shall notify the Secretary-General of the Council of Europe of this entry into force.

Article 2: *Purpose*

[124] Council of Europe Convention on the Prevention of Terrorism, Council of Europe Treaty Series - No. 196, Warsaw, 16.V.2005.

[125] Council of Europe Convention on the Prevention of Terrorism, Warsaw, 16 May 2005, Official Journal of the European Union.

[126] Council of Europe Convention on the Prevention of Terrorism, Council of Europe Treaty Series - No. 196, Warsaw, 16.V.2005.

The purpose of the present Convention is to enhance the efforts of Parties in preventing terrorism and its negative effects on the full enjoyment of human rights, in particular the right to life, both by measures to be taken at national level and through international cooperation, with due regard to the existing applicable multilateral or bilateral treaties or agreements between the Parties.

Article 3: National prevention policies

1. Each Party shall take appropriate measures, particularly in the field of training of law enforcement authorities and other bodies, and in the fields of education, culture, information, media and public awareness raising, with a view to preventing terrorist offences and their negative effects while respecting human rights obligations as set forth in, where applicable to that Party, the Convention for the Protection of Human Rights and Fundamental Freedoms, the International Covenant on Civil and Political Rights, and other obligations under international law.

2. Each Party shall take such measures as may be necessary to improve and develop the cooperation among national authorities with a view to preventing terrorist offences and their negative effects by, inter alia:

a. exchanging information;

b. improving the physical protection of persons and facilities;

c. enhancing training and coordination plans for civil emergencies.

3. Each Party shall promote tolerance by encouraging inter-religious and cross-cultural dialogue involving, where appropriate, non-governmental organisations and other elements of civil society with a view to preventing tensions that might contribute to the commission of terrorist offences.

4. Each Party shall endeavour to promote public awareness regarding the existence, causes and gravity of and the threat posed by terrorist offences and the offences set forth in this Convention and consider encouraging the public to provide factual, specific help to its competent authorities that may contribute to preventing terrorist offences and offences set forth in this Convention.

Article 4: *International cooperation on prevention*

Parties shall, as appropriate and with due regard to their capabilities, assist and support each other with a view to enhancing their capacity to prevent the commission of terrorist offences, including through exchange of information and

best practices, as well as through training and other joint efforts of a preventive character[127]."

L'intera Direttiva verrà comunque integrata da un *Protocollo Addizionale della Convenzione del Consiglio d'Europa per la prevenzione del terrorismo,* [128] redatto a Riga in data 22 ottobre 2015 allo scopo di meglio delineare i tratti distintivi dell'indole terroristica di ogni condotta e cristallizzare condizioni e garanzie più generose. Al Protocollo, poi, seguirono due ulteriori atti: la Decisione (UE) 2018/889[129] che conclude la convenzione del Consiglio d'Europa sulla prevenzione del terrorismo a nome dell'UE e la Decisione (UE) 2018/890[130] che, a sua volta, conclude il Protocollo di supplemento alla Convenzione del Consiglio d'Europa sulla prevenzione del terrorismo per conto dell'UE, entrambe redatte in data 4 giugno 2018 a Lussemburgo, all'interno delle quali si ritrova il riconoscimento del suddetto Protocollo addizionale e della Convenzione stessa[131].

Sulla scia di importanti Risoluzioni del Consiglio di Sicurezza delle Nazioni Unite,[132] dunque, l'Unione Europea decise di uniformare una disciplina comunitaria che potesse stare al passo con quella statunitense in continuo sviluppo all'indomani della strage delle *Twin Towers*[133].

---

[127] Council of Europe Convention on the Prevention of Terrorism, Council of Europe Treaty Series - No. 196, Warsaw, 16.V.2005.

[128] Commission Delegated Regulation (EU) 2022/486 of 21 January 2022 amending Annexes I and III to Delegated Regulation (EU) No 906/2014 supplementing Regulation (EU) No 1306/2013 of the European Parliament and of the Council as regards the calculation methods of public intervention expenditure.

[129] Commission Delegated Regulation (EU) 2022/486 of 21 January 2022 amending Annexes I and III to Delegated Regulation (EU) No 906/2014 supplementing Regulation (EU) No 1306/2013 of the European Parliament and of the Council as regards the calculation methods of public intervention expenditure.

[130] Commission Delegated Regulation (EU) 2022/486 of 21 January 2022 amending Annexes I and III to Delegated Regulation (EU) No 906/2014 supplementing Regulation (EU) No 1306/2013 of the European Parliament and of the Council as regards the calculation methods of public intervention expenditure.

[131] Trattato aperto alla firma degli Stati membri, degli Stati non membri i quali hanno partecipato alla sua elaborazione e dell'Unione europea e all'adesione degli altri Stati non membri, entrata in vigore il 01/06/2007 con 6 Ratifiche inclusi 4 Stati membri.

[132] Resolution 2178, Threats to international peace and security caused by terrorist acts, Security Council Distr.: General 24 September 2014, Resolution 2178 (2014), adopted by the Security Council at its 7272nd meeting, on 24 September 2014.

[133] World Trade Center History, da 911memorial.org

L'attacco terroristico alle torri gemelle dell'11 settembre del 2001 mutò radicalmente l'assetto di sorveglianza nazionale ed internazionale, con particolare riferimento al regime statunitense. I tre giorni successivi, fino al 14 settembre, furono decisivi per l'implemento della *mass surveillance*, al termine dei quali, l'amministrazione americana, a quei tempi sotto la guida di George W. Bush, emanò la *Declaration of National Emergency by Reason of Certain Terrorist Attacks*[134], di concerto con il Congresso. Il contenuto della dichiarazione prevedeva la possibilità di "utilizzare tutte le forze adeguate e necessarie contro tutte le nazioni, organizzazioni o persone"[135] che il Presidente riteneva potessero essere coinvolti in potenziali azioni terroristiche. La dichiarazione d'emergenza nazionale di metà settembre 2001 fu emanata sulla falsariga del *War Power Resolution*- ovvero *War Powers Act*[136]- emanato quarantotto anni prima, nel 1973 sotto l'amministrazione Nixon- che rappresentava *"a congressional Resolution designed to limit the U.S. president's ability to initiate or escalate military actions abroad."*[137] Il contenuto di questa Risoluzione legittimò *latu sensu* il Presidente Bush a dichiarare l'emergenza nazionale ed emanare il *Military Order* a seguito dell'attacco terroristico, con il quale dichiarava la nazione in uno stato di conflitto armato, potenzialmente necessitante di forze militari armate degli Stati Uniti.

All'ordine militare seguì poi l'emanazione da parte dello stesso Presidente dello *USA Patriot Act*-ovvero *Uniting and Strenghtening America by Providing Appropriate Tool Required to Intercept and Obstruct Terrorism Act*[138]- il 26 ottobre 2001: il contenuto dell'atto fu un passo fin troppo grande per il diritto di sorveglianza, implicando un incremento dei poteri invasivi delle maggiori agenzie di sicurezza interna nazionale e d'intelligence, quali la CIA, l'FBI e l'NSA.

Tra questi rientrava la totale discrezionalità rimessa alle forze di polizia circa l'intrusione nella vita privata dei cittadini americane, senza distinzioni,

---

[134] Executive Documents, Proc. No. 7463. Declaration of National Emergency by Reason of Certain Terrorist Attacks, Proc. No. 7463, Sept. 14, 2001, 66 F.R. 48199.

[135] Roberto Colella, *Patriot Act: il concetto di 'wartime' che schiaccia i diritti costituzionali* in Il Fatto Quotidiano (2021).

[136] Joint Resolution of November 7, 1973, Public Law 93-148, 87 STAT 555, concerning the war powers of congress and the president; 11/7/1973.

[137] Nixon Library, War Powers Resolution of 1973 July 27, 2021, da nixonlibrary.gov.

[138] ADIR, L'altro diritto, Cyber-sorveglianza e tutela della privacy dopo l'11 settembre 2001, Marika Surace, 2005. (par. 3.2.1).

intercettando anche gli individui non sospettati, avendo accesso ai luoghi d'interesse e potendo effettuare perquisizioni senza previa autorizzazione di un magistrato. Ad incrementare la pericolosità del contenuto, vi era l'introduzione della nozione di *azioni terroristiche*, del tutto generica e la cui qualificazione era rimessa nelle mani di un'ampia discrezionalità[139]. L'invasività e l'incidenza di misure del genere nella vita dei cittadini portò questi ultimi a sollevare importanti questioni di illegittimità costituzionale circa alcune sezioni del Patriot Act, con particolar riferimento alla 215, la 218 e la 505, lesive della tutela della privacy e libertà personali[140].

A mitigare queste gravi violazioni delle libertà personali, sarebbero state introdotte le c.d. "*sunset provisio*ns", che oggi potremmo definire riserve in grado di invalidare alcune delle disposizioni maggiormente lesive del Patriot Act. Già all'indomani dell'attacco terroristico[141], il Presidente Bush aveva dichiarato che la sua amministrazione non avrebbe parlato dei piani previsti, ma prometteva di trovare gli autori dell'attacco e di far scontare loro le rispettive pene. Il giorno dell'attacco si stimava che il 74% dei cittadini americani avrebbero dovuto rinunciare ad una parte delle loro libertà personali; di questo 74%, l'86% si mostrava propenso a sacrificare propri diritti in cambio di maggiore sicurezza.[142] Il Patriot Act fu seguito poi dall'Homeland Security Act[143], emanato anch'esso sotto l'amministrazione Bush il 25 novembre del 2002, a poco più di un anno dall'attacco al World Trade Center. Anche quest'ultimo introduceva un ampliamento dei poteri delle forze dell'ordine e dell'intelligence americana, permettendo addirittura l'intercettazione di e-mail di chiunque fosse sospettato di coinvolgimento in azioni

[139] Associazione Italiana dei Costituzionalisti, Stati Uniti: emergenza terrorismo e due process of law, Tania Groppi, Democrazia e Terrorismo. Diritti fondamentali e sicurezza dopo l'11 settembre 2001, Editoriale Scientifica, Napoli, 2006.
[140] Roberto Colella, Patriot Act: il concetto di 'wartime' che schiaccia i diritti costituzionali in Il Fatto Quotidiano (2021).
[141] De Vergottini G., La difficile convivenza tra libertà e sicurezza. La risposta delle democrazie al terrorismo, in Rassegna parlamentare, 2004.
[142] ADIR, L'altro diritto, *Cyber-sorveglianza e tutela della privacy dopo l'11 settembre 2001*, Marika Surace, 2005, (par.3.2.2).
[143] Homeland Security Act of 2002, Public Law 107–296—NOV. 25, 2002 116 STAT. 2135, Public Law 107–296 ,107th Congress.

o movimenti terroristici, senza previa autorizzazione da parte di un'autorità giudiziaria, essendo sufficiente quella di "*un'entità governativa*[144]*."*

Ciò che scatenò una rivoluzione del controllo fu l'idea-a tratti insinuazione- che se i colpevoli dell'attacco fossero stati schedati e registrati, se fossero stati controllati, probabilmente nessun attacco avrebbe avuto luogo.

È così che nel panorama collettivo furono formulate pesanti accuse nei confronti delle agenzie di intelligence che gestivano tutti i dati da trasmettere alla White House: le accuse sostenevano un'importante negligenza dei servizi segreti nella tempestiva comunicazione dei rischi di un attacco terroristico simile. Non meno gravi accuse furono mosse nei confronti del discussissimo Echelon[145], il Grande Occhio elettronico di cui si servivano i servizi segreti statunitensi per spiare il resto del mondo.

Questo perché tutte le agenzie d'intelligence erano obbligate ad inviare ogni giorno un sunto di tutti i dati ricevuti; ma si trattava di dati più volte e da più agenti- gerarchicamente posizionati a livelli diversi- selezionati[146], trascurandone inevitabilmente qualcuno che, come nel caso delle Torri Gemelle, avrebbe potuto rivelarsi fatale e decisivo.[147]

Per tutta risposta, l'intelligence propose di comunicare giornalmente l'intero ammontare di dati acquisiti, senza apportare alcuna modifica ovvero selezione, che- qualora fosse stata considerata necessaria- sarebbe poi stata apportata direttamente dalla Casa Bianca o dal Presidente in persona: il sociologo e scrittore tedesco Kreissl, definisce questa prassi come "*cercare un ago in un pagliaio*."

Con questa premessa, Kreissl ha voluto dimostrare la fallacia dell'assetto di sorveglianza così come previsto a quel tempo[148], proponendo, d'altro canto, un modello che valorizzasse e si concentrasse maggiormente a livello locale, non

---

[144] ADIR, L'altro diritto, Cyber-sorveglianza e tutela della privacy dopo l'11 settembre 2001, Marika Surace, 2005, (par.3.2.3)

[145] Lawner K. J., Post-Sept. 11th International Surveillance Activity - A Failure of Intelligence: The Echelon Interception System & the Fundamental Right to Privacy in Europe, 14 Pace Int'l, (2002).

[146] Si trattava di centinaia di migliaia di dati che passavano per le mani di migliaia di analisti, che venivano poi sottoposti ad innumerevoli selezioni e controlli da parte dei preposti, capi, fino ad arrivare alle agenzie di intelligence statunitensi.

[147] La guerra tra CIA e FBI e gli errori dell'11 settembre, Alberto Bellotto, 12 settembre 2018, da insideover.com

[148] Dr Reinhard Kreissl, Terrorism, mass surveillance and civil rights, www.vicesse.eu

focalizzato sui *mass data*, citando come esempio calzante il sistema di servizi segreti gestito dalla Città del Vaticano.

Per questo motivo, sarebbe auspicabile affiancare al sistema di sorveglianza internazionale, incentrato sulla lotta al terrorismo, una pseudo succursale, che si preoccupi di quanto succeda nel territorio simultaneamente; dunque, una non esclude l'altra. Il cambiamento di una procedura di sorveglianza è dato dalla constatazione della fallacia dei precedenti procedimenti[149].

E lo dimostra adducendo esempi di restrizioni e maggiori controlli dovuti ad episodi che dimostravano l'inidoneità dei precedenti: dopo il tentativo di Richard Reid di portare su un aereo un esplosivo in una scarpa, tutti i passeggeri presso gli aeroporti statunitensi- da lì in poi- avrebbero dovuto sottoporre le loro calzature ad un controllo tramite scanner e passare dal metal detector scalzi. Un secondo esempio apportato da Kreissl è il tentativo di introdurre clandestinamente un esplosivo su un aereo in un contenitore per liquidi; dopo quell'episodio, vennero proibiti- o ridottane la quantità trasportabile- i liquidi in cabina.

Qualche anno più tardi, la storia si ripeté con l'attacco terroristico alla maratona di Boston il 15 luglio 2013.

Nonostante i servizi segreti russi avessero previamente segnalato la potenziale pericolosità dei due fratelli, autori dell'attacco, per il loro esagerato avvicinamento all'Islam radicale- Dzokar e Tamerlav Tsarnaev[150]- l'informazione sembrò essere presa sottogamba. Qui di seguito viene illustrato l'assetto della sorveglianza delle agenzie di intelligence americane prima dell'attacco di Boston e le informazioni di cui erano a conoscenza [151].

Letteralmente un grafico su "*cosa pensiamo di sapere su chi sapeva e quando*", che include: cosa conoscessero le agenzie federali, cosa ci fosse da conoscere e cosa le forze dell'ordine locali sapessero. Con un semplice schema, rappresenta la logica errata che sottostava ad una sorveglianza piena solo astrattamente.

---

[149] Dr Reinhard Kreissl, Terrorism, mass surveillance and civil rights, www.vicesse.eu

[150] Entrambi islamisti radicali che, in nome della religione, fecero esplodere due ordigni costruiti amatorialmente con pentole a pressione, posizionate in punti strategici di Boston, causando 3 morti e 260 feriti. Tamerlav morì in uno scontro a fuoco con la polizia statunitense; Dzokar venne catturato pochi giorni dopo e processato, con successiva condanna alla pena capitale, sancita dall'unanimità della giuria.

[151] Dr Reinhard Kreissl, *Terrorism, mass surveillance and civil rights,* www.vicesse.eu

In conclusione, la legislazione americana ha vissuto imponenti sviluppi per quanto riguarda il diritto di sorveglianza attribuito in grande misura alle agenzie di intelligence; ma ciò che colpisce e fa riflettere è la brevità del lasso di tempo durante il quale, il suddetto quadro normativo ha subito importanti modifiche, tutte quante approvate- non senza opposizioni scomode- ed entrate in vigore nel giro di un anno[152].

[152] ADIR, L'altro diritto, Cyber-sorveglianza e tutela della privacy dopo l'11 settembre 2001, Marika Surace, 2005.

1.6 Il diritto di sorveglianza ed i Business Rights: The Wassenaar Arrangement

I Business Rights-letteralmente Diritti d'Impresa- appartengono ai titolari delle attività d'impresa ovvero alle multinazionali e devono necessariamente essere analizzati *in compliance* con i diritti umani[153], il cui rispetto è- o dovrebbe- essere garantito dai pilastri stilati dalle Nazioni Unite[154]: I Principi Guida in materia di impresa e diritti umani. Sono tre le materie fondamentali alla base dei Principi: l'obbligo che grava sugli Stati di proteggere i diritti umani[155], la responsabilità dell'impresa di rispettare i diritti umani (facenti parte della prima sezione dedicata allo Stato) e l'accesso ai rimedi [156](parte della seconda sezione dedicata alle imprese). Corollario dell'intera lista dei Principi Guida è la c.d. "due diligence"[157], pretesa dalle condotte di imprese e stati[158] [159].

Un'esaustiva definizione dei business rights viene fornita dal *Law Insider Dictionary* che indica i diritti d'impresa come "the benefit of all rights, entitlements or claims to which the CTSL Business is entitled arising directly or indirectly out of or in connection with the operation of the CTSL Business (including as arising under any warranty, condition, guarantee, indemnity, contract, agreement or policy of insurance) other than, for the avoidance of doubt, any rights, entitlements or

[153] About business and human rights, OHCHR and business and human rights, da ohchr.org, (Even if States do not fulfill their obligations, all business enterprises are expected to respect human rights, meaning they should avoid infringing on the human rights of others, and should address adverse human rights impacts with which they are involved.)

[154] Guiding Principles on Business and Human Rights, Implementing the United Nations "Protect, Respect and Remedy" Framework, United Nations Human Rights Office of the High Commissioner, New York and Geneva, 2011.

[155] Business and Human Rights, Bureau of Democracy, Human Rights and Labor, U.S. Department of State, da state.gov

[156] Claudia Cantone, *Business and Human rights*: intervista all'avv. Giacomo Maria Cremonesi, in Ius In Itinere, (2018).

[157] 10th anniversary of the UN Guiding Principles on Business and Human Rights, United Nations Human Rights Office of the High Commissioner, 16 luglio 2021.

[158] Business and Human Rights: Access to Justice and Effective Remedies (with input from the European Union Agency for Fundamental Rights, FRA), Report of the European Law Institute, ELI, (2018-2021).

[159] Bray R., Pretelli I., *Accesso alla giustizia per vittime di violazioni di diritti fondamentali e danni socioambientali nella catena di approvvigionamento delle imprese multinazionali*, 2021.

claims of the Seller arising from or in connection with this Agreement or the Deed of Warranty and "Business Right" shall mean the benefit of any of them[160].

Ma in che modo i Business Rights possono essere oggetto di sorveglianza da parte degli stati? Si può risolvere il quesito apportando un esempio, che è emblema di quanto invadente possa essere il controllo nazionale ed internazionale anche sulla vendita di beni o servizi: The Wassenaar Arrangement[161].

Con precisione, *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* è un regime di controllo multilaterale sulle esportazioni (MECR, Multilateral Export Control Regime) di cui fanno parte 42 stati[162].

Si tratta di un accordo con il quale le potenze aderenti attuano una politica volta ad assicurare la trasparenza nelle transazioni che abbiano ad oggetto *conventional arms and dual-use goods and technologies*[163], per la sicurezza nazionale ed internazionale; lo scopo ultimo è comunque quello di controllare che non vi siano accumulamenti di beni di quella natura che implicherebbero un incremento del potere militare a favore di alcuni stati[164].

L'accordo non permette a nessuno degli stati membri, di esercitare potere di veto ed è comunque necessario evidenziare che gli atti derivanti da questo accordo ovvero ogni loro espletamento non è giuridicamente vincolante non godendo di natura pattizia; quindi, si tratta di una condotta totalmente gratuita e spontanea degli stati a volersi sottoporre ad un controllo simile.

La sorveglianza di armi convenzionali è d'altronde necessaria per assicurare che anche stati non membri dell'accordo non godano di un eccessivo potere militare[165],

[160] Business Rights definition, Law Insider dictionary, da lawinsider.com

[161] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies Fact Sheet Released by the Bureau of Nonproliferation March 22, 2000, Washington, D.C.U.S. Department of State.

[162] Wikipedia, The Wassenaar Arrangement

[163] Wassenaar Arrangement, NTI Building a Safer World, Nuclear, Conventional Weapons and Dual-Use, 14 luglio 2020, da nti.org

[164] The Wassenaar Arrangement at a Glance, Arms Control Association, Daryl Kimball, Executive Director, 2022, da armscontrol.org

[165] L'Accordo di Wassenaar, Gli Stati parte dell'Accordo di Wassenaar (Wassenaar Arrangement) mirano a impedire l'accumulazione destabilizzante di armi convenzionali e beni dual use, Confederazione Svizzera, Segreteria di Stato dell'Economia SECO, 30 aprile 2021.

ragion per cui vi è uno scambio di informazioni tra gli stati membri e non, perlomeno sulle transazioni di beni più significative (aerei militari, elicotteri militari, navi da guerra, ecc.).

Infine, l'accordo di Wassenaar ha costituito un Segretariato generale con funzioni gestionali con sede a Vienna.

1.7 I social media come principale risorsa di *mass surveillance*

La sorveglianza di massa così come intesa fin qui, ha trovato un fedele alleato nella sua spasmodica ricerca del controllo totale: si tratta della nascita delle piattaforme sociali, o più comunemente chiamate *social media*[166].

Muovendo i primi passi dalla piattaforma *MSN Messenger*[167], la tecnologia ha progressivamente traslato parti sempre più importanti della vita sociale dalla realtà pragmatica della quotidianità[168] a piattaforme online che consentono di interagire con utenti da ogni parte del mondo[169].

La piattaforma di Msn consentiva un'attività di messaggistica servendosi della rete Internet che- con una veloce registrazione attraverso la creazione di un'e-mail- permetteva di aggiungere alla rete di contatti ogni soggetto di cui si conoscesse la mera e-mail. Così, in realtà, senza l'accertamento dell'età e identità degli users, ci si poteva collegare con ogni potenziale interlocutore a conoscenza del proprio indirizzo elettronico. Dalla piattaforma introdotta sul mercato da Microsoft, iniziò un'escalation di piattaforme sociali, progressivamente più sofisticate, con maggiori funzioni e scopi anche più spinti. La grande svolta arrivò con il lancio di *Facebook*[170] nel febbraio del 2004 ad opera di Mark Zuckerberg, il vero primo e proprio social network su scala mondiale che inglobava una quantità di dati di gran lunga più consistente rispetto a tutto ciò che era esistito fino a quel momento[171].

---

[166] Definition of social media, Merriam-Webster since 1928, (: forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos), febbraio 2004.

[167] Microsoft Launches MSN Messenger Service, July 21 1999, REDMOND, Wash., July 21, 1999

[168] Benkler Y., *La ricchezza della rete. La produzione sociale trasforma il mercato e aumenta le libertà*, Università Bocconi, 2006.

[169] Kaplan A. M., Haenlein M., *Users of the world, unite! The challenges and opportunities of social media*, Business Horizons, Vol. 53, 2010.

[170] Facebook launches, HISTORY, A&E Television Networks, Last Updated February 2, 2021, Original Published Date October 24, 2019, da History.com Editors.

[171] The History of Facebook: From BASIC to Global Giant, Brandwatch, January 25th 2019, Josh Boyd, da brandwatch.org

Basti pensare alla possibilità di fare upload illimitati di foto, video e qualsiasi file multimediale, immediatamente alla mercé di tutta la rete. Ciò che in un primo momento sembrò essere l'alleato migliore della rete sociale[172], si rivelò non subito essere il peggior nemico della privacy personale[173].

La capacità dei social media di archiviare quantità infinite di dati ha attirato la curiosità prima, e l'attenzione poi, delle più grandi agenzie di intelligence, consapevoli del potenziale in possesso di quei colossi del mondo social.

Così, ben presto, la condivisione di una foto con annessa geo localizzazione in un locale esclusivo, diventò un dato prezioso per formulare statistiche e controllare i movimenti di ogni singolo utente[174].

Non a caso, per poter inserire una localizzazione su qualsiasi piattaforma, è necessario che l'utente dia espressa autorizzazione all'accesso da parte del social alla posizione rintracciabile grazie al GPS presente nei dispositivi tecnologici.

L'analisi di flussi ingenti di dati, di spostamenti nel mondo, di tendenze, di mode, di opinioni, idee, divergenze, non viene poi sfruttato solo per attività di sorveglianza, ma importanti agenti che ne usufruiscono sono anche le grandi aziende, le imprese e le multinazionali, l'intero mondo dell'e-commerce per esercitare attività di *profiling*[175], letteralmente "the activity of collecting information about someone, especially a criminal, in order to give a description of them"[176]: una vera e propria collezione di dati, archivio e cronologia dei siti web visitati, dell'oggetto d'interesse dell'utente, al fine di ricostruire una personalità fittizia e sottoporre alla sua attenzione offerte, pubblicità sotto ogni forma, di beni e servizi affini all'entità astrattamente costruita[177].

---

[172] De Felice L., Marketing conversazionale. Dialogare con i clienti attraverso i social media e il Real-Time Web di Twitter, FriendFeed, Facebook, Foursquare, 2ª ed., Milano, Il Sole 24 Ore, 2011.

[173] How to Protect Your Privacy on Social Media?, Data Privacy Manager, 20/10/2021, in Blog, Data Privacy, da dataprivacymanager.net

[174] Key Social Media Privacy Issues for 2020, Tulane University, School of Professional Advancement, 2020.

[175] Art. 22 GDPR Automated individual decision-making, including profiling, General Data Protection Regulation.

[176] Cambridge Dictionary.

[177] What does the UK GDPR say about automated decision-making and profiling?, Information Commissioner's Office, da ico.org.uk

Un esempio semplice e diretto di *profiling* è la comparsa di pubblicità nei social di beni e servizi ricercati poco prima su piattaforme di e-commerce[178].

Se, banalmente, effettuo una ricerca su Google per l'acquisto di libri, qualche minuto dopo Instagram mi proporrà un'offerta in corso di una collana di libri o convenienti promozioni di editori famosi[179], disposti a pagare un significativo ammontare di denaro per apparire sulle piattaforme social.

Anche le ricerche di studio o di lavoro, che riguardino articoli online, e-book, documentari su YouTube o un semplice forum di scambio informazioni e opinioni, chiederà l'autorizzazione di rilasciare i cosiddetti *cookies*[180]: con questo termine si intende far riferimento alle tracce che ogni utente lascia su uno specifico sito web che-potenzialmente- aiutano l'utente ad effettuare ricerche più proficue e centrate con i suggerimenti proposti dalla rete stessa. Il nome dato a questo genere di fenomeno si deve all'allusione alle briciole lasciate quando si mangia un biscotto[181].

Dunque, i resti ritrovati permettono di risalire ad un soggetto ben individuato ed asserire *chi è stato dove*.

Per alcuni siti o social media spesso l'accettazione dei cookies è necessaria ed obbligatoria se si vuole usufruire dei servizi offerti e la gran parte degli utenti accetta tutti i cookies[182]- e non soltanto quelli essenziali- ignorando le condizioni generali previste dal regolamento della privacy[183], solitamente pagine e pagine di informazioni dal carattere minuscolo che vengono trascurate poiché ritenute ininfluenti sulla propria permanenza in una piattaforma social.[184]

La realtà dei fatti suggerisce il contrario e, con l'avanzare del tempo e lo sviluppo tecnologico, le funzionalità dei dispositivi sempre più invadenti si celano dietro una

[178] Social Media Monitoring, Personal information gleaned from social media posts has been used to target dissent and subject religious and ethnic minorities to enhanced vetting and surveillance, Patel F., Levinson-Waldman R., Koreh R., DenUyl S., published May 22 2019, last updated March 11 2020, Brennan Center for Justice, da brennancenter.org

[179] Anon D., *How cookies track you around the web and how to stop them*, PRIVACY.net, February 24 2018, da privacy.net

[180] Struttura Informatica, Cookie Policy, Definizione di "cookie" e tecnologie similari

[181] A Guide to Tracking Cookies, CookieYes, March 24, 2022, da cookieyes.com

[182] Dan Q., *Visitor Tracking Without Cookies* (or How To Abuse HTTP 301s), DANQ, 24 April, 2012, da danq.me

[183] Anthony S., How to visualize behavior tracking cookies with a Firefox add-on, Extreme Tech, July 8, 2011, da extremetech.com

[184] Rafter D., *Tracking cookies: What are tracking cookies and how do they work?*, NortonLifeLock, May 6, 2021, Privacy, Norton, da us.norton.com

maschera di facilitazione dell'utilizzo delle app (es. in un dispositivo cellulare o un tablet) e dei servizi, consistendo, in verità, in strumenti sempre più pericolosi ed invasivi della privacy personale[185].

Basti pensare alla nuova tecnologia di riconoscimento facciale che consente di sbloccare un iPhone senza inserire il PIN, ma che allo stesso tempo analizza e archivia la biometria facciale di ogni utente che se ne serva[186].

[185] Geary J., *Tracking the trackers: What are cookies? An introduction to web tracking, Battle for the Internet, Cookies and web tracking*, The Guardian, da theguardian.com, 2017.
[186] Art. 4, par. 1, n. 14 General Data Protection Regulation.

1.8 L'impatto dell'emergenza pandemica da Covid-19 sull'esercizio di operazioni di sorveglianza di massa

Il 2020 è stato l'anno dell'emergenza, dello sconforto, dei fallimenti economici e dell'urgenza di tenere sotto controllo la salute della popolazione. Ma la salute ed i contagi non stati l'unico oggetto di sorveglianza da parte degli agenti nazionali.
Per monitorare i cali e gli aumenti dei contagi, delle morti, dei posti disponibili in terapia intensiva, si è reso necessario un controllo sempre più invadente dei dati personali di chiunque si sottoponesse alle cure, ai tamponi, registrando sulle apposite piattaforme tutti i dati sensibili e creando un vero e proprio archivio dei vivi e dei morti, dei malati e dei guariti[187] [188].
Ancora una volta, a giocare un ruolo decisivo è stata la mano dell'intelligenza artificiale. Simultaneamente all'avvento del virus su scala globale, viene ideata e pubblicizzata una nuova app dall'azienda Bending Spoons, selezionata dal Consiglio dei ministri per il lancio della relativa svolta tecnologico-sanitaria: l'app *Immuni*[189].

Registrando i dati personali, ogni utente autorizza l'app ad avere accesso alla propria geo localizzazione[190], utile perché-attraverso la rete Bluetooth- ne viene segnata la traccia, in modo tale da segnalare eventuali contatti con individui positivi al Covid-19, che avevano registrato la propria presenza nello stesso luogo[191].
Certamente l'app configura uno strumento per la lotta contro il Corona Virus; tuttavia, opinioni contrastanti sono state esposte circa il rispetto della privacy personale con l'avvenuta registrazione e conseguente accesso al Bluetooth che avrebbe conosciuto e riportato ogni spostamento effettuato.

[187] Informativa sul trattamento dei dati personali ex art. 13 del Regolamento (UE) 2016/679, Ministero del Lavoro e delle Politiche Sociali.
[188] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[189] App "Immuni": via libera del Garante privacy, Garante per la Protezione dei Dati Personali, 2020, da garanteprivacy.it
[190] Solombrino E., *La app Immuni vista dal lato della privacy*, Privacy, Risk Management360, Network Digital 360, 21 settembre 2021, da riskmanagement360.it
[191] Punto Informatico, App Immuni: così controlleremo il contagio (2021).

Vero è, però, che- come obiettato dagli inventori dell'app- i dati restano comunque anonimi anche in caso di risultati di positività al virus, così da rispettare il diritto alla privacy[192].

Almeno in parte. Le rassicurazioni dell'azienda non sembrano aver avuto successo se si considera che una grande percentuale dei cittadini italiani ha rifiutato di consentire l'accesso ai propri spostamenti geografici. Infatti, solo il 21% degli smartphone presenti sul territorio nazionale ha scaricato l'applicazione (circa 8 milioni di utenti), di cui il relativo 15% è composto da soggetti maggiori di 14 anni. Ma le accuse di un'imponente sorveglianza di massa vengono mosse già a partire dalle prime disposizioni governative, dunque i meri controlli di assembramenti quando e dove[193].

Considerando le mosse ministeriali, prima fra tutte, il lockdown totale, ogni segnalazione di aggregamenti di un paesino o di un gruppo di amici, era considerata una notizia straordinaria che conduceva l'opinione pubblica a puntare il dito senza pensarci due volte. Come anticipato, forme più incisive di controllo sono subentrate con l'ideazione di nuovi strumenti digitali che permettevano e permettono il c.d. "contact tracing": tracciamento dei contatti, quasi un inseguimento dei positivi al Covid-19[194].

È così che si può ravvisare un parallelismo come prospettato da Bentham ai tempi dell'epidemia da peste nel Seicento. In quella cornice storica, Jeremy Bentham auspicava ad applicare il suo progetto panottico all'emergenza in corso, per avere il controllo sulla patologia e sui malati rimasti vittime.

Il parallelismo tra il Panopticon per la peste e la sorveglianza di massa con strumenti digitali per il Covid-19 non è condivisibile per un solo motivo: la differenza dell'oggetto di sorveglianza.

[192] Occhipinti S., *App Immuni, via libera dal Garante della privacy*, IP, IT e Data Protection, Altalex,da altalex.com, 2020.
[193] Lemma V., *COVID-19: il trattamento dei dati sanitari tra privacy e interesse pubblico*, 8 giugno 2020, OMAR osservatorio malattie rare, da osservatoriomalattierare.it
[194] Coronavirus e protezione dei dati, Garante per la Protezione dei Dati Personali, 2020, da garanteprivacy.it

Se in un primo momento la caccia puntava al corpo, adesso ha come unico scopo la mente[195].

È proprio la *paura sociale* ad aver spinto milioni di cittadini titolari di diritti e libertà personali, a segregarsi in casa, a non avere più nessun contatto interpersonale: per paura di un contagio, di un ricovero, della morte. La paura sociale ha permesso di sacrificare un bene minore del singolo- quali ad esempio la libertà di circolazione, la riservatezza di alcuni dati sensibili- a favore di un bene maggiore della collettività: la sicurezza sanitaria nazionale.

Il problema della sorveglianza di massa durante un'epidemia o pandemia, però, continua a preoccupare filosofi e scrittori, uno fra tanti Yuval Noah Harari, che in uno spazio del Financial Times[196] si è espresso circa il pericolo latente che deriva dal ricorso a questa digitalizzazione a lungo termine.

Harari ha già sottolineato la differenza dell'interesse degli stati, dei governi e delle agenzie di intelligence con il passare degli anni. In passato, infatti «the government wanted to know what exactly your finger was clicking on»[197], dunque le preferenze commerciali, gli scambi di corrispondenze ovvero i flussi di spostamenti nel mondo. Oggi, invece, «the focus of interest shifts. Now the government wants to know the temperature of your finger and the blood-pressure under its skin»[198].

L'interesse degli stati sarebbe quindi quello di tracciare non più il singolo spostamento, ma monitorare la salute da dietro uno schermo. Tuttavia, sarebbe importante individuare un unico e vero responsabile di ogni forma di controllo e sorveglianze, ma- come asserito da Gabriele Della Morte[199]- in Italia l'unico agente a cui risulterebbe imputabile l'esercizio di una simile attività è l'Autorità Garante per la protezione dei dati personali, che però, al momento non risulta occuparsene se non svolgendo funzioni più garantistiche che sorveglianti.

---

[195] The Vision, *La pandemia ha giustificato nuove forme di sorveglianza di massa. Anche più di quante pensiamo,* (2020).

[196] Yuval Noah Harari: the world after coronavirus, this storm will pass. But the choices we make now could change our lives for years to come, March 20, 2020, Financial Times.

[197] Gabriele Della Morte, *La tempesta perfetta Covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa* in SIDIBlog, (2020)

[198] Yuval Noah Harari: *the world after coronavirus, this storm will pass. But the choices we make now could change our lives for years to come*, March 20, 2020, Financial Times.

[199] Gabriele Della Morte, *La tempesta perfetta Covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa* in SIDIBlog, (2020).

Se soltanto qualcuno-controcorrente al pensiero comune- ha reputato eccessivamente invasivo della propria privacy l'utilizzo degli strumenti digitali riportati *supra*, è pacifico l'eccessivo e lesivo controllo al quale sono stati obbligati- a differenza di altri Paesi- i cittadini cinesi.[200] Ricordiamo che la Cina è stato il primo paese colpito dalla pandemia, e questo ha incrementato le preoccupazioni del governo prima di tutti gli altri. L'evoluzione digitale in Cina ha portato alla creazione di un'app, la *Alipay Health Code*[201].

Il principio alla base del progetto è lo stesso di Immuni, ma a differenza di quest'ultima, l'app cinese-una volta ricevuti i dati dalla registrazione degli utenti- genera un vero e proprio codice basato sugli spostamenti e soprattutto sui contatti avuti[202].

Ogni codice è dotato di un colore, al quale viene associata una diversa gravità: per poter circolare è necessario esibire il proprio QR Code, con il quale si determina il coefficiente di rischio dell'utente. Ciò implica che-ad esempio- nel peggiore dei casi, chi sarà in possesso di un QR code rosso, sarà costretto a restare in casa. Non essendo rimessa alcuna discrezionalità ai cittadini[203], come anticipato, coloro che si oppongono all'assegnazione di un QR code, saranno automaticamente schedati come soggetti a rischio, di colore rosso[204].

In definitiva, ogni evento, sviluppo, progresso od emergenza sono in grado di spianare la strada a nuovi e sempre più invasivi strumenti di *mass surveillance*, e si tratta di decidere quale bene sacrificare.

---

[200] Mozur P., Zhong R., Krolik A., *In Coronavirus Fight*, China Gives Citizens a Color Code, With Red Flags, The New York Times, published March 1, 2020, updated July 26, 2021, da nytimes.com

[201] Tan S., *China's Novel Health Tracker: Green on Public Health, Red on Data Surveillance*, Center for Strategic and International Studies, CSIS, May 4, 2020, da csis.org

[202] Wang J., China: *The QR Code System - a battle between privacy and public interests*?, Lex.Atlas: Covid-19, 6 May 2021, da lexatlas-c19.org

[203] China: Alipay Health Code app shares data with law enforcement, Privacy International, 1st March 2020, da privacyinternational.org

[204] Gabriele Della Morte, *La tempesta perfetta Covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa* in SIDIBlog, (2020)

1.9 L'età dell'oro della sorveglianza: dal capitalismo industriale al capitalismo di sorveglianza

Per capire al meglio la transizione dal capitalismo industriale al capitalismo di sorveglianza, è necessario avere ben chiare la definizione di entrambi. Il capitalismo industriale[205] nasce alla fine del XVIII secolo fino a toccare l'apice della sua crescita con l'avvento della c.d. "rivoluzione industriale", nella seconda metà del XIX secolo. La rivoluzione industriale[206] prende il via dallo *spirito capitalistico*[207] [208]di alcuni soggetti, che -secondo quanto riportato dalla Consob- "realizzano, mediante impiego delle proprie risorse finanziarie […] e/o del credito ottenuto dalle banche , un sistema di produzione "seriale" di merci fondato sul lavoro[…] di altri individui, dietro pagamento di un salario e nell'uso sistematico di macchine (i c.d. fattori produttivi), organizzati in un unico luogo fisico (la fabbrica) secondo un principio di divisione tecnologica delle operazioni produttive e di specializzazione del lavoro."

La Consob è molto puntuale nel segnalare la serialità della produzione, nonché chiave di un'intera rivoluzione fondata, per la prima volta, su rapporti di lavoro subordinato, anelli di una più grande catena. Grazie alla strumentalizzazione di beni e manodopera, la rivoluzione industriale ha portato all'affermarsi di un concetto più ampio e che ha inglobato l'operato di industrie, aziende ed imprese per più di due secoli: il capitalismo industriale. Sempre la Consob definisce così il fenomeno del capitalismo industriale:

"è un sistema di produzione di merci finalizzato allo scambio con profitto legittimo. Il commercio è il presupposto logico del capitalismo; il suo sviluppo abbisogna di un'economia monetaria (e finanziaria) sempre più sofisticata[209]."

---

[205] Il capitalismo industriale, La modernizzazione, DeAgostini, Sapere.it

[206] Pellicani L., *La genesi del capitalismo e le origini della modernità*, Soveria Mannelli (CZ), Rubbettino Editore, 2013 (I Ed., 1988).

[207] Weber M., *L'etica protestante e lo spirito del capitalismo* (Die protestantische Ethik und der Geist des Kapitalismus), 1904-1905

[208] Colli G., *Introduzione a M. Weber, L'etica protestante e lo spirito del capitalismo*, Ed. Rizzoli, 1997.

[209] CONSOB (Commissione Nazionale per le Società e per la Borsa), Autorità Italiana per la vigilanza dei mercati finanziari, *L'età moderna…dalla "nuova" finanza alla rivoluzione industriale.*

Il capitalismo industriale[210], come inteso fino alla fine del XIX secolo, è stato sorpassato da una nuova rivoluzione che ha portato con sé una nuova forma di capitalismo: il capitalismo della sorveglianza[211].

Quest'ultimo integra un duplice concetto che fa riferimento al nuovo capitalismo, inteso come sostituto del precedente industriale e quello di un sistema alla cui base sta il controllo del comportamento dei singoli[212].

Ad occuparsi a fondo di questo fenomeno è stata Shoshanna Zuboff[213], una professoressa di Harvard[214], scrittrice, sociologa, filosofa e ricercatrice, che- con il suo libro *The age of surveillance capitalism: the fight for the future at the new frontier of power*[215]- ha scardinato ogni minimo particolare del marchingegno responsabile di tutto ciò. Il libro, dedicato al futuro, fornisce-ancora prima dell'introduzione- la definizione di capitalismo di sorveglianza, stilando una serie di punti sintetici dell'impostazione madre del sistema:

"*1. Un nuovo ordine economico che sfrutta l'esperienza umana come materia prima per pratiche commerciali segrete di estrazione, previsione e vendita; 2. Una logica economica parassitaria nella quale la produzione di beni e servizi è subordinata a una nuova architettura globale per il cambiamento dei comportamenti; 3. Una mutazione pirata del capitalismo caratterizzata da concentrazioni di ricchezza, conoscenza e potere senza precedenti nella storia dell'umanità; 4. Lo scenario alla base dell'economia di sorveglianza; 5. Un'importante minaccia per la natura umana nel Ventunesimo secolo, proprio come il capitalismo industriale lo era per la natura nei secoli Diciannovesimo e Ventesimo; 6. L'origine di un nuovo potere strumentalizzante che impone il proprio dominio sulla società e sfida la democrazia dei mercati; 7. Un movimento che cerca*

[210] Marx K., Engels F., *Il Capitale* (Das Kapital), 1ª ed. Original 1867, 1885, 1894 1ª ed. Italiana 1886.

[211] Naughton J., *'The goal is to automate us': welcome to the age of surveillance capitalism, in The Observer, 20 January 2019.*

[212] Paolo Pecere, *L'età del capitalismo della sorveglianza* in Il Tascabile, (2020)

[213] Zuboff S., Möllers N. e Wood D., *Surveillance Capitalism: An Interview with Shoshana Zuboff*, in Surveillance & Society, vol. 17, n. 1/2, 31 marzo 2019.

[214] Bridle J., *The Age of Surveillance Capitalism by Shoshana Zub*off review – we are the pawns, in The Guardian, 2 February 2019.

[215] The age of surveillance capitalism: the fight for the future at the new frontier of power, Shoshanna Zuboff, Profile Books (2019); nella versione italiana: Il capitalismo della sorveglianza, Luiss University Press (2019), traduzione a cura di Paolo Bassotti.

di imporre un nuovo ordine collettivo basato sulla sicurezza assoluta; 8. Un'espropriazione dei diritti umani fondamentali che proviene dall'alto: la sovversione della sovranità del popolo[216]."

Alcuni di questi punti sono la chiave per capire la ragione alla base della minaccia prospettata già a partire dalla definizione stessa.

E per comprendere perché viviamo *nell'età dell'oro* del capitalismo della sorveglianza, basta accostare la natura e gli effetti dei due tipi di capitalismo susseguitisi nei secoli. In primis, come sottolineato dal punto 5, ad essere minacciato nell'era del capitalismo industriale era il mondo naturale a cavallo tra il XIX ed il XX secolo, mentre nell'era corrente, il capitalismo della sorveglianza minaccia la natura umana. Tuttavia, come a seguito della rivoluzione industriale non vi era alcuna disciplina legale a tutela del lavoro minorile e dell'ambiente, ad oggi non vi è ancora un quadro normativo ben definito ed in grado di tutelare i singoli dalla minaccia della sorveglianza. Per ultima- ma non per importanza- vi è la distinzione che veniva fatta dai capitalisti industriali tra mercato e persone/società, sconosciuta nel capitalismo della sorveglianza, ove unico fulcro d'interesse sono gli interessi, le attitudini e preferenze dei consumatori, così da poter anticipare le future[217].

In conclusione, in un panorama in cui migliaia di aziende sono disposte a pagare somme insormontabili di denaro ai colossi che detengono ogni tipo di dati personali, non si può asserire altro se non che il capitalismo della sorveglianza abbia toccato l'apice del suo successo distopico[218].

---

[216] Zuboff S., *Il capitalismo della sorveglianza*, Luiss University Press (2019), traduzione a cura di Paolo Bassotti.

[217] Enrico Lobina, *Il 'capitalismo della sorveglianza' agisce sui nostri desideri tramite il web. Altro che libertà* in Il Fatto Quotidiano, (2020).

[218] Lyon D., *La cultura della sorveglianza, come la società del controllo ci ha reso tutti controllori*, introduzione di Gabriele Balbi e Philip Di Salvo, traduzione di Chiara Veltri, Luiss Guido University Press, 2018.

1.10 Conclusione

Da quanto esposto si evince l'assenza di un quadro legislativo idoneo alla protezione degli individui dall'ingerenza del controllo statale, volto a tutelare più il singolo che la collettività. Questa lacuna normativa consente a svariati agenti di approfittarsi della mancata penalizzazione di alcune condotte per porre in essere vere e proprie violazioni della privacy personale. Come si analizzerà nel capitolo che segue, in realtà, gli ultimi anni hanno vissuto uno sviluppo legislativo importante relativo alla protezione e sicurezza dei dati personali che, seppur lacunoso, è stato calorosamente adottato ed ampiamente accolto dalla giurisprudenza.

CAPITOLO SECONDO

IL DIRITTO ALLA PRIVACY

"La privacy non è qualcosa di separato dal rispetto e dalla dignità umana"

Tim Cook

2.1 Premessa

Nel capitolo che segue, si tratterà del diritto alla privacy e della sua crescente e progressiva protezione nell'ambito del diritto internazionale dei diritti umani. In particolare, si approfondirà il suo rapporto con le armi di *mass surveillance* e le eventuali configurazioni di violazioni di diritti umani.

2.2 Il diritto alla privacy: fonti internazionali

Il diritto alla privacy, come si vedrà a breve, trova ormai un ampio riconoscimento nel diritto internazionale, tra strumenti pattizi, regionali e codici interni.

2.2.1 La Dichiarazione Universale dei Diritti Umani

Nel 1947, in un contesto storico particolarmente travagliato, tra la Guerra Fredda e i diversi schieramenti venutisi a creare, le Nazioni Unite istituirono un apposito organismo composto da membri di otto Stati differenti, scelti dal Consiglio economico e sociale dell'ONU: il Comitato per i Diritti Umani[219].

Quest'ultimo si è occupato di stilare trenta articoli tradotti non soltanto nelle cinque lingue ufficiali, ma in quante più lingue possibili. Il documento, seppur non di per sé direttamente vincolante, è stato oggetto di trattati internazionali fondamentali che hanno comportato la vincolatività dello stesso nei confronti degli ordinamenti domestici degli Stati parte delle Nazioni Unite.

I lavori preparatori della Dichiarazione erano già sintomatici della rivoluzione che sarebbe avvenuta sul piano della tutela dei diritti umani: ruolo fondamentale fu rivestito da Eleanor Roosvelt, moglie dell'omonimo presidente degli Stati Uniti, avendo, quest'ultima presieduto lo stesso Comitato di cui sopra ed avendo portato una fondamentale rappresentanza femminile nello scenario istituzionale[220].

Il testo passa in rassegna tutti i diritti umani inalienabili, riconoscendo già nel Preambolo il valore della dignità intesa in termini familiari, costituendo "il fondamento della libertà, della pace e della giustizia nel mondo"[221].

Evidenziando, poi, l'indispensabilità delle relazioni amichevoli tra le Nazioni, configura la Dichiarazione stessa come un'ideale di tutela il cui raggiungimento si auspicava per l'intero orizzonte internazionale. Gli Articoli difendono, per la prima volta, il diritto alla vita, il riconoscimento alla propria personalità giuridica,

[219] Partipilo F., *La Dichiarazione Universale dei Diritti Umani dal 1948 ai nostri giorni*, Osservatoriodiritti, 2018.
[220] Partipilo F., *La Dichiarazione Universale dei Diritti Umani dal 1948 ai nostri giorni*, Osservatoriodiritti, 2018.
[221] Dichiarazione Universale dei Diritti Umani, Assemblea Generale Nazioni Unite, approvata il 10 dicembre 1948

l'uguaglianza dinanzi alla legge, il diritto ad una nazionalità fino a giungere al fulcro di questa tesi: il diritto alla vita privata, nonché quello che ad oggi si considera il diritto alla privacy[222].

Il diritto alla privacy nasce nel 1948 con espresso riconoscimento nella Dichiarazione Universale dei Diritti Umani, approvata dall'Assemblea Generale delle Nazioni Unite il 10 dicembre[223]. All'Articolo 12 della Carta viene così sancito[224]:

"Nessun 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[225]."

La Carta qui riconosce espressamente un diritto negativo, configurandosi - quest'ultimo- come un'astensione dall'interferenza nella vita privata del singolo in modo arbitrario[226].

L'Articolo 12 specifica, poi, dei precisi luoghi in cui la riservatezza dovrebbe essere protetta. Lo Stato, infatti, non dovrebbe limitarsi ad una condotta omissiva, bensì assicurare e tutelare attivamente la privacy del singolo.

In particolare, in famiglia, in casa, nella corrispondenza, l'individuo gode del pieno diritto di essere lasciato da solo, letteralmente "to be left alone[227]."

È lo stesso Comitato delle Nazioni Unite a specificare cosa si debba intendere per *casa*: il luogo in cui il soggetto risiede abitualmente e realizza la sua occupazione.

---

[222] Dichiarazione Universale dei Diritti Umani, Assemblea Generale Nazioni Unite, approvata il 10 dicembre 1948.

[223] Soffientini M., Caccialupi M., *Privacy: protezione e trattamento dei dati*, PSOA Manuali, 2018.

[224]Dichiarazione Universale dei Diritti Umani, Assemblea Generale Nazioni Unite, approvata il 10 dicembre 1948.

[225] Focarelli C., La privacy: proteggere i dati personali oggi, Universale paperbacks, Il mulino, 2015.

[226] Pelino E., Alagna I., Bolognini L., *Codice della disciplina privacy,* Codici commentati Giuffrè, 2019.

[227] Green M., Nørgaard L., Cyril B., Mette b., Birkedal B., *Early Modern Privacy: Sources and Approaches*, MetteIntersections, 2022.

Le Nazioni Unite si sono quindi preoccupate di tutelare il diritto alla privacy nel panorama internazionale, ma tenendo un occhio di riguardo agli ordinamenti interni degli Stati, al fine di assicurare un assorbimento sufficiente del dettato della Dichiarazione[228].

[228] Tosi E., *Codice della privacy: tutela e sicurezza dei dati personali*, I codici vigenti, 2018, Undicesima edizione.

2.2.2 Le fonti regionali del diritto alla privacy

Tra gli strumenti di tutela del diritto alla privacy, ne vengono in rilievo alcuni di rango regionale: tra i meccanismi sovranazionali vi è, ad esempio, la Convenzione Europea dei Diritti dell'Uomo [229], istitutiva della complementare Corte Europea dei Diritti dell'Uomo o CEDU.

Il panorama internazionale del diritto alla privacy è stato, di conseguenza, largamente influenzato dal disposto delle Nazioni Unite, unito all'azione della giurisprudenza della Corte di Lussemburgo[230].

Quest'ultima, anche nota come Corte Europea dei Diritti dell'Uomo, nasce per assicurare la protezione di diritti intesi nella loro concretezza ricorrendo, nel giudizio, a nozioni autonome ed indipendenti da quelle previste dagli ordinamenti domestici. Le decisioni della Corte non hanno, tuttavia, valore di *precedenti*, rimettendo agli Stati un c.d. *margine di apprezzamento* nazionale nella trasposizione del contenuto della Convenzione nella legislazione interna[231].

A comporre la Corte sono chiamati giudici per ogni Membro firmatario della Convenzione Europea dei Diritti dell'Uomo, di cui si parlerà a breve, dunque 47 giudici[232].

All'interno della Corte vi sono ulteriori suddivisioni in cinque sezioni accompagnate da un'Assemblea plenaria, una sesta sezione, chiamata sezione filtro per la mansione di esaminare l'irricevibilità dei ricordi ed infine la Grande Camera, chiamata ad esaminare nei tassativi casi specificati all'Articolo 31 della Convenzione[233].

---

[229] La Convenzione europea sui diritti dell'uomo fu firmata il 4 novembre 1950 a Roma, con 47 stati firmatari ed entrata in vigore il 3 settembre 1953, nelle lingue ufficiali inglese e francese.

[230] Sala M., *Privacy: guida alla lettura del Regolamento (UE) 2016/679 sulla protezione dei dati e del Codice Privacy*, 2018.

[231] Zagrebelsky V., Chenal R., Tomasi L., *Manuale dei diritti fondamentali in Europa*, il Mulino, seconda edizione, 2016.

[232] Zagrebelsky V., Chenal R., Tomasi L., *Manuale dei diritti fondamentali in Europa*, il Mulino, seconda edizione, 2016.

[233] Si tratta dei casi di: rimessione da parte di una Camera, decisione di un collegio di Cinque Giudici su un caso già esaminato da una Camera, decisione del Comitato dei Ministri, richiesta di un parere consultivo da parte del Comitato dei Ministri e in caso di ammissione da parte del Collegio dei Cinque Giudici di un caso già esaminato da un tribunale superiore interno.

Quest'ultima, nata in seno al Consiglio d'Europa nel 1950 e firmata da 47 Stati, ha ereditato i principi internazionali della Dichiarazione Universale dei Diritti Umani, avendo compiuto oramai più di 70 anni[234].

Il testo della Convenzione è diventata la lingua europea, con cui si realizza il dialogo tra le Corti interne, pacificamente auspicato dall'intera Comunità Europea in tema di diritti dell'uomo. Ad oggi, la Convenzione così come modificata dai Protocolli numeri 1,4,6,7,11,12,13,14, è composta da 59 articoli, divisi in 3 Titoli, ed entrata ufficialmente in vigore il 3 settembre 1953.

In particolare, per quanto attiene il diritto alla privacy, la Convenzione, tutela la riservatezza del singolo nel disposto dell'Articolo 8:

"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 stessa Corte ha delimitato il campo d'applicazione dell'Articolo 8, precisando, però, che lo stesso non è illimitato. Così come sancisce la Dichiarazione delle Nazioni Unite, la Convenzione impone un obbligo contestualmente negativo e positivo, implicando che gli Stati debbano astenersi da interferenze arbitrarie nella vita privata del singolo, ed al contempo agire attivamente affinché il diritto precisato non venga leso neppure nelle relazioni interpersonali, dunque nei rapporti tra i privati[235].

La condotta di un'ingerenza da parte delle autorità pubbliche non è, tuttavia, sempre vietata, dal momento che l'ambito d'applicazione del testo normativo resta in parte indefinito, prevedendo alcune eccezioni.

---

[234] Moretti S., *La Convenzione Europea dei Diritti dell'Uomo compie 70 anni*, Questione di Giustizia, 2020.

[235] Dichiarazione Universale dei Diritti Umani, Assemblea Generale Nazioni Unite, approvata il 10 dicembre 1948.

Al secondo paragrafo dell'articolo in questione, si precisano quelle che sono le eccezioni all'obbligo negativo: la previsione di legge, tutela della sicurezza nazionale, della pubblica sicurezza, del benessere economico del paese, difesa dell'ordine e alla prevenzione dei reati, protezione della salute o della morale, o protezione dei diritti e delle libertà altrui.[236].

Ciò significa che questi scenari legittimeranno lo Stato a realizzare una vera e propria ingerenza nella privacy del cittadino, senza che ne venga considerata la lesione.

Va da sé che non basterà il mero manifestarsi di una di queste minacce per legittimare l'interferenza, ma giocherà un ruolo fondamentale la discrezionalità di ogni singolo Stato, che valuterà di volta in volta l'essenzialità dei valori fondamentali in gioco, effettuando un analitico bilanciamento tra gli interessi in gioco[237] [238].

Ci si è interrogati circa l'effettiva necessità dell'ingerenza statale in una società democratica, avendo la Corte sottolineato—tra le tante questioni irrisolte—l'assenza precisamente voluta dal legislatore di parole "ragionevole" ovvero "auspicabile", nell'interpretazione dell'Articolo 8.

È lo stesso orientamento consolidato dalla Corte [239]nella pronuncia *Dudgeon c. Regno Unito*[240] [241]del 1981, nella quale si escludeva la necessarietà dell'interferenza statale in una società che poggia le basi sui principi della liberalità e della tolleranza.

---

236 *Privacy e data protection*, IPSOA InPratica, 2021.

237 Stoddart J., Chan B., Joly Y., *The European Union's Adequacy Approach to Privacy and International Data Sharing* edited by Rothstein M., A; Knoppers B.M., The Journal of law, medicine & ethics, 03/2016, Volume 44, Fascicolo 1.

238 *International data privacy law*, International data privacy law, 2011

239 Sala stampa: "Negli anni 1970, vi era un clima di grande ostilità": nuovi video per celebrare 40 anni di progressi per i diritti delle persone LGBTI, Consiglio d'Europa Strasburgo, 22 ottobre 2021.

240 European Court of Human Rights, Court (PLENARY) Case of *dudgeon v. the united kingdom (Application no. 7525/76)* Judgment Strasbourg, 22 October 1981.

241 Dudgeon v United Kingdom, Merits, Just Satisfaction, App No 7525/76, 1982. 4 EHRR 149, IHRL 31 (ECHR 1981), 22nd October 1981, European Court of Human Rights, *Whether and to what extent the right to respect for private life extends to cover homosexual acts.*

Tra le prime mosse nel panorama internazionali, in relazione alla diffusione della tutela del diritto alla privacy, a seguito della Dichiarazione Universale dei Diritti dell'Uomo delle Nazioni Unite e della Convenzione Europea dei Diritti dell'Uomo, la Svizzera fu la prima a promulgare una legge in materia, il c.d. *Data Act* del 1973. [242]Sette anni dopo, l'*Organization for Economic Cooperation and Development* (OECD), elaborò le prime line guida per la protezione e circolazione dei dati personali. [243]

[242] Kenyon A., Richardson M., *New Dimensions in Privacy Law: International and Comparative Law*, edited by Kenyon, Andrew T; Richardson M., 2006.
[243] Kenyon A., Richardson M., *New Dimensions in Privacy Law: International and Comparative Law*, edited by Kenyon, Andrew T; Richardson M., 2006.

2.2.3 Altri strumenti di protezione della privacy

Tra gli altri strumenti di tutela della privacy nel panorama internazionale, ve ne sono alcuni che—seppur di rango regionale—hanno dimostrato di avere una potenziale influenza sugli ordinamenti legislativi di altri Stati.

Si veda, ad esempio il Decreto Legislativo n. 196/2003, nonché il Codice della Privacy[244], il quale si occupa di tutela del trattamento delle società dei servizi dell'informazione offerti ai minori di età, il trattamento dei dati utilizzati nel settore pubblico ovvero il sistema sanzionatorio sia sul versante penale che amministrativo[245].

A livello statale, nell'ordinamento italiano, sono stati integrati dalla legislazione comunitaria, numerosi codici di condotta, che racchiudono delle vere e proprie regole deontologiche, facendo espresso riferimento ad obblighi legali in relazione al trattamento di specifiche situazioni: l'ambito del lavoro, gli obblighi di segretezza, l'identificazione delle persone fisiche, ecc.

Un esempio significativo è sicuramente il Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica[246]; nient'altro che il Provvedimento emanato dal Garante il 29 luglio 1988[247].

[244] Venkataramanan N., *Data privacy: principles and practice*, 2017.

[245] Bolognini L., Pelino E., *Codice privacy: tutte le novità del d.lgs. 101/2018: in vigore dal 19 settembre 2018*, Civilista, Milan, Italy, 2018.

[246] *Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica*, Garante per la privacy.

[247] Con il Decreto del Ministro della Giustizia del 31 gennaio 2019, pubblicato nella Gazzetta Ufficiale n. 35 dell'11 febbraio 2019, le presenti Regole deontologiche sono state riportate nell'allegato A del decreto legislativo 30 giugno 2003, n. 196 in sostituzione del corrispondente Codice di deontologia.

2.3 International Covenant on Civil and Political Rights

Nell'iter che coinvolse il diritto internazionale nella protezione della vita privata e della privacy del singolo, una svolta importante venne segnata dall'International *Covenant on Civil and Political Rights* o *Patto Internazionale sui Diritti Civili e Politici*[248].

Il Patto Internazionale sui Diritti Civili e Politici fu firmato dall'Assemblea Generale delle Nazioni Unite il 16 dicembre 1966 a New York ed entrò in vigore il 23 marzo 1976. Con questo strumento, il diritto internazionale si interessò di tutelare i diritti che rischiavano di essere privi di protezione, segnando la svolta da un quadro giuridico letteralmente "non-binding" dettato dalla Dichiarazione Universale sui Diritti Umani del 1948 ad una vincolatività assicurata da obblighi immediatamente esecutivi per tutti gli Stati parte e creando un quadro di riferimento per gli standard universali dei diritti civili e politici[249].

L'origine di questo tipo di diritti va ricercata nelle teorie filosofiche già consolidate nella seconda metà del Seicento, con la corrente di John Locke[250], che introdusse il concetto di "Stato di natura", derivandone la nascita dei cosiddetti *diritti naturali*, quali il diritto alla vita, alla proprietà e alla libertà, poi ripresi da Rousseau, Montesquieu e Voltaire. Questi filoni di pensiero influenzarono sempre più quello che stava diventando il nuovo habitat dei diritti umani quasi globalmente: seguirono la Dichiarazione d'Indipendenza Statunitense del 1776, la Dichiarazione Francese dei Diritti dell'Uomo e del Cittadino del 1789, l'US Bill of Rights, fino a giungere allo strumento di protezione dei diritti umani per eccellenza, la Dichiarazione Universale dei Diritti Umani[251].

---

[248] La Convenzione internazionale sui diritti civili e politici è un trattato delle Nazioni Unite nato dall'esperienza della Dichiarazione Universale dei Diritti dell'Uomo, adottato nel 1966 ed entrato in vigore il 23 marzo del 1976.

[249] Taylor P., *A Commentary on the International Covenant on Civil and Political Rights*, The UN Human Rights Committee's Monitoring of ICCPR Rights, Cambridge University Press, 2020.

[250] Bertolone L., *Lo stato di natura: il mondo preopolitico per Hobbes e Locke*, Treccani, 2020.

[251] Joseph S., Castan M., *The International Covenantg on Civil and Political Rights: Cases, Materials and Commentary*, Oxford Public International Law, 2013.

Lo stesso Patto sui Diritti Civili e Politici istituì un organismo di controllo circa l'effettiva esecutività degli obblighi nelle giurisdizioni domestiche: il Comitato dei Diritti Umani. Quest'ultimo si preoccupa di rintracciare elementi sintomatici di violazioni di diritti umani, nonostante fosse stato inizialmente osteggiato dalle dinamiche della Guerra Fredda, stilando delle Osservazioni Generali che progressivamente incrementarono la loro importanza nel panorama domestico. Il contenuto di questi Commenti confluì nel bacino di spiegazioni circa le disposizioni del Patto stesso circoscrivendo molto più dettagliatamente l'ambito di applicazione degli Articoli. Con ulteriori osservazioni, prese posizione in merito, ad esempio, al diritto alla vita e palesando il proprio dissenso nei confronti della pena di morte ancora presente in alcuni ordinamenti statali penali[252].

Al Patto venne successivamente aggiunto un *Protocollo Facoltativo sul Patto Internazionale sui diritti civili e politici,* che si proponeva di implementare il successo della tutela prefissata, "abilitando" il Comitato de Diritti dell'Uomo, istituito dalla Parte Quarta dell'Accordo, ad esaminare le denunce di violazioni provenienti dai privati di alcuno dei diritti e secondo le modalità previste dal Protocollo[253].

[252] Harris D., Professor Emeritus and Co-Director Human Rights Law Centre, School of Law, University of Nottingham.

[253] Protocolo Facultativo ao Pacto Internacional sobre os Direitos Civis e Politicos, dhnet.org.

2.3.1 Articolo 17, International Covenant on Civil and Political Rights:

L'Articolo 17 recita: "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."
Sempre le Nazioni Unite, a distanza di diciotto anni dalla sopracitata Dichiarazione, con il Covenant implementarono l'intenzione, ormai ampiamente affermata di voler assicurare sempre maggior tutela al diritto *di essere lasciato da solo* del singolo, ribadendo l'illegittimità delle interferenze arbitrarie e rimarcando l'obbligo complementarmente positivo e negativo che grava sugli Stati.
L'attenzione rivolta a questo diritto, a distanza di quasi due decenni, si spiega con la volontà dell'ONU di incrementare i controlli esercitabili sulle decisioni dei governi, facendo sì che un numero sempre crescente di Paesi firmassero il Patto ONU II. Tra i firmatari rientravano, infatti, nazioni che non si erano mostrate—fino a quel momento— particolarmente sensibili alla tutela di diritti simili a quelli contenuti nel Patto. Questo spinse l'ONU ad istituire dei meccanismi internazionali di controllo, tra i quali spicca il Comitato per i diritti dell'uomo, disposto dall'Articolo 28 dello stesso Patto. [254]

[254] *Human Rights Instruments,* Core Instrument, United Nations Human Rights, Office of High Commissioner.

2.3.2 Articolo 19 International Covenant on Civil and Political Rights

Apparentemente distaccato dal disposto del precedente articolo, l'Articolo 19 si occupa e preoccupa di proteggere la libertà di espressione, non meramente intesa come all'Articolo 21 della Nostra Carta.

L'articolo così sancisce:

"1. Ogni individuo ha diritto a non essere molestato per le proprie opinioni.

2. Ogni individuo ha il diritto alla libertà di espressione; tale diritto comprende la libertà di cercare, ricevere e diffondere informazioni e idee di ogni genere, senza riguardo a frontiere, oralmente, per iscritto, attraverso la stampa, in forma artistica o attraverso qualsiasi altro mezzo di sua scelta[255]."

Già in questi due primi paragrafi, le Nazioni Unite hanno inteso tutelare la possibilità rimessa ad ogni individuo di condividere, anche pubblicamente, le loro idee, orientamenti ovvero, anche implicitamente, dati personali. Il vero e proprio obbligo gravante sullo Stato, simmetrico al diritto, è precisato al terzo paragrafo:

"3. L'esercizio delle libertà previste al paragrafo 2 del presente articolo comporta doveri e responsabilità speciali.

Esso può essere pertanto sottoposto a talune restrizioni che però devono essere espressamente stabilite dalla legge ed essere necessarie:

a) al rispetto dei diritti o della reputazione altrui;

b) alla salvaguardia della sicurezza nazionale, dell'ordine pubblico, della sanità o della morale pubbliche[256]".

Ancora una volta, viene evidenziata la necessità della riserva di legge, del principio di legalità e la sensibilità alla tutela dei diritti umani[257].

---

[255] *Human Rights Instruments*, Core Instrument, United Nations Human Rights, Office of High Commissioner.

[256] *Human Rights Instruments*, Core Instrument, United Nations Human Rights, Office of High Commissioner.

[257] Michael O'Flaherty, *Freedom of Expression: Article 19 of the International Covenant on Civil and Political Rights and the Human Rights Committee's,* General Comment No 34**,** *Human Rights Law Review*, Volume 12, Issue 4, December 2012, Pages 627–654, Published: 12 December 2012.

2.4 Quadro giuridico internazionale: il contrastante parallelismo tra regolamentazione UE/USA

Tra le legislazioni fondamentali relative alla tutela dei dati personali, spiccano senz'altro quelle europee e statunitensi: questo perché è proprio nei rispettivi territori Statali che si consuma il traffido di dati personali più ingente a livello mondiale, con particolare riferimento alla circolazione di dati e libera trasmissione e scambi tra le agenzie di intelligence dei governi più potenti al mondo. Basti pensare all'alleanza dei *Five Eyes*[258] , di cardinale importanza nel caso Snowden, di cui a breve si tratterà, ovvero dell'ESISC[259], agenzia d'intelligence europea addetta ai reports dei dati geopolitici, economici e relativi alla sicurezza pubblica dell'intera Comunità.

[258] Si tratta di un'alleanza fra Stati Uniti, Canada, Regno Unito, Australia e Nuova Zelanda con cui i governi stipulano un accordo per il reciproco scambio di informazioni e dati coperti da segreti di stato.
[259] ESISC: European Strategic Intelligence and Security Center.

2.4.1 La legislazione statunitense in merito alla protezione dei dati personali

Il quadro normativo disposto dagli Stati Uniti d'America vanta tanti punti di congruenza con la legislazione Europea, quanti elementi che stridono parecchio in tema di tutela dei dati personali.

Nel panorama statunitense, un ruolo decisivo per lo sviluppo del diritto alla privacy, fu giocato dall'operato dei giudici, dunque dalla giurisprudenza[260].

In diverse sentenze, venne fornita un'interpretazione evolutiva del *Bill of Rights*, rintracciando le radici di quello che sarebbe diventato un vero e proprio diritto di protezione dei dati personali.

Negli Stati Uniti, tuttavia, il riconoscimento di un diritto alla privacy visse un percorso perlopiù travagliato, tenendo conto che soltanto negli anni Sessanta del 1900, la Corte Suprema configurò per la prima volta la privacy del singolo come oggetto sensibile di tutela da parte della legislazione statunitense.[261].

Fu così, che nel 1974 si giunse all'emanazione della prima legge in materia, con il Privacy Act[262]: un codice di pratiche per garantire la giusta informazione circa la raccolta, archivio e diffusione dei dati personali degli individui, custoditi dalle agenzie federali.

Nonostante queste iniziative, è pacifico che, ancora oggi, la legislazione statunitense si interessi della tutela e protezione dei dati personali del singolo inteso in qualità di *consumatore*, dunque in relazione al mero esercizio di attività economica.

---

260 *Perspectives on Privacy: Increasing Regulation in the USA, Canada, Australia and European Countries*, 2015, edited by Dieter D., Russell L., Weaver Perspectives on Privacy: Increasing Regulation in the USA, online information review, 06/2015, Volume 39, Fascicolo 3.

261 Asunción E., *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA*, International data privacy law, 02/2017, Volume 7, Fascicolo 1.

262 The United States, Department of Justice: Privacy Act of 1974, Overview of the privacy Act, Updated on April 30, 2021.

Per tale ragione, l'autorità adibita alla gestione dei dati è la *Federal Trade Commission*[263], responsabile del controllo sulle aziende e la correttezza delle loro pratiche con i consumatori.

La scarsa attenzione del governo statunitense circa la protezione dei dati personali, è da ricercare nel più marcata interesse da parte dello stesso alla protezione della sicurezza ed ordine pubblico, il che fonda la ratio delle proprie radici nell'attentato dell'11 settembre del 2001 delle Torri Gemelle. Questa politica ha portato alla formazione di un quadro regolamentare improntato sull'assunto del "più sicurezza, meno privacy"[264], posizionando in cima alla scala delle priorità, la sicurezza pubblica, inevitabilmente implicando ingerenze nella vita privata degli individui[265]. È proprio il bilanciamento tra il diritto non fondamentale del singolo ed i diritti rimessi agli agenti imprenditori, la principale e sostanziale differenza tra la regolamentazione europea e quella statunitense.

[263] Federal Trade Commission, usa.gov.,: The Federal Trade Commission works to prevent fraudulent, deceptive, and unfair business practices. They also provide information to help consumers spot, stop, and avoid scams and fraud.

[264] Kuntze J.,*The Abolishment of the Right to Privacy?: The USA, Mass Surveillance and the Spiral Model***,** 2018.

[265] Saetta B., Privacy negli Usa, Normativa, 7 Settembre 2016 Ultima modifica:4 Giugno 2021, protezionedatipersonali.it

2.4.2 La legislazione comunitaria in merito alla protezione dei dati personali

Il quadro legislativo europeo vanta un iter ben differente, ma non per questo più efficiente, fondando le proprie radici nel vuoto normativo che perdurò fino agli anni Settanta.

Spinta dal contenuto della CEDU, l'Unione Europea segnò una svolta con la Carta di Nizza del 2000[266], alla quale si giunse grazie al Trattato di Mastricht[267] di sette anni prima.

Tuttavia, lo strumento regionale configurabile come il prologo di questo progresso normativo, è senz'altro la *Data Protecion Directive* ovvero 'Direttiva madre', nonchè la Direttiva 95/46/CE. [268]

Con l'emanazione della Direttiva, l'Unione ha effettuato, per la prima volta, un bilanciamento d'interessi sul piano sovranazionale, regolamentando una disciplina che assicurasse un equilibrio tra la privatezza dei singoli ed il diritto dei Paesi membri al libero scambio di dati, anche personali. [269]

La soluzione a questa bilancia d'interessi fu standardizzare la protezione dei dati personali, fissando appunto uno standard a cui gli Stati Membri avrebbero dovuto conformarsi.

Gli ordinamenti interni di questi ultimi, tuttavia, testimoniano la fallacia della Direttiva nel voler perseguire questo scopo, evidenziando come l'omogeneità

[266] La Carta dei diritti fondamentali dell'Unione europea (CDFUE), in Italia anche nota come Carta di Nizza, è stata solennemente proclamata una prima volta il 7 dicembre 2000 a Nizza e una seconda volta, in una versione adattata, il 12 dicembre 2007 a Strasburgo da Parlamento, Consiglio e Commissione Europei.

[267] Il Trattato di Maastricht, o Trattato sull'Unione europea (TUE), è stato firmato il 7 febbraio 1992 a Maastricht, dai 12 Membri della Comunità europea, oggi Unione europea, ed entrato in vigore l'1 novembre 1993, che definisce i cosiddetti tre pilastri dell'Unione europea, fissando anche le regole politiche e i parametri economici e sociali necessari per l'ingresso dei vari Stati aderenti nella suddetta Unione (*parametri di convergenza di Maastricht*).

[268] Direttiva 95/46/CE: èstata adottata il 24 ottobre 1995, con lo specifico scopo di armonizzare le norme in materia di protezione dei dati personali per garantire un "flusso libero" (free flow of data) dei dati e promuovere un elevato livello di tutela dei diritti fondamentali dei cittadini.

[269] Tosi E., Soro A., Franceschelli V., *Privacy digitale: riservatezza e protezione dei dati personali tra GDPR e nuovo Codice privacy*, DNT Milano, Italy, 2019.

legislativa auspicata venne ostacolata dalle norme palesemente contrastanti dei singoli Membri[270].

A coronare la funzionalità della Direttiva, venne creata, per la prima volta, un'autorità di controllo del rispetto della legislazione in materia di protezione dei dati personali: il Garante per la privacy[271]. Quest'ultima figura—ancora esistente—era ed è dotata di importanti poteri investigativi ovvero inquisitori e a questa è rimessa la possibilità di promuovere azioni giudiziarie e, se dal caso, emettere sanzioni in caso di violazioni[272].

La Carta permise di declinare l'attenzione della legislazione europea dal singolo in qualità di consumatore al singolo e la tutela di un suo diritto—per la prima volta—ritenuto fondamentale.

Si assiste, dunque, ad una scissione tra il concetto di vita privata e quello della protezione dei dati personali: il fulcro della differenza va rintracciato nell'assunto secondo il quale per la vita privata si fa riferimento ad un mero potere di escludere l'ingerenza delle autorità statali; per quanto attiene la protezione dei dati, invece, si parla di veri e propri poteri di intervento.

270 Pelino E., Alagna I., Bolognini L., *Codice della disciplina privacy*, Codici commentati Giuffrè, 2019.

271 Riccio G., Scorza P., Belisario E., *GDPR e normativa privacy: commentario*, Commentari (IPSOA, S.p.a.), 2018.

272 Iaselli M., *Sanzioni e responsabilità in ambito GDPR*, Compliance, 2019.

2.5 Il regolamento GDPR e la protezione dei dati personali

Il Regolamento del Parlamento Europeo del 27 aprile 2016 n.2016/679/UE[273] relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati o General Data Protection Regulation (GDPR) è entrato in vigore il 24 maggio 2016 e si applica dal 25 maggio del 2018.

Con l'entrata in vigore del Regolamento, è stata contestualmente abrogata la vecchia Direttiva UE 95/46/CE e tutte le leggi relative alla tutela della privacy emanate dagli Stati Membri[274].

La finalità del regolamento è duplice: la protezione delle persone fisiche in relazione al trattamento dei dati personali e la libera circolazione degli stessi. Tutto ciò mira ad un complessivo rafforzamento dell'uniformità della disciplina europea in materia; [275]uniformità voluta ed auspicata constatando la disomogeneità dei quadri normativi interni nel panorama europeo.

A tal proposito, il C7 del Regolamento[276] dispone che l'attuale—ai tempi—contesto sociale "*richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione*". Queste ultime si rendono necessarie tenendo conto della conseguenza della mancata certezza del diritto e mancata fiducia dei cittadini nei confronti delle autorità che dovrebbero –o avrebbero dovuto— fare da garanti alla loro protezione di dati, strettamente collegata alla lacuna legislativa in materia di privacy[277].

La necessità di un'omogeneità nel quadro europeo, tuttavia, non ha implicato un'assenza di margine di discrezionalità e manovra dei Membri.

---

[273] Denley, A., Foulsham M., Hitchen B., *GDPR: how to achieve and maintain compliance*, 2019.

[274] Krzysztofek M., GDPR: Post-Reform Personal Data Protection in the European Union, 2018.
EU GDPR: A Pocket Guide, second edition di Calder A., 2018, 2nd edition.

[275] Applicare il GDPR, Linee Guida europee, Garante per la Protezione dei Dati Personali, ottobre 2019.

[276] Gawronski M., Guide to the GDPR, 2019.

[277] Zorzi Galgano N., *Persona e mercato dei dati: riflessioni sul GDPR,* Le monografie di Contratto e impresa, serie diretta da Francesco Galgano, 2019.

A questi ultimi, in particolare, è rimessa la possibilità di gestire e regolamentare particolari tipi di dati, dalla natura più delicata (i c.d. *dati sensibili*)[278].

In particolare, in Italia, il GDPR ha abrogato gli articoli del Codice per la protezione dei dati personali del Decreto Legislativo 196/2003[279]: vi è una simmetria tra il contenuto dei due disposti legislativi già evidente all'Articolo 1[280] della disciplina statale. Quest'ultimo così dispone:

"Chiunque ha diritto alla protezione dei dati personali che lo riguardano."

Non è nient'altro che una delle due finalità che si propone il Regolamento Europeo, evidenziando il vuoto normativo relativo alla circolazione dei dati collezionati. L'asimmetria, al contrario, consiste nel bene oggetto di tutela che, nel panorama italiano, era il mero rispetto del diritto alla vita privata, appositamente evitando di trattare come oggetto di tutela la privacy nella sua interezza[281].

Il C1 del GDPR, statuisce coerentemente che in Europa "la protezione delle persone fisiche, con riguardo al trattamento dei dati di carattere personale, è un diritto fondamentale". Precisa, poi, al C2 che a tale scopo è consigliabile la "realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica[282]".

L'ambito di applicazione del GDPR è immediatamente specificato nel C1 dell'Articolo 2, identificando come raggio d'azione del testo, il trattamento di dati

---

[278] Bygrave L.A., Docksey C., Kuner C., *The EU General Data Protection Regulation (GDPR): a commentary*, 2020.

[279] Tosi E., Soro A., Franceschelli V., Buttarelli G., Battelli E., *Privacy digitale: riservatezza e protezione dei dati personali tra GDPR e nuovo Codice privacy*, 2019.

[280] Decreto Legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali *(, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)*. Entrata in vigore del decreto: 1-1-2004, ad eccezione delle disposizioni di cui agli artt. 156, 176, commi 3, 4 ,5 e 6, e 182 che entrano in vigore il 30/7/2003; dalla medesima data si osservano altresì i termini in materia di ricorsi di cui agli artt. 149, comma 8, e 150, comma 2.

[281] Jackson C., Ayshe Namid J., *Piano di Adeguamento al Regolamento Generale Sulla Protezione dei Dati (GDPR): Guida aziendale per lavorare in conformità con i requisiti del GDPR*, 2020.

[282] Calder A., EU GDPR – An international guide to compliance, 2020.

personali che siano totalmente o parzialmente automatizzati o, per nulla automatizzati purché contenuti in un archivio o destinati a figurarvi[283].

Quest'ultima precisazione, come disposto dal C15, nasce dall'accortezza del legislatore europeo di non lasciare scoperto quel bacino di dati personali che— non essendo strettamente collegati al profilo tecnologico— potrebbe essere facilmente eluso ed escluso dalla protezione garantita dal Regolamento: si parla, a questo proposito, di neutralità tecnologica.

A quest'ultima è opponibile una ed una sola eccezione, già rintracciata nello stesso C15, relativa alla natura materiale dei dati, che necessitano di un archivio ad essi ricollegabile, in mancanza del quale verrebbe meno qualsiasi protezione europea.[284]

È per questo che diventa fondamentale circoscrivere chirurgicamente la nozione di archivio, contenuta nell'art. 6 n.4 del Regolamento, il quale—non distaccandosi dal disposto della Direttiva 95/46/CE— precisa che per archivio debba intendersi "qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico[285]".

La circoscrizione dell'ambito di applicazione implica, indirettamente, che vi saranno dei trattamenti esclusi dalla protezione del Regolamento; sono due le categorie che ne restano estranee: la prima è costituita dai trattamenti svolti nell'ambito di attività estranee all'ambito di applicazione del diritto dell'Unione e dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del Titolo V, Capitolo 2, TUE[286].

Il problema relativo all'individuazione delle materie non oggetto d'applicazione del diritto comunitario, nasce dall'assunto—pacifico, ma non particolarmente definito e specificato— secondo cui le materie di competenza dell'Unione sono espressamente sancite dai Trattati. In materia di privacy, l'unico riferimento

---

283 Tamburri D., *Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation*, An Information systems (Oxford), 07/2020, Volume 91.

284 Panetta A., Iannini A., Alpa G., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato: commentario al Regolamento UE n. 2016/679*, 2019.

285 Riccio G., Scorza P., Belisario E., *GDPR e normativa privacy: commentario*, Commentari (IPSOA, S.p.a.), 2018.

286 Martorana M., Barberisi A., Pizzetti F., GDPR e Decreto Legislativo 101/2018, 2019.

contenuto nel diritto pattizio è rintracciabile solo all'Articolo 16 del Trattato sul Funzionamento dell'Unione Europea,[287] il quale tratta la materia della privacy in relazione agli organi competenti ad occuparsene.

In particolare, vi è una controversia in merito alla competenza a normare tra Parlamento e Consiglio, ma solo ed esclusivamente per i dati personali svolti dai soggetti pubblici, estromettendo la categoria di dai trattati da soggetti diversi da quelli nominati espressamente nell'articolo[288].

La seconda categoria di dati che vengono esclusi è ben più semplice da circoscrivere con precisione: si tratta di dati relativi ad attività che rientrano nell'ambito delle relazioni internazionali dei singoli Paesi e della sicurezza pubblica non espressamente rimesse ad organi comunitari[289].

Il Regolamento si occupa della protezione dei dati personali: è necessario, in questa sede, elencare la classificazione dei diversi tipi di dati, derivandone una minore o maggiore protezione.

Innanzitutto, i dati personali sono soggetti ad una flessibile nozione, flessibilità fortemente voluta dal Parlamento Europeo, finalizzata a consentire un ampio margine di discrezionalità agli Stati nell'importare il GDPR negli ordinamenti interni[290].

Dunque, si ha una definizione dettata da ampia generalità: l'Articolo 4 del Regolamento precisa che si intende per dati personali "qualsiasi informazione che riguarda una persona fisica identificata o identificabile[291]".

Ad accompagnare i generali dati personali, vi sono speciali categorie di dati, particolarmente bisognose di protezione, indicati dallo stesso Articolo 4 del

---

[287] Gazzetta ufficiale dell'Unione europea C 326/47, Trattato sul Funzionamento dell'Unione Europea, versione consolidata, 20.10.2012.

[288] Nascimbene B., Unione europea: trattati, L'Europa in movimento, 2017, Quarta edizione.

[289] Pocar F., Baruffi M.C., Commentario breve ai trattati dell'Unione Europea, Breviaria juris, 2014, 2. ed.

[290] Panetta A., Iannini A., Alpa G., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato: commentario al Regolamento UE n. 2016/679*, 2019.

[291] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione 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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

Regolamento, rispettivamente ai numeri 13, 14 e 15:[292] i dati genetici[293], risultanti dall'analisi di un campione biologico di una persona che consente di risalire all'identità di quest'ultima; i dati biometrici, capaci di identificare una persona attraverso gli strumenti di riconoscimento facciale, analizzando i tratti somatici; infine, i dati sanitari ovvero dati relativi alla salute di un individuo[294], relativi alle condizioni di salute, siano esse fisiche o psichiche, di quest'ultimo[295].

I principi da rispettare nel Regolamento sono stati espressamente previsti per consentire una gestione consapevole dei dati, garantendo al contempo la sicurezza e la trasparenza nel fornire il consenso da parte dell'interessato. Ciò implica che a governare la protezione dei dati personali nell'Unione Europea vi saranno i principi sanciti dall'Articolo 5 del Regolamento[296].

Il primo e più importante fra i principi è quello di liceità[297]: questo va letto congiuntamente al principio di legalità, nell'ottica di una funziona strettamente garantista, disponendo le condizioni in presenza delle quali si può esigere una limitazione ovvero un consenso dei dati personali.

Si parla, dunque di liceità del trattamento dei dati personali, allorquando sussista— anche non cumulativamente— una delle seguenti condizioni, come disposto dall'Articolo 6[298]:

---

[292] Kirwan M., Mee B.,Clarke N., Tanaka A., Manaloto L., Halpin E.,Gibbons U., Cullen,A., McGarrigle S., Connolly E.B., Bennett K., Gaffney E., Flanagan C., Tier L., Flavin R., McElvaney N.G., *What GDPR and the Health Research Regulations (HRRs) mean for Ireland: a research perspective*, Irish journal of medical science, 7/2020, Volume 190, Fascicolo 2.

[293] *GDPR and Biobanking*, edited by Slokenberga S., Tzortzatou O., Reichel J., Law, Governance and Technology Series, 2021.

[294] Bradford L., Aboy M., Liddell K., *COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes*, *Journal of Law and the Biosciences*, Volume 7, Issue 1, January-June 2020, published: 28 May 2020.

[295]Carro G., Masato S., Parla M.D., *La privacy nella sanità*, Teoria e pratica del diritto, 2018.

[296] Krzysztofek M., *GDPR: General Data Protection Regulation (EU) 2016/679Post-Reform Personal Data Protection Regulation EU 2016/679*, 2018.

[297] Laybats C., Davies J., *GDPR: Implementing the regulations*, Business information review, 06/2018, Volume 35, Fascicolo 2.

[298] *EU General Data Protection Regulation (GDPR): An Implementation and compliance guide*, fourth edition, di Team, IT Governance Privacy, 2020.

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore [299].
Altro principio sancito dall'Articolo 5 è il principio di correttezza: il rispetto di quest'ultimo è finalizzato a regolare le modalità con cui i dati raccolti devono essere trattati.
Il terzo principio è quello della trasparenza, complementare al principio di correttezza, facendo riferimento alla tutela dell'interessato al momento della prestazione del consenso, in modo tale che quest'ultimo sia fornito con cognizione di causa, conscio delle finalità per cui verranno utilizzati i propri dati, da chi vengono collezionati, dove vengono archiviati e soprattutto, quali sono le condizioni in presenza delle quali il consenso può essere revocato.
Al secondo comma, l'Articolo 5 fissa la c.d. limitazione delle finalità: la raccolta, trattamento e circolazione dei dati personali deve avvenire per raggiungere scopi

[299] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione 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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

determinati, espliciti e legittimi, con la sola esplicita eccezione relativa all'ipotesi di trattamento dei dati successivamente archiviati per pubblico interesse, ricerca scientifica o storica o ancora a fini statistici.

A seguire, vi è il principio di minimizzazione dei dati, secondo cui questi ultimi devono essere utilizzati in modo adeguato, pertinente e limitato a quanto necessario. In ordine, il principio di esattezza, la limitazione della conservazione, il principio di integrità e riservatezza, che rispettivamente prevedono la fedeltà e completezza delle condizioni e finalità del trattamento dei dati, un limite temporale che non consente l'identificazione di un soggetto per un periodo superiore a quello necessario, la prevenzione del danneggiamento, perdita e distruzione dei dati, anche accidentalmente; infine, la riservatezza comporta che i dati raccolti grazie al consenso non possono essere trasmessi per altri scopi a terzi senza previa autorizzazione dell'interessato, dovendo restare nello stretto dominio di chi li ha raccolti.

Per quanto attiene la sfera dell'esercizio dei diritti dell'interessato, a quest'ultimo deve essere assicurata la trasparenza delle informazioni, comunicazioni e modalità per l'esercizio del relativo diritto.

In particolare, il dovere di trasparenza assume una configurazione fondamentale se lo si considera strettamente collegato alla sua incisività sull'esercizio di controllo dei propri dati personali da parte dell'interessato. La stessa trasparenza, principio ormai consolidato dalla giurisprudenza comunitaria, non permette al titolare di sottrarsi incondizionatamente alle richieste dell'interessato, a meno che non sia accertato che egli è impossibilitato a provarne l'identità.

L'interessato gode del diritto di ricevere le informazioni e le comunicazioni circa il trattamento e la circolazione dei suoi dati personali, a titolo gratuito ed in ogni momento è necessario che l'interessato presti il proprio consenso, a nulla valendo la manifestazione di un consenso non pieno ed espresso.

Il Regolamento Europeo prevede, inoltre, l'istituzione di un organo di controllo ad hoc nel panorama comunitario: l'Autorità Garante per la privacy, alla quale è espressamente rimesso il potere ispettivo, che si espleta attraverso una mappatura dei singoli trattamenti, la conoscenza di aspetti organizzativi degli enti che trattano i dati, l'accertamento della correttezza dei rapporti con gli interessati, l'esame delle

svariate politiche di sicurezza informatiche e l'individuazione di un organigramma privacy. Allo stesso organo è poi rimesso il potere di avviare un procedimento sanzionatorio, all'esito del quale può applicare sanzioni amministrative o pecuniarie.

2.5.1 I provvedimenti del legislatore europeo: il testo approvato dal Parlamento Europeo sulla proposta di deroga temporanea della

Direttiva UE 2002/58/EC allo scopo di contrastare il fenomeno di abusi sessuali sui minori online

Il Parlamento Europeo ha recentemente approvato un testo relativo alla proposta di deroga della Direttiva 2002/58/CE [300]-o *Chatcontrol*- dello stesso in concerto con il Consiglio del 12 luglio 2002 per il trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche, attuando gli Articoli 7 e 8 della Carta Europea dei Diritti Umani[301]. Ed in particolare, la deroga si riferisce al disposto dell'Articolo 5 primo comma e Articolo 6 primo comma della Direttiva *eprivacy*[302].

La proposta di proroga della sospensione della Direttiva[303] anche detta e-privacy, nasce allo scopo di contrastare l'abuso sessuale di minori e la pornografia minorile online, attraverso un controllo radicato dei servizi di comunicazione, telefonia ed Internet.[304] Tenendo conto della particolare gravità dei reati in questione, l'Unione si è preoccupata di intensificare i meccanismi di controllo che gravano sui servitori di servizi[305].

---

[300] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)**,** *Gazzetta Ufficiale n. L 201 del 31/07/2002.*

[301] La Convenzione europea sui diritti dell'uomo fu firmata il 4 novembre 1950 a Roma, con 47 stati firmatari ed entrata in vigore il 3 settembre 1953, nelle lingue ufficiali inglese e francese.

[302] La direttiva è una delle cinque direttive che insieme formano il pacchetto Telecom, un quadro normativo che disciplina il settore delle comunicazioni elettroniche. Le altre direttive disciplinano il quadro generale, l'accesso e l'interconnessione, l'autorizzazione e le licenze e il servizio universale. Il pacchetto è stato modificato nel 2009 dalle due direttive « Legiferare meglio » e « Diritto dei cittadini » nonché da un regolamento che istituisce l'Organismo dei regolatori europei delle comunicazioni elettroniche; eur-lex.europa.eu.

[303] Starnoni, A., Chatcontrol, nel 2022 la decisione definitiva dell'Ue sulla sorveglianza delle conversazioni private, Il controllo di massa delle chat per combattere gli abusi sui minori potrebbe presto diventare realtà, Mashable Italia, 9 Gennaio 2022.

[304]Carbone M.R., Regolamento Chatcontrol ovvero la sorveglianza di massa anche in Europa, La lotta alla pedopornografia è motivo di un regolamento approvato dal Parlamento europeo, che consentirà ai provider dei servizi di messaggistica di effettuare un super controllo sul contenuto delle chat svolte sulle proprie piattaforme. Molte le critiche: primo caso di sorveglianza di massa in UE 09 Lug 2021.

[305] Navacci M., Regolamento chatcontrol, cosa prevede e perché rischia di violare i diritti privacy, In votazione al Parlamento europeo il regolamento chatcontrol, che prevede una deroga alla Direttiva ePrivacy al fine di consentire ai provider di

A questo scopo è stato elaborato un testo legislativo che configura "a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online"[306].

Letteralmente si tratta di una deroga normativa che ha destato dialoghi controversi in ambito comunitario e non solo.

Anche Google si è schierato a favore della sospensione della Direttiva, mostrandosi sensibile alla tutela delle vittime di reati minorili, sottolineando, però, che la stessa sospensione non potrebbe implicare una lacuna normativa, che comporterebbe obblighi incondizionati ai fornitori di servizi, tra cui Google.

Quest'ultima riflessione da parte del colosso, non fa altro che evidenziare il problema del bilanciamento tra l'interesse dell'individui all'esercizio dei propri diritti e la sicurezza pubblica.

Il contenuto della Direttiva e-privacy si presta ad essere derogato soltanto limitatamente alla parte in cui si tratta di tutela minorile, conservando la sua natura di indispensabilità relativamente ai fini per cui è stata emanata: garanzia dell'accesso ai dati personali solo agli autorizzati, prevenzione della distruzione, perdita o alterazione accidentale o altre forme illegali di utilizzo dei dati; ed infine l'attuazione di politiche informatiche di sicurezza esercitata da tutti i gestori di servizi online.

Effettuata un'analisi dell'importanza della Direttiva, è necessario circoscrivere chirurgicamente il perimetro della sospensione della stessa e del testo dell'Unione che promuove una proroga.[307] In particolare, l'attenzione è stata posta all'Articolo

controllare i messaggi che transitano sulle piattaforme per individuare contenuti pedopornografici: un obiettivo lodevole, ma che mina i diritti di tutti gli europei, 6 luglio 2021.

[306] Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse; Council of the European Union, European Parliament, Official Journal of the European Union.

[307] Regolamento Chatcontrol, l'UE verso la sorveglianza di massa per prevenire la pedopornografia, 2 Ago 2021.

24 della Carta, nella parte in cui si occupa del compimento di atti relativi a minori da parte di autorità pubbliche o private, specificando che il tutto deve essere posto in essere preoccupandosi di porre in primo piano il c.d. *favor minoris*, cioè l'interesse preminente del minore, che avrà priorità su tutto il resto.

Per quanto nobile l'obiettivo, però, rischia di minare pesantemente il diritto alla privacy e violare del tutto—e non solo parzialmente—il divieto previsto dalla Direttiva *eprivacy*[308]. Persino gli strumenti dotati di criptografia end-to-end, come Whatsapp da qualche anno, sono a rischio di intercettazione. Il problema sorge dal momento che verrebbero decriptati messaggi, conversazioni, e-mail e qualsiasi altro genere di corrispondenza telematica alla ricerca di scambi pedopornografici tra utenti. Indiscriminatamente ogni contenuto potrebbe essere un potenziale oggetto di controllo dell'intelligenza artificiale[309]; proprio quest'ultima rappresenta complementarmente la più importante critica mossa al *ChatControl.*

L'addetto al controllo degli scambi online è una machine learning[310], cioè una macchina automatizzata che effettua un'analisi standardizzata dei contenuti, non differenziando le eventuali fonti e differenze d'età, incidendo approfonditamente sulla vita privata ed intima degli utenti.

Un primo controllo standard, dunque, viene effettuata dall'intelligenza artificiale che, in caso di sospette violazioni, collega quanto visto alla presenza di un c.d. *hash*[311], già registrato in un apposito database al quale fare riferimento per il controllo standardizzato.

---

[308] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)**,** *Gazzetta Ufficiale n. L 201 del 31/07/2002.*

[308] Carbone M.R., *Regolamento Chatcontrol ovvero la sorveglianza di massa anche in Europa, La lotta alla pedopornografia è motivo di un regolamento approvato dal Parlamento europeo, che consentirà ai provider dei servizi di messaggistica di effettuare un super controllo sul contenuto delle chat svolte sulle proprie piattaforme.* Molte le critiche: primo caso di sorveglianza di massa in UE 09 Lug 2021.

[309]Solanas A., Martínez-Ballesté A., *Advances in artificial intelligence for privacy protection and security*, Intelligent information systems, 2010.

[310] Hallinan D., Leenes R., De Hert P., Leenes R.E., *Data protection and privacy: data protection and artificial intelligence*, EComputers, privacy and data protection, 2021.

[311] Samtani S., Kantarcioglu M., Chen H., *A Multi-Disciplinary Perspective for Conducting Artificial Intelligence-enabled Privacy Analytics*, 2021.

Dunque, segnala automaticamente alle forze dell'ordine e queste ultime, in quanto persone fisiche, effettueranno di persona ulteriori indagini sui contenuti, configurando una seconda lesione del diritto alla privacy.

A mitigare questo tipo di rischio, però, vi è il GDPR, che all'Articolo 22[312] stabilisce una particolare tutela dei dati personali se in gioco c'è il controllo da parte di macchine automatizzate e dunque stabilendo delle condizioni alle quali sono subordinati controlli di questa natura. Al terzo comma, infatti, esso stabilisce che "il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione[313]."

Una volta rispettate queste condizioni, va da sé che non tutta la corrispondenza privata potrà essere violata indiscriminatamente, fungendo il GDPR da zona cuscinetto per prevenire abusi del diritto di intervento dell'Unione per perseguire fini legittimi in modo illegittimo.

Ancora, lo stesso Regolamento *ChatControl* [314]all'Articolo 3 si autolimita nella misura in cui prevede la disposizione di condizioni accurate a cui è subordinata l'attività d'indagine da parte delle machine learning: la proporzionalità del trattamento e la limitazione dello stesso alle "tecnologie utilizzate dai provider per

---

[312] "1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il paragrafo 1 non si applica nel caso in cui la decisione:
a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
c) si basi sul consenso esplicito dell'interessato.
3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione."

[313] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione 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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[314]Notaro S., *Le novità del Regolamento Europeo "ChatControl*, 27 settembre 2021, e-lex.it.

la sola finalità della prevenzione dei reati di pedopornografia e adescamento di minori;" la conformità delle tecnologie utilizzate e la minor invasione possibile delle stesse nei confronti della privacy dei singoli; una previa valutazione d'impatto e sia stata attivata una procedura di consultazione preventiva di cui agli Articoli 35 e 36 del GDPR[315]; rispetto del limite temporale delle tecnologie usate per il contrasto alla pedopornografia, non servendosene se non dopo l'entrata in vigore del Regolamento Chatcontrol; previa informazione agli utenti circa lo scopo delle tecnologie utilizzate per effettuare controlli finalizzati esclusivamente alla rilevazione di materiale pedopornografico; previa informazione dell'utente circa i diritti da lui esercitabili, come l'azione giudiziaria; gli standard inclusi nel database di riferimento delle machine learning deve contemplare una differenziazione tra il materiale pornografico inteso nella sua generalità e ciò che lo diversifica da quello connotato dalla pedofilia, quindi l'età[316].

In definitiva, la problematica contrapposizione tra la tutela dei diritti individuali e la protezione della sicurezza pubblica che comporta l'ingerenza delle autorità nella vita privata dei singoli, non sarà facilmente risolvibile, considerando il continuo sviluppo di nuove tecnologie, al quale seguirà la necessità di introdurre nuove tutele.

[315] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle

[316] Izzo L., *Regolamento ChatControl: le nostre mail e conversazioni sotto controllo?*, StudioCataldi.it, 27 ago 2021.

2.6 Il problematico bilanciamento del diritto alla privacy degli individui con il diritto di sorveglianza degli Stati

La dicotomia di cui sopra vanta uno scenario giudiziario alle spalle che ha da sempre comportato la necessità di bilanciare interessi fondamentali in gioco, sin dalla nascita di innovazioni potenzialmente funzionali alla sorveglianza intesa non soltanto come mera vigilanza statale per la tutela della sicurezza pubblica. In questo senso, è da considerare che non vi è un interesse preponderante su un altro, dovendo analizzare caso per caso se e quale sia l'interesse destinato a soccombere per uno scopo più nobile[317].

È fuori dubbio che nella maggior parte dei casi, a soccombere è il diritto alla privacy, ma ciò va contestualizzato in un'ottica di geopolitica, attualità e *habitat* sociale. La differenza tra versante europeo e statunitense[318] è indice della decisività di un ecosistema sociale con un certo background storico piuttosto che un altro. È più probabile, quindi, che in uno scenario come quello americano, a soccombere sia il diritto alla privacy, come testimoniato anche da casi mediatici e giudiziari—tra cui il caso Snowden [319]di cui si tratterà nel prossimo capitolo— piuttosto che in un continente che vanta una maggiore tranquillità in tal senso. Nonostante ciò, è indispensabile effettuare un bilanciamento per evitare di ledere uno dei due interessi, ovvero tentare di farlo solo superficialmente.

[317]Friedewald M., Burgess J.P., Bellanova R., Peissl W., edited by Friedewald M., Burgess J.P., Čas J., Bellanova R., Peissl W., *Surveillance, Privacy and Security, PRIO New Security Studies*, 2017.

[318] Kuntze J., *The abolishment of the right to privacy?: the USA, mass surveillance and the spiral model*, 2018.

[319] Dylan H., Beyond Snowden: *Privacy, Mass Surveillance, and the Struggle to Reform the NSA*, RUSI Journal, 03/2018, Volume 163, Fascicolo 2.

2.6.1 La risposta del "*Checks and balances*"

A seguito dell'attacco terroristico alle Torri Gemelle, l'Unione elaborò uno strumento di un pacchetto di Direttive del 2002 fra cui spiccò senza dubbio la c.d. *data retention*[320], entrata in vigore nel 2006, in particolare dopo gli attacchi di natura terroristici efferati a Madrid prima e a Londra poi. Quest'ultima si preoccupava di collezionare dati raccolti da providers e servizi di comunicazione elettronica a disposizione della collettività, in forma del tutto preventiva, e di conservarli per un periodo non inferiore a sei mesi e non superiore a due anni[321].
La natura preventiva del contenuto della Direttiva comunitaria, tuttavia, poneva seri dubbi di legittimità in quanto giustificata meramente da un'eventualità di indagini future, che non trovavano ragione d'esistere al momento della collezione dei metadati.

[320] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.

[321] Balzamo A., *Tutela della Sicurezza Pubblica vs Tutela della Privacy: un bilanciamento necessario, 30 ottobre 2020.*

2.6.1.1 Il caso Irlanda c. Parlamento Europeo e Consiglio dell'Unione Europea

La Corte di Giustizia ha provveduto ad eliminare i dubbi di cui sopra, come si evince dal disposto della sentenza del 10 febbraio 2009[322], C-301/06, circa la liceità delle fondamenta giuridiche della Direttiva *data retention*.[323] Ecco che diviene di basilare importanza la decisione della Corte in merito al ricorso da parte dell'Irlanda contro il Parlamento ed il Consiglio, proposto dal governo irlandese per chiedere l'annullamento della Direttiva Europea 2006/24/CE relativa alla conservazione dei dati generati, trattati o memorizzati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o dei dati sulle reti pubbliche di comunicazione a fini di prevenzione, ricerca, accertamento e perseguimento della criminalità, reati e terrorismo, per non essere stata adottata sulla base normativa corretta. Di tutta risposta, il Parlamento Europeo ed il Consiglio dell'Unione, chiedevano che fosse dichiarata l'infondatezza del ricorso. E la Corte si espresse proprio in quest'ultimo senso, sottolineando che il ricorso proposto dall'Irlanda non si basasse su un'eventuale violazione di diritti fondamentali, dati da ingerenze pubbliche nel diritto alla vita privata del singolo e che, dunque, l'intero ricorso che poggiava sul contrasto con l'Articolo 95 CE, non poteva essere accolto considerando che l'intera Direttiva si occupa dell'indagine, accertamento e persecuzione di reati.

[322] Sentenza della Corte, Grande Sezione, 10 febbraio 2009, nella causa C-301/06, avente ad oggetto il ricorso di annullamento, ai sensi dell'art. 230 CE, proposta il 6 luglio 2006.
[323] Caggiano G., *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*.

2.6.1.2 Mutamento dell'orientamento giurisprudenziale della Corte: la sentenza *Digital Rights*

L'orientamento della Corte è però drasticamente mutato ed emblematica del problema del *checks and balances* è la sentenza della stessa Corte, *Digital Rights Ireland*[324], in cui è stata sottolineata la delicatezza dei metadati, mettendo in luce l'irrilevanza della loro natura, trattasi di dati personali o no. La controversia riguardava gli obblighi imposti nei governi svedesi e britannici relativi alla conservazione di dati relativi a comunicazioni elettroniche gravanti in capo ai fornitori dei relativi servizi, sulla base della Direttiva 2006/24/CE dichiarata invalida.[325]

Come testualmente riportato, "Questi dati, presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati".[326]

A tal proposito, la Corte effettua il test di necessità circa la complessità delle misure implicanti collezione e trattamento dei dati personali e potenziali minacce del diritto alla vita privata, rendendosi imprescindibile un'analisi dei personali autorizzato all'accesso ai dati personali.

Al test di necessità, si affianca poi, quello di proporzionalità, contemperando l'interesse generale al raggiungimento di finalità collettive e il diritto alla "non intrusione" del singolo da parte delle autorità competenti. È così che la Corte, accertando l'eccesiva ingerenza delle azioni nei diritti fondamentali sanciti dalla

[324] Sentenza della Corte (Grande Sezione) 8 aprile 2014; Nelle cause riunite *C-293/12 e C-594/12*, aventi ad oggetto domande di pronuncia pregiudiziale proposte alla Corte, ai sensi dell'articolo 267 TFUE, dalla High Court (Irlanda) e dal Verfassungsgerichtshof (Austria), con decisioni, rispettivamente, del 27 gennaio e 28 novembre 2012, pervenute in cancelleria l'11 giugno e il 19 dicembre 2012.

[325] La Stampa, La conservazione dei dati delle comunicazioni elettroniche va giustificata da esigenze gravi, 2016.

[326] Sentenza della Corte, Grande Sezione,8 aprile 2014, «Comunicazioni elettroniche — Direttiva 2006/24/CE — Servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione — Conservazione di dati generati o trattati nell'ambito della fornitura di tali servizi — Validità — Articoli 7, 8 e 11 della Carta dei diritti fondamentali dell'Unione europea, Questioni pregiudiziali, Paragrafo 27.

Carta, dichiara l'invalidità della *data retention con effetti* ex tunc[327], sancendo la sproporzionalità fra l'ingerenza esercitata e la necessità delle garanzie in gioco.

[327]Caggiano G., *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*.

2.6.1.3 Il caso *Google Spain vs. AEPD and Mario Costeja Gonzales*

Simmetricamente alla sentenza di cui sopra, si pone la simbolica sentenza relativa al diritto all'oblio, *Google Spain*[328]*: causa C-131/12* . Il ricorso era proposto dal cittadino spagnolo contro Google SL e Google Inc. a seguito della sua richiesta di rimozione dal sito e da Google dei suoi dati personali pubblicati dal giornale *Lavanguardia Editiones* SL ormai non più attuali. L'Agencia Espanola de Proteccion de Datos aveva ordinato a Google di procedere con la rimozione dei dati richiesta, avendo per tutta risposta un diniego da parte del colosso in virtù della potenziale lesione dei diritti d'espressione online. Il caso è stato sottoposto dalla Corte Suprema Spagnola alla Corte di Giustizia in relazione all'ambito di applicazione della Direttiva 95/46/CE e al diritto all'oblio[329].

Veniva, dunque, in rilievo il ruolo giocato dal rinomato motore di ricerca nel panorama europeo: nel caso di specie, infatti, si faceva riferimento alla possibilità rimessa alle autorità nazionali di conservare una mole di dati personali nonostante il diritto rimesso all'individuo di cancellazione degli stessi. Nella sempreverde pronuncia, si ribadì come ai diritti evinti dalla Carta Europeo sia obbligatorio attribuire rilievo, non potendoli ignorare in virtù di nessuna giustificazione.

Lo scopo ultimo della sentenza, però, era quello di ampliare l'ambito di applicazione della Direttiva 95/46 CE[330], ovvero la *free flow of data*, includendo tra i campi applicativi in questione anche territori extraeuropei considerando la provenienza del motore di ricerca. Nello specifico, si trattò del divieto di trasferimento di dati raccolti nel territorio comunitario a Stati terzi, senza previa valutazione e autorizzazione della Commissione Europea.

---

[328] Sentenza della Corte (Grande Sezione)13 maggio 2014; Nella causa *C-131/12*, avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dall'Audiencia Nacional (Spagna), con decisione del 27 febbraio 2012, pervenuta in cancelleria il 9 marzo 2012, nel procedimento.

[329] Cavallari G., *Il diritto all'oblio in seguito al caso Google Spain vs. AEPD e Mario Costeja Gonzales*, iusiinitenere, 2018.

[330] 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 di tali dati, *Gazzetta ufficiale n. L 281 del 23/11/1995 pag. 0031 – 0050.*

La Corte si pronunciò affermando che l'attività di un motore di ricerca, come quella di Google, è configurabile a tutti gli effetti come trattamento dei dati personali, rintracciandone, nel caso di specie la violazione della protezione, riconoscendo al cittadino spagnolo il diritto all'oblio e condannando la controparte[331].

[331] Sentenza della Corte, Grande Sezione, 13 maggio 2014, nella causa C-131/12, avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dall'Audiencia Nacional, con decisione del 27 febbraio 2012.

2.6.2 La risposta della CEDU nel caso *Big Brother Watch and others v. UK*

L'importanza dell'operato della giurisprudenza Europea non si esaurisce con le sole due sentenze qui sopra citate, ma vanta un caso che ha segnato una svolta nelle controversie legate alla mass surveillance: il caso *Big Brother Watch e altri c. UK*[332].

Quest'ultimo nasce nel 2013, quando diversi giornalisti ed organizzazioni internazionali per i diritti umani, decisero di denunciare il governo britannico per l'attuazione di diversi regimi di sorveglianza, rispettivamente in relazione all'intercettazione di massa della corrispondenza, con particolare riferimento alle comunicazioni telematiche, ricezione di comunicazioni oggetto di sorveglianza di massa esercitata da altri governi stranieri e la fornitura di dati di comunicazione da parte di providers di servizi di comunicazione.

L'intercettazione di comunicazioni da parte del governo britannico, però, era legittimata al momento della commissione dei fatti, da un importante testo normativo: il RIPA (Regulation of Investigatory Powers Act) [333]del 2000, revisionato nel 2016.

La Corte statuì che l'atto in sé non era da considerarsi contrario alla Carta; tuttavia, nella sfera domestica, il governo avrebbe dovuto preoccuparsi di effettuare un previo test di proporzionalità e necessità, mai contemplato nell'esecuzione dell'operato dell'intelligence britannica.

Di conseguenza, la mancata supervisione da parte di un organo indipendente, essendo rimesse al Segretario di Stato tutte le autorizzazioni relative alle azioni di sorveglianza di massa, causò una violazione degli Articoli 7 e 8 della Carta Fondamentale. Tutto ciò, sommato ad un'assenza di crittografia end-to-end, premise all'intelligence britannica di avere libero accesso indistintamente a telefonate, e-mail e addirittura attività di Internet di qualsiasi genere, servendosi del

[332] Grand Chamber, Case of *Big Brother Watch and others v. The United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15) Judgement.

[333] Regulation of Investigatory Powers Act 2000 UK Public General Acts, legislation.gov.uk.

programma *Tempora*, lo stesso di cui si era servita precedentemente l'NSA per l'intercettazione dei cittadini statunitensi, come svelato durante il *Datagate*[334].

In termini giuridici, questo si tradusse in una mass surveillance lesiva dell'Articolo 8 della Carta Europea dei Diritti dell'Uomo, non ribadita, però, nella sentenza in questione. La Grande Camera, infatti, con una maggioranza di 12 voti a 5, ha sancito la liceità degli scambi intergovernativi di dati personali tra i diversi servizi segreti, in virtù di un sistema legislativo ampiamente tollerante in questo senso, vantando una serie di regolamenti che permettevano un simile scambio[335].

La Corte, a seguito della sentenza, rilasciò una comunicato stampa, nel quale forniva accurate spiegazioni circa l'orientamento prescelto, giustificando la decisione sulla base di una larga discrezione—ovvero "*margin of appreciaton*"—rimessa agli stati in materia di sorveglianza di massa, e di un progressivo sviluppo e mutamento delle forme di comunicazione, al quale deve seguire necessariamente una nuova forma di sorveglianza.[336]

Nel caso di specie, il Regno Unito, a detta della Corte, aveva peccato di lacune funzionali in tre direzioni: la mancanza di un'autorità competente a rilasciare autorizzazioni in materia di sorveglianza di massa che godesse di indipendenza; la mancata inclusion di selettori nell'application per l'autorizzazione; la mancata garanzia che i terms collegati ad ogni singolo utente fossero subordinate ad una previa autorizzazione interna.

Nonostante ciò, la stessa Corte sostenne che *"*owing to the proliferation of threats that States faced from networks of international actors, who used the Internet for communication and who often avoided detection through the use of sophisticated technology, the Court considered that they had a wide discretion ("margin of appreciation") in deciding what kind of surveillance scheme was necessary to protect national security. The decision to operate a bulk interception regime did not therefore in and of itself violate Article 8.*"* [337]

---

[334] Zacaria S., Martorana M., *Sorveglianza di massa nel Regno Unito, condanna della CEDU, Uno sguardo in Europa alla luce della recente sentenza della Corte europea dei diritti dell'uomo: vittoria della privacy come diritto umano*, altalex.com.

[335] Grand Chamber, Case of *Big Brother Watch and others v. The United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15) Judgement.

[336] *UK surveillance regime: some aspects contrary to the Convention*, Press Release, issued by the Registrar of the Court ECHR 165 (2021) 25/05/2021.

[337] *UK surveillance regime: some aspects contrary to the Convention*, Press Release, issued by the Registrar of the Court ECHR 165 (2021) 25/05/2021.

A questa corrente di pensiero, si opposero i cinque giudici con *separate conclusions*: come si evince dal dispositivo della sentenza, le considerazioni dell'opposizione non lasciarono margine di condivisione nei confronti della maggioranza.

Per questo motivo, si legge che "This judgment fundamentally alters the existing balance in Europe between the right to respect for private life and public security interests, in that it admits non-targeted surveillance of the content of electronic communications and related communications data, and even worse, the exchange of data with third countries which do not have comparable protection to that of the Council of Europe States. This conclusion is all the more justified in view of the CJEU's peremptory rejection of access on a generalised basis to the content of electronic communication, […] its limitation of exchanges of data with foreign intelligence services which do not ensure a level of protection essentially equivalent to that guaranteed by the Charter of Fundamental Rights."[338]

In conclusione, l'astratta violazione dei diritti fondamentali dell'uomo non ha trovato pratico riscontro nella giurisprudenza europea e gli applicants non hanno visto alcun riconoscimento dei propri diritti, essendosi la Corte limitata ad una mera liquidazione a questi ultimi di €91.000 in qualità di rimborso di spese processuali[339].

[338] *UK surveillance regime: some aspects contrary to the Convention*, Press Release, issued by the Registrar of the Court ECHR 165 (2021) 25/05/2021.

[339] Grand Chamber, Case of *Big Brother Watch and others v. The United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15) Judgement.

2.7 Conclusione

Il definitivo bilanciamento tra gli interessi in gioco, dunque, non avrà vita facile in nessun ordinamento nazionale; ancor meno, se si allarga lo sguardo verso un orizzonte internazionale, che mira alla collaborazione reciproca—fatta di continui scambi di dati personali, statistici, commerciali, sanitari— per perseguire scopi di natura sicuramente nobile, ma configurando, d'altra parte, un'arma a doppio taglio.

CAPITOLO TERZO

IL CASO SNOWDEN

"Il vero valore di una persona non si misura
dalle cose in cui sostiene di credere,
ma da che cosa è disposto a fare per proteggerle."

Edward Snowden

3.1 Premessa

Nel capitolo che segue si proverà come i servizi d'intelligence rappresentino un'arma a doppio taglio e, nel caso di specie, verrà esaminato l'altro lato della medaglia, quello che non rende di certo onore ai governi ed ai sistemi di difesa interna che esercitano i loro poteri, sconfinandone i limiti.

Questa problematica è stata particolarmente segnalata in relazione ai servizi segreti statunitensi, che nel 2013 sono stati protagonisti dell'eclatante caso Snowden.

Questo caso, oltre ad aver causato un contrasto politico, diplomatico e mediatico, ha sollevato un importante dibattito circa il regime dello spionaggio nel diritto internazionale, rilevante per governi, organizzazioni internazionali e persino individui.

Ci si soffermerà, per l'appunto, sulla lacunosa disciplina prevista in merito, configurandosi una vera e propria area grigia del diritto internazionale.

3.2 Il ruolo e le operazioni dell'NSA (National Security Agency) come affermazione di un regime tecnocratico

Gli Stati Uniti d'America hanno da sempre puntato ad un regime di sicurezza pubblica che fosse totalizzante, spesso facendo sì che lo scopo giustificasse i mezzi troppo ingerenti nella vita privata dei cittadini. Questo regime venne drasticamente rafforzato, guadagnando la configurazione di una vera e propria tecnocrazia consensuale e ben voluta. Il buon volere della collettività[340], tuttavia, fece i conti con un agente ben più potente di quanto si potesse immaginare: l'NSA[341].

L'NSA—ovvero National Security Agency[342]—è il corpo dell'intelligence americana più accreditato dal governo, che negli ultimi due decenni ha affermato la propria posizione dominante sul complesso di comunicazioni di qualsiasi natura scambiate fra i singoli, dimostrando di poter bypassare ogni autorizzazione dell'utente. Insieme alla CIA (Central Intelligence Agency)[343] e all'FBI (Federal Bureau of Investigation)[344], l'NSA si occupa dunque di monitorare lo scambio di comunicazioni sia interne al territorio che quelle estere, soprattutto quando quest'ultime riguardano affari intergovernativi, con particolare riferimento alla Casa Bianca[345].

L'NSA nasce dall'esigenza di coordinazione regionale e nazione tra le diverse organizzazioni d'intelligence che si occupavano di monitorare i dati circolanti, essendovi dunque separati archivi di database, e sconnessi tra loro.

La suddetta esigenza venne evidenziata dall'allora capo della CIA, Walter Bedell Smith, che con un rapporto al Consiglio per la sicurezza nazionale nel 1951—il

[340] Newport F., *Americans Disapprove of Government Surveillance Programs,* 12 giugno 2013.

[341] Choi P., *Intelligence: NSA: Washington's Best Kept Secret*, Harvard International Review, 1983.

[342] National Security Agency/Central Security Center, nsa.gov.

[343] Central Intelligence Agency, USA.GOV

[344] Federal Bureau of Investigation, The Federal Bureau of Investigation (FBI) enforces federal law, and investigates a variety of criminal activity including terrorism, cybercrime, white collar crimes, public corruption, civil rights violations, and other major crimes, USA.GOV

[345] Burns T.L., *The origins of the National Security Agency*, United States Cryptological History, 1990.

Rapporto della Commissione Brownell[346]— sottolineò l'inefficacia del sistema così come impostato, poiché si focalizzava su un monitoraggio che aveva ad oggetto indagini di poco rilievo per la nazione[347].

L'agenzia venne però ufficialmente autorizzata sotto l'amministrazione Truman nel giugno del 1952 ed istituita nel novembre del 1953[348]. È necessario precisare che il raggio d'azione dell'agenzia è stato parecchio ampliato a seguito dell'attacco terroristico del 2001 a New York: si passò da un mero controllo sulle comunicazioni estere, all'autorizzazione d'azione sulle comunicazioni interne. Questo venne realizzato supervisionando da vicino quella che venne denominata *contact chaining* o catena di contatto[349]. con cui si ottenevano registri interi di rubriche telefoniche di soggetti anche non sospetti da spiare[350].

L'operato dell'NSA, dunque, si è tradotto—e si traduce—in operazioni di intercettazione e decodificazione di messaggi, che sono perlopiù criptati.[351] A questo proposito, l'agente si è dotato di esperti del settore, ingegneri informatici o hacker in grado di effettuare una crittoanalisi e di avere accesso indiscriminatamente persino ai dispositivi mobili, quali webcam e microfoni seppur disattivati.

Si tratta dunque di un monitoraggio di cellulari, computer, televisioni, radio, il cui fine ultimo è la collezione di dati che lavori in prevenzione per la sicurezza pubblica[352]: questa supervisione, infatti, è finalizzata ad assicurare che non vi siano

---

[346] Dujmovic N., *The Significance of Walter Bedell Smith as Director of Central Intelligence,* CIA History Staff, Center for the Study of Intelligence, 1950-53.

[347] Bamford J., Cohen E. A., *Body of Secrets: Anatomy of the Ultra Secret National Security Agency,* Anchor Books, 2001.

[348] *Boak D. G., A History of U.S. Communications Security;* the David G. Boak Lectures, Vol.1, 1966.

[349] *What American intelligence & especially the NSA have been doing to defend the nation,* Vital speeches of the day, 2006.

[350] *National Security Agency – 60 Years of Defending Our Nation,* Archived 2018-06-23 at the Wayback Machine, Anniversary booklet, 2012.

[351] Agrestino C., *NSA, Datagate, sorveglianza di massa e altre storie*, Inchiostro, 19 dicembre 2016.

[352] Bonfatti R., *Datagate ed NSA. Tutto sullo scandalo spionaggio rivelato da Edward Snowden*, ALGROUNG, Portale di Sicurezza Informatica, 30 dicembre 2013.

dubbi circa la pericolosità e gli indici sintomatici di fenomeni terroristici neppure fra i più innocui cittadini[353].

Già nel 2005 l'NSA venne segnalata, per la prima volta, per l'ingerenza ingiustificata dell'autorità sulla corrispondenza privata dei singoli, sotto l'amministrazione Bush[354].

Venne autorizzata dal Presidente un'indiscriminata ed arbitraria indagine condotta dall'intelligence sui cittadini statunitensi ed in particolare sulle informazioni che venivano scambiate con l'estero, per rintracciare eventuali rischi terroristici[355].

Questo primo scenario venne denunciato dal rinomato giornale americano, il *New York Times*, al quale il governo in persona chiese di desistere dalla pubblicazione dell'articolo per evitare di vanificare le indagini fino ad allora condotte dalle agenzie d'intelligence interessate; per tutta risposta, il quotidiano si impegnò a ritardarne la diffusione per evitare di fornire informazioni potenzialmente utili ai terroristi[356].

Nonostante le pesanti critiche mosse a questa modalità d'azione, l'NSA, fortemente difesa dal Presidente Bush[357], non rallentò la corsa contro il tempo per vincere contro Al Qaida[358].

Quest'episodio, infatti, non configurò una battuta d'arresto per il controllo sui cittadini, traducibile in spionaggio interno ed estero, che continua ad evolversi con la progettazione di software, hardware, oltre che l'utilizzo di innumerevoli satelliti localizzati in tutta l'America.

---

[353] McLaughlin J., *NSA intelligence-gathering programs keep us safe*, The Washington Post, 2014.

[354] *"The National Archives, Records of the National Security Agency"*.

[355] *NSA: National Security vs. Individual Rights*, Amitai Etzioni, 24 gennaio 2014.

[356] Hirsh M., Isikoff M., *No More Hide and Seek: Armed with secret new intelligence, including NSA intercepts, America takes the case against Saddam to the world,* Newsweek global, 2003.

[357]Nakashima E., *"Bush Order Expands Network Monitoring: Intelligence Agencies to Track Intrusions"*, The Washington Post., 26 gennaio 2008.

[358]Kenny J., *NSA spying: it didn't start with 9/11: the NSA, an enormous agency created to collect and analyze intelligence on foreign threats, failed to stop 9/11 and now spies on Americans. Has it outlived its usefulness?,* The New American, 2013.

Gli esperti dell'intelligence, inoltre, si stima essere dislocati in tutto il mondo, per supervisionare e spiare in loco le comunicazioni interessanti, come nel caso di Edward Snowden di cui a breve si tratterà[359].

L'NSA agiva, in un primo momento, servendosi del programma *Stellar Wind* o *Vento Stellare*[360]*:* questo permetteva di spiare la corrispondenza via e-mail, fino a giungere alla corrispondenza telefonica, quella di Internet e qualsiasi altro scambio di informazioni che avvenisse con un soggetto che si trovasse al di fuori del territorio statunitense ovvero in caso di comunicazioni tra cittadini stranieri presenti sul territorio nazionale[361].

La prima vera battuta d'arresto subita dall'NSA risale al marzo 2000, dettata da James Comey, l'allora Viceministro della Giustizia, che segnalò l'assenza di una giustificazione di natura giuridica che permettesse il protrarsi dell'esercizio arbitrario di controllo in atto[362].

Cruciale in questo contesto, fu il ruolo giocato dalla FISA (*Foreign Intelligence Surveillance Act*)[363]: si tratta di un'introduzione legislativa dettata dalla necessità di monitorare le ingerenze estere, la sorveglianza internazionale, nel territorio americano, letteralmente, per l'appunto, Legge sulla Sorveglianza d'Intelligence Straniera[364].

---

[359] Greenwald G., *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, traduzione di Annoni I., Peri F., Rizzoli, 2014.

[360]Karlstrom E., *"Stellar Wind" (NSA warrantless surveillance program begun under Pres. G. W. Bush's President's Surveillance Program (PSP)*, Gang Stalking, Mind Control, and Cults, Exposing and Defeating Organized Gang Stalking, Mind Control, and Cults, 27 febbraio 2019.

[361] Di Marco E., *Un leak sul Guardian rivela l'incubo del programma Stellar Wind*, AgoraVox, 8 giugno 2013.

[362]Siobhan G., *"NSA killed system that sifted phone data legally"*, Baltimore Sun, Tribune Company (Chicago, IL), 17 maggio 2016.

[363] Ben O'Neill, *FISA, the NSA, and America's Secret Court System*, MISES Institute, 22 febbraio 2014.

[364] Francel M.T., *Rubber-stamping: legislative, executive, and judicial responses to critiques of the foreign intelligence surveillance court one year after the 2013 NSA leaks*, Administrative Law Review, 2014.

In particolare, il FISA Amendements Act[365], che regola la sorveglianza dell'NSA dal 2008, distingue la figura delle US person , cioè i cittadini americani o residenti legalmente sul territorio statunitense da tutti gli altri individui.

La FISA vanta anche un corpo giuridico[366], presieduto da un tribunale segreto speciale al quale l'NSA ha l'obbligo di rivolgersi per ottenere l'autorizzazione ad intercettare un US person; è lo stesso Articolo 702[367] della normativa[368] a sancire l'obbligatorietà della sottoposizione di linee guida per la sorveglianza al tribunale FISA per ottenere un permesso in bianco[369].

Proprio affinché l'operato del programma Stellar Wind venisse conformate su basi giuridiche, l'NSA dovette rivolgersi al giudice; per fare ciò, all'agenzia vennero concessi 90 giorni di tempo per aderire in toto alla legge. Il programma così conformato si protrasse per altri sette anni, sotto l'amministrazione Obama[370], che segnò la fine del progetto *stellare*, mai giustificata ufficialmente. Questo non implicò, comunque, il termine delle attività di spionaggio durante la presidenza di Barack Obama[371], che anzi si ampliò fino a raggiungere l'intercettazione degli indirizzi IP degli utenti, con un monitoraggio anche di metadati, giustificato, ancora una volta, da motivi di sicurezza pubblica[372].

---

[365] Forgang J.D., *"The right of the people": the NSA, the FISA Amendments Act of 2008, and foreign intelligence surveillance of Americans overseas,* Fordham Law Review, 2009.

[366] Foreign Intelligence Surveillance Court, United States, fisc.uscourts.gov, About Foreign Intelligence Surveillance Court.

[367] Indrajit S., Louoie C., Beyer J.L., *FISA's Section 702 & the Privacy Conundrum: Surveillance in the U.S and Globally*, The Henry M. Jackson School of International Studies, University of Washington, 25 ottobre 2017.

[368] Section 702 Title VII, Section 702 of the Foreign Intelligence Surveillance Act (FISA), "Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons".

[369] "*The Church Committee and FISA*", Bill Moyers Journal, Public Affairs Television, 26 ottobre 2007.

[370] Kumar M., *Stellar Wind Surveillance program under Obama administration*, The Hacker News, 27 giugno2013.

[371] Karlstrom E., *"Stellar Wind" (NSA warrantless surveillance program begun under Pres. G. W. Bush's President's Surveillance Program (PSP)*, Gang Stalking, Mind Control, and Cults, Exposing and Defeating Organized Gang Stalking, Mind Control, and Cults, 27 febbraio 2019.

[372] *"National Security Agency and the U.S. Department of Homeland Security Form New Partnership to Increase National Focus on Cyber Security Education"*, NSA Public and Media Affairs, 22 aprile 2004.

È stato poi il Wall Street Journal a stimare che ancora ad oggi il 75% del traffico dei metadati negli Stati Uniti sia sotto il controllo dell'NSA[373].

Nonostante ciò, l'agenzia continua a difendersi rilasciando dichiarazioni circa la liceità e legalità delle proprie operazioni[374]: la portavoce Vanee Vines ha infatti sottolineato l'incidentalità delle eventuali intercettazioni c.d. civili, ma che comunque mai configurano una lesione del diritto alla privacy[375], poiché rientranti tra i pieni poteri rimessi all'intelligence; ha manifestato altresì l'impegno di ridurre al minimo questo genere di ingerenze nella vita privata dei cittadini statunitensi[376].
Il servizio d'intelligence fu coadiuvato da un importante protagonista ex post della vicenda: l'AT&T[377], una delle maggiori compagnie di telecomunicazioni nel territorio americano, che partecipò al suddetto operato illegale per ben dieci anni, dal 2003 al 2013. L'assistenza della compagnia fu ritenuta di fondamentale importanza e di grande produttività per lo spionaggio dell'NSA, giacché le intere raccolte di e-mail ed utenti registrati venivano costantemente forniti all'agenzia[378].
Qui di seguito viene riportata la mappa delle intercettazioni e dei trasferimenti dei dati raccolti in tutto il mondo dall'NSA: come appare evidente, la raccolta di dati si concentra di gran lunga sulla corrispondenza comunitaria, statunitense e sudamericana, rendendo quasi immune il territorio del Cremlino da ogni interferenza.
Il traffico di dati a livello globale, interessava anche altri governi, ma è importante precisare che questi ultimi prendevano parte attivamente all' abuso di potere,

[373] Gearan A., *"'No Such Agency' spies on the communications of the world"*, The Washington Post, 7 giugno 2013.

[374] Dozier K., *"NSA claims know-how to ensure no illegal spying"*, Associated Press, 9 giugno 2013.
[375] Miller R. A., *Privacy and power: a transatlantic dialogue in the shadow of the NSA-affair*, Washington and Lee University, Virginia, Cambridge University Press, 2017.
[376] Wise D., *"Espionage Case Pits CIA Against News Media"*, The Los Angeles Times, 18 maggio 1986.
[377] Mosca G., *Datagate, AT&T ha aiutato l'Nsa a controllare il traffico internet*, Wired.it, 17 agosto 2015.
[378] *AT&T avrebbe aiutato la NSA nella raccolta di dati e intercettazioni*, informazione.it, 17 agosto 2015.

creando un apposito accordo, il c.d. *Five Eyes*[379], il cui nome prende vita dai cinque membri che lo sottoscrissero: Canada, Australia, Nuova Zelanda, Regno Unito e Stati Uniti.

Si trattava di un accordo stipulato per la circolazione di dati personali, firmato direttamente dai servizi segreti dei relativi Paesi, la cui nascita venne giustificata—ancora una volta—in nome di una maggiore efficienza della collaborazione internazionale per la lotta al fenomeno terroristico, ma qualche anno dopo smentita dalla Corte Europea dei Diritti dell'Uomo, che condannò il Regno Unito[380] nella sentenza *Big Brother Watch*, e dalla Corte d'Appello Statunitense che dichiarò l'illegalità delle operazioni dell'NSA denunciate da Snowden, come si vedrà qui di seguito.

[379] Five Eyes, Secret agreements allow secretive intelligence agencies in Australia, Canada, New Zealand, the United Kingdom, and the USA to spy on the world, Privacy International.

[380] Schweda S., *UK Surveillance Under Judicial Scrutiny: GCHQ Intelligence Sharing with NSA Contravened Human Rights, But Is Now Legal*, European Data Protection law review, 2015.

3.3 Il Datagate

Il Datagate nasce a seguito di importanti rivelazioni sull'operato dell'intelligence statunitense, in particolare dell'NSA, che coinvolgevano anche Paesi terzi, denunciando lo scambio e l'illegittima circolazione di dati personali tra Governi e lo spionaggio arbitrario sui cittadini statunitensi, senza previo consenso o mandato giuridico[381].

Il primo scandalo fu destato dal fenomeno di whistleblowing[382]—nonché la denuncia da parte di un dipendente di una condotta illegittima tenuta dal datore di lavoro ovvero nel luogo di lavoro, di cui ha avuto cognizione in virtù del rapporto di lavoro che lo lega all'ambiente in cui si consuma la condotta— messo in atto, per la prima volta, da WikiLeaks[383], l'organizzazione internazionale senza scopo di lucro, fondata da Julian Assange[384].

Il sito di WikiLeaks si occupava, per l'appunto di diffondere rivelazioni circa segreti di Stato che pervenivano da fonti sempre rimaste anonime, ma per la maggior parte whistleblower[385].

In particolare, si occupa di vere e proprie denunce sociali che hanno ad oggetto condotte non etiche di aziende e soprattutto governi, assicurando agli informatori che non ci siano fughe di notizie che possano mettere a repentaglio l'anonimato, motivo per cui la stessa WikiLeaks non ha mai voluto localizzare la propria sede, ritenendosi irrintracciabile[386] .

WikiLeaks diede il via al Dagatagate nel 2010, quando decise di pubblicare documenti secretati dal governo statunitense, provenienti dalle ambasciate americane dislocate nel mondo ed indirizzati agli uffici della Casa Bianca: il

---

[381] *Cos'è il Datagate e come è cominciato*, internazionale.it, Stati Uniti, 25 giugno 2015.
[382] *What is whistleblowing?,* whistleblowersinternational.com, Piacentile, Stefanowski & Associates LLP d/b/a Whistleblowers International, 2021.
[383] Caretto G*., Intercettazioni NSA: lo scandalo del Datagate dal 2013 ad oggi*, Startmagazine, economia, 24 febbraio 2016.
[384]Lagasnerie G., *The art of revolt: Snowden, Assange, Manning*, Stanford University Press, 2017.
[385]Munro I., *Whistleblowing and the politics of truth: Mobilizing 'truth games' in the WikiLeaks case*, SAGE journals, 16 dicembre 2016.
[386] Fowler A., *The most dangerous man in the world: Julian Assange and WikiLeaks' fight for freedom*, Melbourne University Press, 2020.

contenuto di quelle comunicazioni poneva l'amministrazione Obama sotto una luce potenzialmente attaccabile agli occhi degli altri governi e, soprattutto, dei loro leader, anch'essi protagonisti delle comunicazioni del governo statunitense.

Nel caso di specie, si trattava di spionaggio e considerazioni su capi e leader di Stato, fra cui lo stesso Presidente del Consiglio Berlusconi ed il suo legame diplomatico con il Cremlino Putin, fortemente criticato dall'amministrazione americana. Neanche il Presidente francese Sarkozy restò immune alle critiche del governo americano, anch'egli oggetto di considerazioni espresse in senso del tutto negativo circa il suo operato internazionale[387].

A seguito di questa fuga di notizie, WikiLeakes ricevette importanti accuse dalla Casa Bianca che si trovò in una posizione diplomaticamente scomoda e tutta da giustificare: a Julian Assange venne imputata l'illiceità del possesso di quelle informazioni, aldilà dell'illegittima diffusione delle stesse ai danni del governo americano.

L'organizzazione fu costretta a chiudere il sito Internet, poiché sfrattata dal dominio originariamente creato, per poi spostarsi su altre piattaforme come Twitter e portare avanti la propria attività di denuncia, nonostante le gravi conseguenze penali ricadute sul fondatore di WikiLeaks.

Nello stesso anno, Barack Obama istituì un organismo interamente adibito ad occuparsi della questione WikiLeaks e alla riparazione dei danni diplomatici e commerciali che quel whistleblowing stava causando: l'Interagency Policy Committee for WikiLeaks (IPCW)[388].

Di lì a poco, il governo statunitense sarebbe stato ancora una volta bersaglio di ben più gravi accuse che interessarono comunicazioni internazionali, intercettazioni e condotte illegittime esercitate dai servizi segreti, ancora una volta denunciate da colui che sarebbe diventato negli anni il whistleblower per eccellenza: Edward Joseph Snowden.

---

[387] Leigh D., Harding L., Pilkington E., Booth R., Arthur C., *Wikileaks: inside Julian Assange's war on secrecy*, Guardian nooks, 2011.

[388] Heembsergen L., *Radical transparency and digital democracy: WikiLeaks and beyond*, Emerald Publishing Limited, 2021.

3.3.1 Le rivelazioni di Edward Snowden sulle operazioni d'intelligence americana

La reputazione dei servizi segreti americani ha vissuto una profonda crisi, aggravando pesantemente la già presente insofferenza dei cittadini nei confronti di un'autorità così ingerente.

Nel 2013, Edward Snowden[389], ai tempi dipendente dell'NSA, decise di rilasciare dichiarazioni di portata mai vista, denunciando apertamente la reale entità delle intercettazioni e violazioni della privacy[390] da parte dell'intelligence[391].

Il 6 giugno 2013, Edward Snowden divenne ufficialmente un *whistleblower* non ancora identificato, quando il *The Guardian*[392], pubblicò il primo articolo sulle rivelazioni fatte dall'hacker[393], in cui si accusava non senza prove l'NSA di avere accesso a tutti i dati telefonici forniti dalla *Verizon*[394], una rete di comunicazioni americana, la più importante del Paese[395]: ciò implicava che tutte la corrispondenza telefonica della rete più ampia negli Stati Uniti fosse completamente ed indiscriminatamente sotto il controllo dei servizi segreti[396].

Snowden precisò che il governo statunitense era in grado di trasformare i cellulari in veri e propri dispositivi di sorveglianza, attivandoli a distanza in qualunque momento, con la stessa giustificazione della lotta alla criminalità[397].

---

[389] Lyon D., *Surveillance after Snowden*, Wiley, 2015.

[390] *"NSA surveillance exposed by Snowden ruled unlawful"*, BBC News, 3 settembre 2020.

[391] Greenwald G., *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, traduzione di Annoni I., Peri F., Rizzoli, 2014.

[392] Greenwald G., *"NSA taps in to internet giants' systems to mine user data, secret files reveal"*, The Guardian, London, 6 giugno 2013.

[393] Greenwald G., *"The crux of the NSA story in one phrase: 'collect it all': The actual story that matters is not hard to see: the NSA is attempting to collect, monitor and store all forms of human communication"* The Guardian, 15 luglio 2013.

[394] Snowden E. J., *Permanent Record*, Pan Macmillan, pubblicato il 17 settembre 2019, data corrispondente all'entrata in vigore della Costituzione Americana, il 17 settembre 1787.

[395] Bell E., *Journalism After Snowden: The Future of the Free Press in the Surveillance State*, Columbia University Press, 2017.

[396] Bruder J., Maharidge D., *Snowden's box: trust in the age of surveillance*, Verso, 2020.

[397] Fidler D.P., *Office of the Director of National Intelligence and James R. Clapper, Director of National Intelligence, Statements on NSA Cryptological Capabilities, The Snowden Reader*, Indiana University Press, 2015.

Già nel 2006, infatti, grazie ad un mandato giuridico, l'FBI si servì di cellulari trasformati in microspie, c.d. *roving bugs*[398], attivabili a distanza, utili per l'indagine contro un'associazione di stampo mafioso.

Questa capacità di attivazione a distanza condusse Edward Snowden, al momento delle rivelazioni nascosto in un hotel ad Hong Kong, ad isolare ogni tipo di dispositivo presente all'incontro con i giornalisti del The Guardian che sarebbero stati responsabili della pubblicazione di ogni informazione[399], invitandoli a riporre il proprio cellulare nel frigobar[400].

Il primo articolo pubblicato allegava il link che riportava direttamente all'ordinanza del tribunale FISA, con cui si ingiungeva a Verizon di "*comunicare tutti i metadati telefonici in suo possesso*", ogni giorno e su base continuativa, riguardanti scambi telefonici tra gli Stati Uniti e l'estero ed anche quelli meramente interni[401].

A seguito di quel primo scandalo, la Casa Bianca si fece sentire, facendo intervenire anche la senatrice Feinstein, secondo la quale quell'ingerenza era del tutto tollerabile in virtù di un più nobile scopo, sostenendo che gli stessi cittadini volevano continuare a vivere in un Paese più sicuro dopo l'attentato dell'11 settembre[402].

Seppur in un primo momento fosse stato aspramente negata la violazione della normativa FISA, del Patriot Act e persino dell'Executive Order 1233, l'NSA rappresentata da Keith Alexander, capo dell'intelligence statunitense, fu costretta a ritrattare la propria tesi ed ammettere possibili lesioni delle suddette regolamentazioni, a discapito delle *US person*[403].

Tra i programmi svelati da Snowden, oltre al principale PRISM, di cui si parlerà nel prossimo paragrafo, ve ne furono svariati emblematici del proposito che si

---

[398] *"Spy Suspect May Have Revealed U.S. Bugging; Espionage: Hanssen left signs that he told Russia where top-secret overseas eavesdropping devices are placed, officials say"*, Los Angeles Times, 28 febbraio 2001.

[399] Fidler D.P., *The Snowden reader*, Indiana University Press, 2015.

[400] Greenwald G., *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, 2016.

[401] Greenwald G., *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, 2016.

[402] Risen M., *House Intelligence Chairman Considering NSA Reform Legislation*, U.S. news & world report, 2013.

[403] Executive Order 12333 United States Intelligence Activities (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008).

celava dietro l'operato dell'NSA: primo fra tutti TEMPORA, di cui l'intelligence si serviva per archiviare tutti i dati del traffico virtuale; Karma Police, con cui si effettuava una profilazione degli utenti in base alla loro cronologia di operazioni durante la navigazione in Internet; infine, Black Hole, un autentico deposito di azioni effettuate dagli utenti, persino le parole digitate sui motori di ricerca, oltre alle iscrizioni ed operazioni di login/logout dalle diverse piattaforme[404].

Le armi dell'NSA, in definitiva, erano—e sono—probabilmente le più potenti dell'orizzonte globale, in grado di sfidare qualsiasi protezione della riservatezza[405].

[404] Snowden E. J., *Permanent Record*, Pan Macmillan, pubblicato il 17 settembre 2019, data corrispondente all'entrata in vigore della Costituzione Americana, il 17 settembre 1787.

[405]Clarcke R.A., Morell M. J., Stone R.G., Sunstein C.R., Swire P., *Who guards the guardians? The NSA Report Liberty and Security in a Changing World The President's Review Group on Intelligence and Communications Technologies*, Princeton University Press, 2014.

3.3.2 L'utilizzo di PRISM come chiave d'accesso alle piattaforme sociali senza autorizzazione

La seconda rivelazione diffusa da Edward Snowden coinvolse le nove agenzie di telecomunicazioni principali, svelando un espresso accordo fra queste ultime e la National Security Agency, in virtù del quale l'intelligence intercettava gli utenti di Google, Apple, Yahoo!, Skype, Gmail, Facebook[406], con il tacito lasciapassare da parte dei colossi interessati[407].

In particolare, per questo genere di operazioni, l'NSA si serviva di PRISM[408], un programma top secret, al quale le nove società avevano aderito consensualmente, consentendo all'NSA accesso indiscriminato all'archiviazione di foto, video, audio e conversazioni di tutti gli utenti iscritti alle piattaforme[409].

Snowden allegò, a riprova delle dichiarazioni, i documenti segreti dei servizi segreti con cui si provava l'utilizzo di PRISM[410], mostrando delle slide dimostrative del successo che l'intelligence stava raggiungendo grazie a quel potente mezzo di intercettazione, annettendo grafici con l'implemento dei dati a cui riusciva ad accedere.

In uno dei messaggi coperti dal segreto di Stato, si quantificava in percentuale il potenziamento dell'ingerenza dell'NSA dopo l'introduzione di PRISM: nell'ultimo anno fiscale[411]—fiscal year12 (2012)—il totale delle relazioni finali ammontava a 24.096, con un incremento del 27% rispetto all'anno fiscale fy11[412].

Alcuni vertici delle società della Silicon Valley, tra cui Twitter, si sono rifiutati di concedere indiscriminato accesso al governo statunitense al proprio server; diversi

---

[406]Guldner J., *A friend request from the NSA: how intelligence services use social network sites*, International Politik, 2014.

[407] Greenwald G., MacAskill E.,*"NSA Prism program taps in to user data of Apple, Google and others"*., The Guardian, 6 giugno 2013.

[408] Greenwald G., *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, 2016.

[409]Risen L., Poitras L., *"N.S.A. Collecting Millions of Faces From Web Images"*, The New York Times, 31 maggio 2014.

[410] Rosenbach M., Stark H., Stock J., *"Prism Exposed: Data Surveillance with Global Implications"*, 10 giugno 2013.

[411] Greenwald G., *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, 2016.

[412] Snowden E. J., *Permanent Record*, Pan Macmillan, pubblicato il 17 settembre 2019, data corrispondente all'entrata in vigore della Costituzione Americana, il 17 settembre 1787.

funzionari governativi furono inviati, infatti, a far visita agli uffici della Silicon Valley per giungere ad un accordo, che fosse voluto o no.

A tal proposito, nonostante la variabile malleabilità delle diverse società, l'NSA ha comunque ottenuto dialoghi con le reti telematiche che, dal canto loro, si impegnavano a consentire l'accesso, ogni qual volta, legittimamente, l'intelligence lo avesse richiesto sulla base di prerogative mai precisate[413].

Ma fondamentale fu l'intesa con Microsoft, dopo l'acquisto da parte di quest'ultima di Skype; in un altro comunicato segreto dell'NSA si legge, infatti, che dal 7 marzo 2013 PRISM ha acquisito dati da Microsoft SkyDrive per chiavi di ricerca ai sensi del paragrafo 702 del FISA Amendements Act[414], di cui sopra, in virtù del quale dipendenti dell'NSA non avrebbero più dovuto attendere l'accettazione della richiesta da parte della SSO per poter avere accesso a quei dati, così sbloccando una nuova modalità di acquisizione dati di PRISM[415] su Skype: *Skype Stored Communications*.

In questo modo, la SSO creava autentiche chiavi di ricerca con cui semplificare il lavoro di sorveglianza, dopo aver analizzato tutti i dati unici di Skype, fra cui tabulati telefonici, dati bancari, liste di contatti, aumentando esponenzialmente il potere di sorveglianza dell'NSA[416].

Questo modus operandi si è posto in totale contrasto con quanto dichiarato dai vertici di Skype poco tempo addietro, rassicurando i propri utenti circa l'impossibilità di intercettazione delle comunicazioni tenute sulla piattaforma.

Grazie all'utilizzo di PRISM, l'NSA si è servita dello spionaggio anche per fini industriali[417], agendo per conto dei c.d. clienti che non erano più soltanto il governo e la CIA, ma annoveravano anche i Rappresentanti per il commercio internazionale, per i quali fu cruciale l'attività di sorveglianza sugli scambi di comunicazioni fra

---

[414] Cuffo A., *Snowden: "Microsoft lavorava a stretto contatto con la NSA"*, Panorama, Sicurezza, 12 luglio 2014.

[415] Handley J., *PRISM and boundless informant: is nsa surveillance a threat?,* American diplomacy, 2013.

[416] Edgar T.H., Beyond Snowden, Privacy, Mass Surveillance, and the Struggle to Reform the NSA, Brookings Institution Press, 29 agosto 2017.

[417]Becker P., *Development of Surveillance Technology and Risk of Abuse of Economic Information,* Report, STOA, European Parliament, ottobre 1999.

gli Stai terzi: monitorare e spiare le strategie che sarebbero state adottate dalle altre parti contraenti comportava un enorme vantaggio per il settore industriale americano. Una lettera da parte del sottosegretario di Stato, Thomas Shannon, indirizzata proprio agli uffici dell'NSA e resa pubblica, ha testimoniato l'importanza di questa ingerenza in occasione del Quinto Summit delle Americhe[418].

[418] *Snowden, Nsa fa spionaggio industriale,* Redazione ANSA, 26 gennaio 2014.

3.4 Lo sviluppo del caso Snowden

Dopo le rivelazioni trattate, Edward Snowden, si rifugiò in Russia il 23 giugno 2013, dove rimase per due mesi all'aeroporto di Mosca, chiedendo asilo politico al Governo di Mosca e ricevendo un riscontro positivo[419].

Nell'immediatezza dello scandalo, però, l'ex contractor della NSA si trovava ad Hong Kong, meta scelta non a caso, dallo stesso giustificata: i dipendenti dei servizi segreti sono obbligati a comunicare i propri spostamenti con un preavviso di 30 giorni, con la possibilità di essere costantemente controllati per tutta la durata del viaggio[420].

Le uniche due mete che avrebbero permesso a Snowden di lavorare senza il pericolo di un arresto immediato erano l'Islanda e, per l'appunto Hong Kong. La prima meta fu da escludere a seguito della revoca del passaporto statunitense nei confronti di Snowden, dopo che il governo apprese del suo imminente trasferimento da Hong Kong all'Islanda, grazie ad un aereo interamente finanziato da Wiki Leaks[421].

La scelta fu, dunque forzata e l'aereo di Snowden fu costretto ad atterrare a Mosca[422], già in volo al momento della revoca.

Il mancato trattenimento da parte del governo giapponese fu giustificato dalla regolamentazione del Paese in materia di estradizione, non essendovi stata violazione alcuna da parte di Snowden coerentemente allo Stato di diritto del Giappone[423].

Nel frattempo attivisti, organizzazioni internazionali e persino molteplici governi si mobilitarono per assicurare protezione all'ex contractor della CIA, fra cui l'Ecuador, dichiaratosi disposto a concedere asilo politico a Snowden, nonostante la richiesta di estradizione pervenuta dagli Stati Uniti: il diritto ecuadoregno

---

[419] Greenwald G., *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, traduzione di Annoni I., Peri F., Rizzoli, 2014.
[420] Snowden E. J., *Permanent Record*, Pan Macmillan, pubblicato il 17 settembre 2019, data corrispondente all'entrata in vigore della Costituzione Americana, il 17 settembre 1787.
[421] Greenwald G., *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, traduzione di Annoni I., Peri F., Rizzoli, 2014.
[422] Gavazzi L., *Edward Snowden, PRISM e Datagate, le cose da sapere*, Panorama, 2014.
[423] Scheuerman W.E., *Whistleblowing as civil disobedience: The case of Edward Snowden*, SAGE journals, 8 giugno 2014.

prevede, infatti, delle eccezioni in tal senso, disponendo che i reati politici configurano un'eventualità, in presenza della quale, il governo può negare l'estradizione se il soggetto interessato è perseguito per ragioni meramente politiche.

Tra i paesi che si dichiararono disposti ad accogliere politicamente Edward Snowden ci furono, a seguire, Bolivia e Nicaragua[424].

La scelta definitiva dell'ex dipendente dell'intelligence ricadde comunque sulla Russia, territorio nel quale Snowden decise di permanere definitivamente dopo la scadenza dell'asilo politico temporaneo concesso dal governo russo.

Rispettivamente nel 2017 e nel 2020 Snowden ottenne il permesso di residenza e la cittadinanza russa[425].

[424] Harding L., *Snowden. La vera storia dell'uomo più ricercato del mondo*, Newton Compton Editori, 17 novembre 2016.

[425] Lombardi C., *Edward Snowden ha ottenuto il permesso di residenza permanente in Russia*, Wired.it, 26 ottobre 2020.

3.4.1 L'evoluzione giuridica del caso Snowden

La vicenda di Edward Snowden, oltre a rappresentare uno scandalo senza precedenti, costituì anche una controversia giuridica complessa da districare, dal momento che non vi era più un solo governo coinvolto attivamente e passivamente[426].

Se da un lato gli Stati Uniti premevano per ottenere l'estradizione del proprio cittadino, lo scenario internazionale si divise in alleati e nemici di Snowden, fra questi ultimi l'Italia, la Francia e la Spagna che accolsero la richiesta statunitense di vietare il sorvolo dell'aereo di Snowden sul proprio territorio[427].

Nonostante ciò, fu proprio il Parlamento Europeo, con 285 voti favorevoli e 281 contrari, a decidere affinché gli stati membri si adoperassero per la protezione di Edward Snowden: gli fu riconosciuto lo status di informatore e difensore internazionale dei diritti umani, l'Unione Europea si impegnò a ritirare ogni azione penale nei suoi confronti e si dichiarò contraria alla concessione dell'estradizione del cittadino statunitense nonostante la richiesta americana.

È altrettanto vero, però, che tanti altri governi furono additati per aver in qualche modo esercitato complicità con il governo americano: basti pensare al sistema dei Five Eyes di cui sopra, protagonista fra tutti il governo britannico[428].

A distanza di sette anni, nelle aule di tribunale, fu scritta una nuova pagina di giurisprudenza.

Nel caso di specie, la Corte d'Appello americana del Nono Circuito[429], emanò una sentenza che configurò la vittoria giuridica, sociale e personale di Edward Snowden, dichiarando le operazioni della NSA illegali, in quanto lesive del Foreign

[426] Walsh P.F., Miller S., Rethinking *'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden*, Taylor & Francis Online, 22 gennaio 2015.
[427] Edward Snowden, *7 anni dopo i giudici gli danno ragione: "Il programma di sorveglianza della Nsa era illegale"*, il Fatto Quotidiano, 5 settembre 2020.
[428] Walsh P.F., Miller S., *Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden*, Taylor & Francis Online, 22 gennaio 2015.
[429] Robeldo P., *Edward Snowden: avere ragione, sette anni dopo*, The Good Lobby, 11 settembre 2020.

Intelligence Security Act e potenzialmente lesive della Carta Costituzionale Americana[430].

I dirigenti che si erano fatti da portavoce dei servizi segreti americani—fra cui lo stesso Keith Alexander—che in un primo momento avevano negato ogni tipo di operato illegale, furono costretti a ritrattare nel 2020, quando ammisero di aver violato il diritto alla privacy dei cittadini, ancora una volta adducendo come causa giustificativa la lotta al terrorismo e dimostrando la crucialità della sorveglianza, come nel caso dei quattro US person di San Diego, soggetti ad intercettazioni—che ad avviso dell'orientamento giurisprudenziale sarebbero state illegali—e scoperti quali fautori del fenomeno terroristico domestico[431].

Le accuse di Snowden furono ufficializzate il 14 giugno 2013, quando i procuratori federali degli Stati Uniti d'America sporsero denuncia, pubblicata sette giorni dopo, con la quale si formalizzavano i capi d'accusa contro l'ex contractor dell'intelligence: comunicazione non autorizzata di informazioni di difesa nazionale, furto di proprietà dello stato americano, comunicazione di informazioni coperte da segreto di stato a soggetti non autorizzati[432].

In altre parole, tradimento alla patria e spionaggio; quest'ultima accusa fu sottoposta alla legislazione speciale del FISA[433].

---

[430] *Usa, sentenza Snowden: "Dopo 7 anni mai avrei immaginato di trionfare in Usa"*, Redazione Bloglive, 4 settembre 2020.

[431] Fuchs C., Trottier D., *Internet surveillance after Snowden: A critical empirical study of computer experts' attitudes on commercial and state surveillance of the Internet and social media post-Edward Snowden*, Journal of Information, Communication and Ethics in Society, 23 novembre 2017.

[432] Bauman Z., Bigo D., Esteves P., Guild E., *After Snowden: Rethinking the impact of surveillance*, Oxford Academic Journals, International Political Sociology, 2014.

[433] Greenwald G., *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, traduzione di Annoni I., Peri F., Rizzoli, 2014.

3.5 Le conseguenze diplomatiche del Datagate sugli USA: le intercettazioni sulla cancelliera Merkel e sulla presidente Rousseff

Ad aggravare la posizione del governo statunitense, si aggiunsero le inevitabili reazioni dei governi esteri[434], con particolare riferimento a quelli nei confronti di quali l'USA vantava un rapporto amicale.

Nonostante il presunto rapporto di fiducia stretto con Paesi quali il Brasile o la Germania, l'intelligence americana non si risparmiò pesanti operazioni di spionaggio: il Datagate svelò le intercettazioni nei confronti della Presidente brasiliana Rousseff[435], maggiormente nel periodo della campagna elettorale, captando dati anche crittografati dalla corrispondenza telematica scambiata dall'allora candidata con tutta la rubrica di contatti[436].

La conseguenza fu un'immediata e grave accusa sporta dall'allora Ministro della Giustizia brasiliana Cardozo, nei confronti del governo statunitense circa la presunta violazione di sovranità interna[437].

Neppure il Messico rimase immune da questo genere di spionaggio: il Presidente messicano Enrique Pena Nieto, anche lui in campagna elettorale, fu nel mirino dell'NSA, essendo stato intercettato nei suoi scambi di informazioni.

Entrambi i governi si mobilitarono per chiedere chiarimenti in merito alla vicenda che avrebbe potuto compromettere importanti relazioni diplomatiche e comportare ripercussioni anche per il commercio internazionale, ricevendo per tutta risposta, delle spiegazioni lacunose e poco convincenti da parte degli ambasciatori americani[438].

---

[434] *Datagate, spiati 35 leader mondiali. La Ue: risposta forte agli Stati Uniti*, Il Mattino, 24 ottobre 2013.

[435] Treccani, *Il caso Snowden e le conseguenze diplomatiche del Datagate*, Atlante Geopolitico, 2014.

[436] *Caso NSA, Obama chiese chiarimenti dopo notizie su Brasile e Messico*, Libero Quotidiano, 31 ottobre 2013.

437 Suffia G., *Effetti geopolitici del Datagate: appunti e spunti per la geopolitica della sorveglianza globale*, Cyberspazio e Diritto, Mucchi Editore, 2015.

[438] Datagate. Messico condanna spionaggio NSA, Blitz Quotidiano, 21 ottobre 2013.

Così, lo stesso Presidente Obama fu invitato ad aprire un'indagine nei confronti della propria intelligence e decise di mettere in atto una riforma strutturale dell'NSA, dopo pesanti minacce di interruzione della collaborazione internazionale per la lotta al terrorismo da parte dei governi interessati dallo scandalo[439].

L'unica differenza fu una diminuzione del potere del tutto discrezionale rimesso ai dipendenti dell'NSA circa la possibilità di accesso ai dati secretati e non, temperando la potenziale violazione del diritto alla privacy dei singoli.

Ben presto, ci si accorse che quel tentativo di risoluzione, non sarebbe riuscito neppure a tamponare le frammentazioni di respiro internazionale che si stavano realizzando; dunque, in una proposta presentata ad inizio 2014, il Presidente Obama concretizzò una seria svolta nella disciplina dei servizi segreti[440].

Nel caso di specie, sarebbe stato proibito l'uso di PRISM dopo le rivelazioni che ne dimostravano un utilizzo indiscriminato, ma limitato a quanto espressamente permesso; sarebbe stato vietato lo spionaggio di governi con cui si vantava un rapporto di fiducia—nulla fu precisato in relazione ai governi nemici, quali la Russia o la Cina, che dal canto loro ricambiavano operazioni di intercettazione sul governo americano.

La novità più rilevante sul versante giudiziario, però, fu senz'altro l'introduzione dell'obbligo di richiesta da parte dell'NSA di un mandato giustificato in virtù di un'autorizzazione giudiziaria, per poter avere accesso a particolari classi di dati dei singoli, e a far da garante a quest'ultimo proposito, fu istituito un apposito organismo, incaricato di occuparsi delle eventuali violazioni della privacy da chiunque lamentate[441].

La crisi diplomatica più importante, e la stessa che diede la spinta decisiva al Presidente Obama per proporre la riforma, tuttavia, si realizzò con il governo

[439] *Pegasus. La Francia apre un'inchiesta, in Messico spiato anche il presidente Obrador*, Rai News, 20 luglio 2021.
[440] De Scalzi N., *Obama e la riforma NSA*, Treccani, Atlante Geopolitico, 29 gennaio 2014.
[441] Spatti S.*, Il discorso di Obama sulle proposte di riforma della Nsa*, Il Sole 24 Ore, 17 gennaio 2014.

tedesco presieduto dalla cancelliera Angela Merkel[442]anch'ella preda dello spionaggio illecito americano.

Nonostante un primo tentativo di rassicurazione da parte del Presidente degli USA circa l'infondatezza di quella fuga di notizie nei confronti della Merkel, i rapporti transatlantici si incrinarono ulteriormente—e quasi definitivamente— dopo la scoperta di una base di spionaggio inglese proprio a Berlino[443], che diede il finale colpo di grazia al rapporto già incrinato tra i due Paesi.

La cancelliera fu invitata alla Casa Bianca, un incontro finalizzato alla stipula di un accordo anti-spionaggio, mai firmato, data la determinazione mostrata dal governo tedesco nel voler reagire attivamente alle violazioni subite, mettendo sul tavolo del legislatore europeo nuove carte[444], mai viste sino ad allora, che proponevano iniziative per impedire un dejà vu dell'accaduto e che potessero armonizzare il panorama comunitario e non solo quello domestico.

[442] Datagate, *"Usa spiava diplomatici UE", Ira di Schulz, "Enorme scandalo",* Redazione Blitz, Blitz quotidiano, 29 giugno 2013

[443] Treccani, *Il caso Snowden e le conseguenze diplomatiche del Datagate*, Atlante Geopolitico, 2014.

[444] Germania, Datagate: Merkel proporrà a UE la creazione di un network europeo, Notizie Geopolitiche, 16 febbraio 2014.

3.6 Quadro storico del regime di spionaggio nel diritto internazionale

Lo spionaggio esercitato dagli Stati ed il suo regime non è mai stato oggetto di primaria importanza per il diritto internazionale, essendosi interessati alla questione soltanto i Governi, in quanto soggetti attivi e passivi di questo genere di operazioni, nulla contando a questo proposito gli individui ed i diritti umani fondamentali, tra cui quello alla privacy.

Lo spionaggio, tuttavia, iniziò a preoccupare seriamente gli Stati, all'inizio degli anni 50, quando per la prima volta si parlò di sorveglianza in termini informatici, in particolare finalizzata alla *Foreign Surveillance*, letteralmente, sorveglianza estera[445].

Dunque, l'approccio più accreditato dal diritto internazionale nei confronti dello spionaggio, nonostante contrastanti posizioni assunte dagli Stati, è il c.d. *Lotus Approach*[446]: quest'ultimo è applicabile a tutti i casi di vuoti normativi, in cui si necessita di esercitare comunque giurisdizione, ma il modus operandi è interamente rimesso alla libertà di agire degli Stati.

Si tratta dei casi di *non liquet*, circostanze in cui ci si limita a verificare l'assenza di diritto positivo o negativo in materia; accertato il vuoto legislativo, è rimessa ampia discrezionalità agli Stati circa i principi da applicare, come statuito dalla Corte Internazionale di Giustizia nell'omonimo caso *Lotus*[447]: si trattò di una collisione fra una nave francese ed una turca, durante la quale persero la vita otto marinai turchi nel mare greco e si rese necessario giudicare il comandante francese alla guida della nave.

Il luogo della collisione fu fondamentale per le sorti del caso, soffermandosi l'intera controversia sul problema dell'attribuzione di giurisdizione; la Francia aveva già mosso pretese, vantando di battere bandiera sul territorio marittimo greco, ma la Corte sancì l'inesistenza di norme di diritto internazionale in materia,

[445] Deeks A., *An International Legal Framework for Surveillance*, Virginia Journal of International Law, Vol 55:2.
[446] Marrella F., Carreau D., Diritto Internazionale, Giuffrè, edizione 3, 2021.
[447] Marrella F., Carreau D., Diritto Internazionale, Giuffrè, edizione 3, 2021.

conseguendone una pronuncia che diede vita ad un vero e proprio principio che sarebbe stato applicato negli anni a venire.

È proprio questo il caso del regime di spionaggio nel diritto internazionale, ravvisandosi anche qui una totale lacuna normativa che regoli l'esercizio di tali operazioni, rimettendo agli stati la discrezionalità di agire in tal senso: a conferma di ciò, la maggioranza dei governi si è espresso in senso positivo, autoregolamentandosi in termini di spionaggio, rimettendosi al mancato divieto previsto dal diritto internazionale[448].

In definitiva, gli Stati che condividono l'applicabilità del principio Lotus, sono gli stessi che ammettono di esercitare azioni di spionaggio, mostrandosi altresì contestualmente consapevoli di ricevere lo stesso trattamento dagli altri Paesi[449].

È inoltre importante sottolineare che a tal fine rileva anche la violenza con cui le azioni di spionaggio vengono esercitate.

Da accordo tacito, sarà sempre rimesso alle autorità diplomatiche il ruolo di dirimere le controversie in materia di spionaggio tra gli Stati, estromettendo del tutto le fonti di diritto internazionale[450].

Oltre alla discriminante rappresentata dalla violenza nell'esercizio delle operazioni, vi è sicuramente quella configurata dal contesto storico-politico in cui si collocano queste azioni e dunque, se si tratta di tempo di guerra ovvero di pace[451].

A tal proposito, Roger Scott tra le sue considerazioni circa la liceità dello spionaggio internazionale, asserì che in alcun modo l'esercizio di tali operazioni può violare norme di *jus cogens* e, per fornire un'argomentazione di natura legale che desse le basi per la sua tesi, citò alcune fonti di diritto internazionale, fra cui la stessa Carta delle Nazioni Unite, al fine di far rientrare le attività di spionaggio tra

[448] Deeks A., Regulating Foreign Surveillance through International Law, volume 18.
[449] Deeks A., *An International Legal Framework for Surveillance,* Virginia Journal of International Law, Vol 55:2.
[450] Milo C., *Russian Diplomatic Espionage in Italy the Biot Affair and International Law,* The italian review of international and comparative law 1 (2021) 171-180.
[451] Navarrete Mr I., Buchan R., *Out of the Legal Wilderness: Peacetime Espionage*, International Law and the Existence of Customary Exceptions, Cornell International Law Journal, Volume 51, Number 4 Winter 2019, Article 4.

i contenuti del diritto ad un'autodifesa degli Stati anticipatoria e perentoria—letteralmente *anticipatory and peremptory self-decence*[452].

Appartenente ad un filone di dottrina opposto è il pensiero di Manuel Garcia-Mora, secondo cui questa distinzione tra spionaggio in tempo di pace ed in tempo di guerra non avrebbe alcuna ratio, e rintracciando l'illegalità delle azioni in quanto lesive del diritto internazionale, nel caso di specie, lesive del dovere di non ingerenza negli affari domestici di altri Stati e di rispetto dell'integrità territoriale altrui[453].

Infine, un altro importante contributo alla dottrina relativa allo spionaggio è stato apportato da Ingrid Delupis[454], il cui pensiero si è focalizzato sui soggetti che attivamente esercitano attività di spionaggio, rimettendo all'identità di questi ultimi la discriminante per sancire l'illegalità delle stesse attività: in particolare, Delupis introduce il concetto di clandestinità, con esso facendo riferimento alle circostanze in cui ufficiali governativi vengono inviati sotto banco in altri Paesi per spiarne gli affari. Il pensiero di Delupis è, tuttavia, rimasto isolato, considerando che non è mai pervenuta una tassativa definizione di clandestinità[455].

La questione circa la liceità dello spionaggio in tempo di guerra è comunque restata un quesito aperto, che ha visto opporsi una minoranza di proibizionisti alla maggioranza dei governi, che fanno riferimento all'uguaglianza della sovranità, al principio di non intervento, alla collaborazione internazionale, all'integrità degli affari diplomatici, quali fondamenta giuridiche il cui mancato rispetto configurerebbe una violazione del diritto internazionale[456].

Un'ulteriore differenza da sottolineare al fine di ottenere un quadro completo del concetto di spionaggio è quella fra spie governative inviate per ottenere informazioni e coloro che sono ritenuti, invece, traditori del governo: ciò che li distingue, qui, non è una componente meramente personale, piuttosto si rifà allo

[452] Navarrete Mr I., Buchan R., *Out of the Legal Wilderness: Peacetime Espionage*, International Law and the Existence of Customary Exceptions, Cornell International Law Journal, Volume 51, Number 4 Winter 2019, Article 4.
[453] Radsan A. J., *The Unresolved Equation of Espionage and International Law*, Michigan Journal of International Law, Volume 28, Issue 3, 2007.
[454] Radsan A. J., *The Unresolved Equation of Espionage and International Law*, Michigan Journal of International Law, Volume 28, Issue 3, 2007.
[455] Radsan A. J., *The Unresolved Equation of Espionage and International Law*, Michigan Journal of International Law, Volume 28, Issue 3, 2007.
[456] Lubin A., *Espionage as a Sovereign Right under International Law and its Limits*, Maurer School of Law: Indiana University, 2016.

status di spia, non intesa quale risorsa umana di intelligence, ma riferendosi a fonti tecnologiche che fungono da strumenti per esercitare l'attività di spionaggio[457].

[457] Demarest G. B., *Espionage in International Law, Denver Journal of International Law & Policy*, Volume 24 Number 2 Spring, Article 4, January 1996.

3.6.1 L'impatto del Caso Snowden sul regime di spionaggio

Le rivelazioni di Edward Snowden sulle operazioni dell'intelligence americana oltre a denunciare l'ingerenza arbitraria ed indiscriminata nella vita privata dei cittadini, segnalò che lo stesso trattamento veniva riservato anche ai leader stranieri ed in generale, agli altri governi. Quest'ultimo genere di attività rientra nel regime di cui si è appena parlato, dunque lo spionaggio nel diritto internazionale.

Fu quasi fisiologico il dibattito internazionale che ne seguì, essendosi reso necessario venire a capo del quadro giuridico internazionale al fine di stabilire se effettivamente quel tipo di spionaggio fosse lecito o meno.

Ciò comportò che i soggetti interessati—individui, organizzazioni internazionali e persino il Parlamento Europeo— si esprimesse al riguardo, e venendosi a formare una moltitudine di posizioni ed opinioni circa la natura delle attività di spionaggio nel diritto internazionale; nel caso di specie, si trattò di una presa di posizione nei confronti delle azioni imputabili all'NSA[458].

Tra queste, la più importante fu senz'altro quella espressa la Consiglio per i Diritti Umani presso le Nazioni Unite che, con l'emanazione di un'importante Risoluzione, istituì per la prima volta un organismo indipendente esperto di diritto alla privacy, includendo qui anche le potenziali violazioni derivanti dal continuo sviluppo tecnologico[459].

Anche il Consiglio d'Europa si espresse attraverso una Risoluzione, con la quale condannava aspramente la sorveglianza dei dati così come adoperata dall'NSA, non curante del rispetto dei diritti fondamentali, annoverando fra questi la libertà d'espressione o il diritto alla privacy[460].

Restando nel panorama comunitario, la Commissione per le Libertà Civili, la Giustizia e gli Affari Interni (LIBE) presso il Parlamento Europeo, specificò poi che il fine per il quale l'intelligence operava, in alcun modo poteva giustificare i mezzi: la lotta al fenomeno terroristico non rappresentava una valida giustificazione

[458] Two years after Snowden: protecting human rights in an age of mass surveillance.
[459] Two years after Snowden: protecting human rights in an age of mass surveillance.
[460] Consiglio Europa condanna Datagate, Servizi Segreti violano diritti e mettono a rischio sicurezza, ANSA, 21 aprile 2015.

per realizzare violazioni di quel tipo, sviluppando ed adoperando i programmi e software di cui sopra[461].

In ultima istanza, non meno importante fu l'opinione espressa dalla collettività dei cittadini, raccolta da un Report di Amnesty International, in cui veniva chiesto a circa 150.000 persone di 13 Paesi differenti quale fosse la loro posizione in merito alle operazioni di spionaggio realizzate dai propri governi ed in secondo luogo, in merito alle attività di spionaggio dell'NSA all'indomani del polverone politico, giuridico e mediatico sollevato da Snowden[462].

In relazione alla sorveglianza interna esercitata dai propri governi, più della metà dei cittadini si mostrò contraria alle intercettazioni, raccolta, archivio dei dati e l'analisi del loro traffico Internet.

È da precisare che tra questa maggioranza rientrano soprattutto cittadini statunitensi, tedeschi, spagnoli o brasiliani, in virtù delle relative vicende passate in merito alla sorveglianza subita.

Alla domanda circa la concordanza con l'esercizio delle attività di sorveglianza esercitata dal governo americano nei confronti di altri governi, invece, il 71% dei partecipanti al Report si dichiarò nettamente contrario: la maggioranza dell'opposizione qui va riconosciuta ai cittadini tedeschi, forti della posizione assunta dal proprio governo nei confronti dell'NSA[463].

In definitiva, nonostante le svariate correnti di pensiero presenti in dottrina e le diverse posizioni assunte dai governi in merito al regime di spionaggio, quest'ultimo resterà comunque ancorato alle relazioni diplomatiche degli Stati, non essendo sufficiente il lacunoso diritto internazionale vigente in materia, configurando una delle più importanti aree grigie del diritto internazionale.

[461] NSA snooping: MEPs table proposals to protect EU citizens' privacy, News European Parliament, 2014.

[462] Two years after Snowden: protecting human rights in an age of mass surveillance.

[463] International public opinion rejects mass surveillance, Two years after Snowden: protecting human rights in an age of mass surveillance.

3.7 La reazione dell'Unione Europea al Datagate

Ad influenzare maggiormente la posizione comunitaria[464], fu senz'altro l'orientamento tedesco: nonostante il mantenimento della collaborazione con gli Alleati nella lotta al terrorismo, le proposte avanzate segnarono un'importante svolta per la disciplina del diritto alla privacy e la tutela della vita privata dalle ingerenze dei servizi segreti[465].

Di fondamentale portata fu la Risoluzione elaborata dalla Commissione Europea 2013/2683[466] nelle sedute dal 1° al 4 luglio 2013 sul programma di sorveglianza dell'Agenzia per la Sicurezza Nazionale degli Stati Uniti sugli organi di sorveglianza in diversi Stati Membri e sul loro impatto sulla vita privata dei cittadini dell'Unione Europea.

Nel caso di specie, nei suoi 17 punti, il testo sottolineava le esigenze che fino ad allora erano presenti ma rimaste latenti, soprattutto quella di mutare i meri obblighi negativi gravanti sui governi, in obblighi positivi, contemplando fra questi anche quello di garantire l'esercizio del diritto alla privacy e la relativa possibilità di ricorrere dinanzi all'autorità giudiziaria nei casi di lesione dello stesso.

Questo scenario avrebbe potuto prendere vita nel solo caso in cui fosse stato proposto un unico testo organico che, senza mezzi termini, determinasse i confini della discrezionalità statale.

Emblematici della determinatezza di quest'evoluzione sono i punti 2, 3, 4, 6[467].

Rispettivamente il testo si preoccupa di condannare apertamente "lo spionaggio ai danni delle rappresentanze dell'UE in quanto costituirebbe, qualora le informazioni ad oggi disponibili venissero confermate, una grave violazione della Convenzione

[464] Cosimi S., *La prima reazione dell'Unione Europea al Datagate*, Wired.it, 16 ottobre 2015.

[465] *Datagate: Reding, tutti con Merkel su protezione dati Ue*, ANSA, 15 luglio 2013.

[466] Risoluzione del Parlamento europeo sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sulla vita privata dei cittadini dell'Unione europea (2013/2682)(RSP).

[467] Risoluzione del Parlamento europeo sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sulla vita privata dei cittadini dell'Unione europea (2013/2682)(RSP).

di Vienna sulle relazioni diplomatiche, oltre ad avere un potenziale impatto sulle relazioni transatlantiche; esorta le autorità statunitensi a fornire immediatamente chiarimenti sulla questione".

Citando la Convenzione di Vienna, il Parlamento ha marcato il grave stato di vacillazione in cui versavano le relazioni amicali internazionali, fino a quel momento fondate su un rapporto di fiducia; seppur si sapesse che i governi esercitavano spionaggio attivo reciprocamente, mai prima d'allora vi erano state fughe di notizie così gravi da mettere in repentaglio la stabilità della collaborazione internazionale.

Al punto 3[468], la Commissione invita, poi, il governo statunitense a garantire trasparenza circa la controversia PRISM, cioè precisare in che modo il programma avesse agito e quanto gravemente l'utilizzo di quest'ultimo avesse leso la disciplina giuridica in vigore.

Si trattava di capire se—e soprattutto in che forma—quest'ingerenza avesse rispettato "le relative basi giuridiche, la loro necessità e proporzionalità, nonché le salvaguardie adottate per tutelare i diritti fondamentali dei cittadini dell'UE".

Qui la Commissione preme al fine di ribadire la priorità per la quale ci si espone in modo così netto: la garanzia dei diritti dei cittadini comunitari, per evitare che la *causa di giustificazione* della lotta al terrorismo millantata dagli USA continuasse a legittimare la collezione di dati personali dei cittadini dell'Unione Europea, anche se non ritenuti soggetti sospetti; per vietare all'intelligence di agire in nome della sicurezza pubblica, violando la sovranità internazionale.

Il punto 4 suggerisce il modus operandi da adottare per perseguire gli obiettivi che la Commissione Europea aveva proposto: la via indicata prevedeva il ricorso ad ogni strumento disponibile realizzato negli anni tra il governo americano e la Comunità Europea grazie a svariati accordi, discussioni e negoziati, arrivando ad annoverare tra gli stessi "la sospensione degli accordi relativi ai codici di

[468] Risoluzione del Parlamento europeo sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sulla vita privata dei cittadini dell'Unione europea (2013/2682) (RSP).

prenotazione PNR (Passenger Name Record) e al programma di controllo delle transazioni finanziarie dei terroristi (TFTP)"[469].

L'eventualità di sospendere un progetto come quello del PNR, se da un lato mostra la caparbietà del legislatore europeo nella sua volontà di difendere i propri cittadini, al contempo rischiava di avvantaggiare indirettamente il fenomeno terroristico quale effetto collaterale, venendo qui in rilievo—ancora una volta—la problematica controversia circa l'equilibrio tra la garanzia della sicurezza domestica ed internazionale e il diritto alla riservatezza dei singoli.

La finalità più collaborativa viene perseguita dal punto 6[470]. in cui si propone la ripresa dei negoziati tra l'Unione Europea e gli Stati Uniti, contemplando tutti gli strumenti accessibili, al fine di realizzare tutti gli obiettivi elencati nel testo.

In ultima istanza, la proposta della Commissione include l'istituzione di un organismo del tutto indipendente, della stessa natura di simili commissioni interne agli stati membri con poteri d'inchiesta, appositamente create per l'attività di controllo sui rispettivi servizi d'intelligence.

[469] Risoluzione del Parlamento europeo sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sulla vita privata dei cittadini dell'Unione europea (2013/2682)(RSP).

[470] Risoluzione del Parlamento europeo sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sulla vita privata dei cittadini dell'Unione europea (2013/2682)(RSP).

3.7.1 La sentenza *Schrems*

L'eco dell'Unione Europea, tuttavia, si fece sentire anche grazie ad un'importante pronuncia della Corte di Giustizia dell'Unione, con la quale si poneva in serio dubbio la validità del Safe Harbour[471], l'accordo commerciale stipulato fra Unione Europea e Stati Uniti, la cui invalidità—qualora confermata— avrebbe rischiato di vanificare ogni collaborazione transatlantica commerciale, con cui le aziende statunitensi, con particolare riferimento ai colossi della Silicon Valley, potevano avere accesso ai dati personali dei cittadini comunitari e la facoltà di trasferirli negli Stati Uniti.

Alla sentenza della Corte di Giustizia dell'Unione Europea[472] si giunse grazie al ricorso di un cittadino europeo, Maximilian Schrems, il quale decise di esporsi a seguito delle rivelazioni di Edward Snowden circa l'utilizzo dei dati personali che gli Stati Uniti facevano nei confronti dei cittadini europei, con particolare riferimento alla National Security Agency[473].

Il ragazzo austriaco lamentò una controversia contro Facebook, presentando denuncia alla filiale principale del colosso presente in Irlanda, il cui contenuto segnalava l'illegittimo trasferimento dei propri dati agli Stati Uniti, evidenziando la mancata garanzia da parte delle autorità americane circa la protezione assicurata alla collezione dei dati personali.

La denuncia ebbe per riscontro un mero diniego da parte delle autorità irlandesi dell'utilizzo arbitrario di quei dati, giustificando la stessa risposta allegando una decisione della Commissione Europea risalente al 26 luglio 2000[474], nella quale si sanciva un certo regime di protezione dei dati personali da parte degli Stati Uniti, a tal proposito definiti un "porto sicuro".

---

[471] Natali T., *Cos'è il Safe Harbour, l'accordo per la protezione dei dati online?,* Eu news, 1 febbraio 2016.

[472] Judgement of The Court, Grand Chamber, 6 October 2015, n Case C-362/14, Request for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014.

[473]Ressese P., *Gli Usa non garantiscono la protezione dei dati personali. Da Ue si può bloccare il trasferimento*, Eu news, 6 ottobre 2015.

[474] 2000/518/CE: Decisione della Commissione, del 26 luglio 2000, riguardante l'adeguatezza della protezione dei dati personali in Svizzera a norma della direttiva 95/46/CE

La vicenda giudiziaria non soffrì una battuta d'arresto, giacché si giunse dinanzi al giudice europeo che ribaltò quanto sancito fino ad allora, asserendo che "l'esistenza di una decisione della Commissione che dichiara che un paese terzo garantisce un livello di protezione adeguato dei dati personali trasferiti, non può sopprimere e neppure ridurre i poteri di cui dispongono le autorità nazionali di controllo in forza della Carta dei Diritti fondamentali dell'Unione Europea[475]".

La sentenza precisa la differenza tra il modus operandi relativo alla disciplina applicabile alle aziende americane, e quella prevista per le restanti autorità pubbliche, fra cui proprio i servizi dell'intelligence.

Da questa scissione deriva che il trattamento dei dati personali ed il trasferimento degli stessi da Paesi terzi agli Stati Uniti è sottoposto ad un regime ben più stringente per le autorità pubbliche dopo il caso Snowden, ma nulla riguardando le singole aziende come Facebook, citato in giudizio. Gli Stati Uniti, dunque, a seguito della sentenza Schrems, non furono più il porto sicuro di cui si vantò il rappresentante della filiale irlandese.

La Corte di Giustizia, correggendo il disposto della decisione del 26 luglio del 2000 della Commissione, nella parte in cui priva le autorità nazionali del controllo dei loro poteri, sancisce l'invalidità della stessa decisione,[476] con un rimprovero all'operato della Commissione, la quale non avrebbe avuto competenza alcuna di disporre una decisione che privasse gli Stati Membri della facoltà di controllare gli enti domestici.

Ciò comportò che le autorità nazionali fossero definitivamente dichiarate competenti per trattare nel merito il trasferimento dei dati europei nei Paesi extra-UE—ricomprendendo l'autorità giudiziaria irlandese—e la conseguente dichiarazione di invalidità dell'accordo Safe Harbour[477].

---

[475] Judgement of The Court, Grand Chamber, 6 October 2015, in Case C-362/14, Request for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014.

[476] Caso Shrems: la Corte di Giustizia dell'Unione Europea invalida la decisione della Commissione sull'adeguatezza della protezione fornita dallo 'scudo UE-USA per la privacy', Data Protection Law, 27 luglio 2020.

[477] Ressese P., *Gli Usa non garantiscono la protezione dei dati personali. Da Ue si può bloccare il trasferimento*, Eu news, 6 ottobre 2015.

3.8 Il fenomeno del whistleblowing e le Whistleblower Protection Measures

Con lo scandalo del Datagate furono molti di più i *whistleblowers* che uscirono allo scoperto, forti degli esempi di Julian Assange e Edward Snowden che crearono dei precedenti.

I "segnalanti" divennero una fonte sempre più preziosa di informazioni relative alle condotte delle aziende private e delle autorità pubbliche che, d'altro canto, rischiavano di restare oggetto di pesanti ripercussioni da parte del datore di lavoro e privi di tutela.

Nel nostro sistema legislativo il fenomeno del whistleblowing era già stato definito e codificato con la legge 90/2012—quindi già prima dello scandalo del Datagate—rifacendosi all'art.54 bis del Decreto Legislativo 30 marzo 2001 n°165[478], poi modificato dalla Legge 179/2017[479].

Ma questo testo rischiava di rimanere una mera eccezione del panorama comunitario.

Il legislatore europeo si preoccupò[480], dunque, di redigere un testo che rispondesse a queste esigenze: la Direttiva 2019/1937[481] sulla "protezione delle persone che segnalano violazioni del diritto dell'Unione Europea", volta ad armonizzare la regolamentazione in tema di whistleblowing per tutti Paesi Membri ed entrata ufficialmente in vigore il 17 dicembre 2021[482].

Il contenuto della Direttiva circoscrive chirurgicamente i limiti dell'ambito d'applicazione della disciplina in questione, ricomprendendo quindi, solo alcune

[478] Decreto Legislativo 30 marzo 2001, n. 165, Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, vigente al: 8-11-2017.
[479] Legge 30 novembre 2017, n. 179, Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarita' di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato, entrata in vigore del provvedimento: 29/12/2017.

[480] Yurttagul H., *Whistleblower protection by the Council of Europe, the European Court of Human Rights and the European Union: an emerging consensus*, Springer, 2021.
[481] Direttiva UE 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.
[482] *La Direttiva UE sul Whistleblowing*, Integrity Line, 22 aprile 2022.

condotte che configurano illeciti nell'ambito di aziende private o autorità pubbliche (esempi più emblematici sono i reati contro il consumatore o la frode fiscale).
Tuttavia, il legislatore ha rimesso, come sempre, un'ampia discrezionalità ai Membri, consentendo loro di annoverare fra gli illeciti suindicati ulteriori condotte non espressamente contemplate nel testo, cosicché potessero estendere l'ambito oggettivo e soggettivo d'applicazione[483].
Per quanto attiene quest'ultimo, si parla dei destinatari della Direttiva elencando le aziende con più di 50 dipendenti, le autorità pubbliche ed i Comuni con più di 10.000 abitanti.
Si parla di estensione anche soggettiva poiché diversi potrebbero essere i soggetti attivamente legittimati a ricorrere invocando la Direttiva sulla protezione dei whistleblower.
Il fulcro del testo rimane, comunque, la liceità del trattamento dei dati personali e, in particolare, stabilire i casi in cui quest'ultima viene a mancare[484].
Ai sensi della Direttiva Europea, a giustificare il trattamento dei dati sarebbero solo due circostanze: l'adempimento di un obbligo legale ovvero l'esercizio del trattamento ai sensi di un interesse legittimo del datore di lavoro.
Il disposto del testo rischia, però, di scontarsi con una normativa ben più completa ed importante per il diritto alla privacy: il Regolamento Europeo sulla Protezione dei Dati Personali (GDPR)[485].
Come si precisava nel secondo capitolo, il GDPR suddivide i dati personali in categorie, rintracciando anche dei dati speciali, come i dati sanitari o biometrici.
Spetterà dunque alle autorità adibite alle segnalazioni da parte dei whistleblower un'attenta analisi al fine di stabilire se vi sia stata effettivamente una lesione della protezione dei dati personali e, soprattutto, di quali dati.

[483] Saetta B., *Whistleblowing e privacy*, Protezione Dati Personali, 29 dicembre 2021.
[484] *Committing to Effective Whistleblower Protection*, Organisation for Economic Co-operation and Development, OECD Publishing, 2016.
[485] Regolamento UE 2016/679 del Parlamento Europeo e del consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

Viene rimessa al singolo segnalante la facoltà di rivelare la propria identità o restare nell'anonimato a seguito della fuga di notizie[486]; a quest'ultimo spetta altresì la facoltà di scegliere la modalità con cui esercitare il whistleblowing, essendo lecita sia la forma orale che quella scritta[487].

In ogni caso, dopo la segnalazione, la regolamentazione prevede che si invii una notifica di ricevimento al segnalante ed al segnalato, cosicché entrambi, in particolare il secondo, siano nelle condizioni per poter esercitare il diritto di difesa personale, assicurando sempre il rispetto dei principi di lealtà e trasparenza, fornendo un congruo termine temporale[488].

Le forme di protezione dei whistleblower, anche dette Whistleblower Protection Measures[489], restano ad oggi ancora poco sviluppate, nonostante il termine disposto dal legislatore europeo fissato per la fine del 2021 al fine di integrare la disciplina negli ordinamenti domestici.

Solo 12 Membri, infatti, si sono mobilitati in tal senso, nonostante altri quadri giuridici non siano del tutto privi di tutele, seppur minime, dei segnalanti, come nel caso italiano[490].

[486]Direttiva UE 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.
[487] Mechtenberg L., Muehlheusser G., Gerd R.A., *Whistleblower protection: Theory and experimental evidence*, European economic review, 2020.
[488] Direttiva UE 2019/1937 del Parlamento Europeo e del consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.
[489] Murray J., *Whistleblower Laws: What You Need to Know, How the Whistleblower Law Protection Process Works*, The Balance Small Business, 29 aprile 2021.
[490] *La Direttiva UE sul Whistleblowing*, Integrity Line, 22 aprile 2022.

3.8 Conclusione

Si è analizzato qui il quadro giuridico e la sua mutazione a seguito del caso Snowden, non soltanto in riferimento agli Stati Uniti, direttamente colpiti dalle gravi accuse, ma anche in relazione al riscontro politico, commerciale e legislativo proveniente dal versante Europeo.

All'indomani delle rivelazioni dell'ex contractor dell'NSA, dunque, si è iniziato a scrivere una nuova e decisiva pagina del diritto alla privacy, ancora in continua evoluzione, ma sempre più significativa delle preoccupazioni dimostrate dai diversi governi vittime dell'ingerenza statunitense.

CONCLUSIONI

L'elaborato di cui sopra ha voluto tentare di districare la problematica questione dell'equilibrio tra diritto di sorveglianza degli Stati finalizzato alla garanzia della sicurezza nazionale ed il diritto alla privacy dei singoli.

L'analisi conclusiva che si può effettuare in ultima istanza è che, in realtà, uno dei due interessi sarà sempre necessariamente destinato a soccombere in virtù di un altro più nobile scopo: resta, tuttavia, controverso asserire quali siano i criteri per stabilire la prevalenza di un diritto su un altro e le ragioni che lo giustifichino.

È fuori dubbio che il legislatore debba garantire la tutela dei diritti fondamentali, ma vi è una domanda che continua a non trovare risposta: è più urgente la libertà di vivere la propria riservatezza o quella di monitorare ogni corrispondenza per il bene comune?

E ancora, a quanta libertà si è disposti a rinunciare in cambio di una protezione più garantista e ramificata?

Il diritto internazionale si è preoccupato di tutelare la privacy dei singoli, ma dalle stesse fonti che riconoscono il diritto alla vita privata, si evince la facoltà rimessa agli Stati di esercitare attività di sorveglianza se non, addirittura, spionaggio. Si tratta di facoltà non sempre espressamente conferite: lo spionaggio, in particolare, è ad oggi un'area grigia del diritto internazionale, blandamente regolamentata da principi pacificamente riconosciuti.

Ciò implica che i Governi continueranno ad intercettare e decriptare la corrispondenza, anche estera, consci di subire un reciproco trattamento, che mai verrà punito, a meno che quest'ultimo non venga denunciato e presenti connotati di una violazione di un diritto interno.

L'impossibilità di giungere al giusto compromesso tra i due interessi di cui sopra, è stata evidenziata dal caso Snowden, grazie al quale milioni e milioni di utenti hanno scoperto di non poter continuare ad utilizzare i propri dispositivi, senza ritrovarsi vittime di una sorveglianza di massa, mai richiesta, mai voluta, quanto meno non in quei termini, giustificata per anni dalle necessità della lotta al terrorismo.

E nonostante le dichiarazioni e le intenzioni manifestate dai portavoce della National Security Agency e dalla Presidenza Statunitense in persona sotto l'amministrazione Obama, è stato di recente accertato che le ingerenze nella vita privata da parte dell'intelligence americana sono state perpetrate e continuano, ancora oggi, a detenere il 75% dei dati appartenenti alle reti di telecomunicazioni più importanti sul territorio americano.

Il quadro giuridico internazionale continuerà ad evolversi, anche in considerazione del progressivo sviluppo tecnologico che rende necessaria la garanzia di nuove tutele e protezioni strettamente collegate alla funzionalità ed ingerenza di nuovi dispositivi, programmi e software; tuttavia, accanto all'evoluzione della cornice giuridica, vi sarà altresì un mutamento degli strumenti di *mass surveillance* nelle mani dei servizi segreti.

In virtù di queste considerazioni, l'unica soluzione astrattamente idonea ad evitare un'indiscriminata interferenza da parte delle autorità nella privacy degli individui, è quella di istruire questi ultimi in termini di conoscenze informatiche elementari, grazie alle quali decidere scientemente quali consensi rilasciare, a quali dati dare libero accesso e la distanza da mantenere dai dispositivi elettronici al fine di proteggere la propria riservatezza senza incertezze.

BIBLIOGRAFIA

Cerri A, Telecomunicazioni e diritti fondamentali, in Diritto e informatica, 1996.

ADIR, L'altro diritto, Cyber-sorveglianza e tutela della privacy dopo l'11 settembre 2001, Marika Surace, 2005. (par. 3.2.1).

Agrestino C., NSA, Datagate, sorveglianza di massa e altre storie, Inchiostro, 19 dicembre 2016.

Anon D., How cookies track you around the web and how to stop them, PRIVACY.net, February 24 2018, da privacy.net

Anthony S., How to visualize behavior tracking cookies with a Firefox add-on, Extreme Tech, July 8, 2011, da extremetech.com

App "Immuni": via libera del Garante privacy, Garante per la Protezione dei Dati Personali, 2020, da garanteprivacy.it

Rigoni A., Pegasus Spyware, il virus che infetta sistemi iOS e Android, Cyberment, da cyberment.it.

Asunción E., The business of personal data: Google, Facebook, and privacy issues in the EU and the USA, International data privacy law, 02/2017, Volume 7, Fascicolo 1.

AT&T avrebbe aiutato la NSA nella raccolta di dati e intercettazioni, informazione.it, 17 agosto 2015.

Bahmueller C. F., 1981, The National Charity Company: Jeremy Bentham's Silent Revolution, Berkeley, CA: University of California Press.

Balzamo A., Tutela della Sicurezza Pubblica vs Tutela della Privacy: un bilanciamento necessario, 30 ottobre 2020.

Bamford J., Cohen E. A., Body of Secrets: Anatomy of the Ultra Secret National Security Agency, Anchor Books, 2001.

Bauman Z., Bigo D., Esteves P., Guild E., After Snowden: Rethinking the impact of surveillance, Oxford Academic Journals, International Political Sociology, 2014.

Becker P., Development of Surveillance Technology and Risk of Abuse of Economic Information, Report, STOA, European Parliament, ottobre 1999.

Bell E., Journalism After Snowden: The Future of the Free Press in the Surveillance State, Columbia University Press, 2017.

Ben O'Neill, FISA, the NSA, and America's Secret Court System, MISES Institute, 22 febbraio 2014.

Benkler Y., La ricchezza della rete. La produzione sociale trasforma il mercato e aumenta le libertà, Università Bocconi, 2006.

Bertolone L., Lo stato di natura: il mondo preopolitico per Hobbes e Locke, Treccani, 2020.

Boak D. G., A History of U.S. Communications Security; the David G. Boak Lectures, Vol.1, 1966.

Bogard, B., The Simulation of Surveillance: Hyper Control in Telematic Societies, New York: Cambridge University Press, 1996.

Bolognini L., Pelino E., Codice privacy: tutte le novità del d.lgs. 101/2018: in vigore dal 19 settembre 2018, Civilista, Milan, Italy, 2018.

Bonfatti R., Datagate ed NSA. Tutto sullo scandalo spionaggio rivelato da Edward Snowden, ALGROUNG, Portale di Sicurezza Informatica, 30 dicembre 2013.

Bradford L., Aboy M., Liddell K., COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes, Journal of Law and the Biosciences, Volume 7, Issue 1, January-June 2020, published: 28 May 2020.

Bray R., Pretelli I., Accesso alla giustizia per vittime di violazioni di diritti fondamentali e danni socioambientali nella catena di approvvigionamento delle imprese multinazionali, 2021.

Breyer. P, Messaging and Chatcontrol, 2021

Bridle J., The Age of Surveillance Capitalism by Shoshana Zuboff review – we are the pawns, in The Guardian, 2 February 2019.

Bruder J., Maharidge D., Snowden's box: trust in the age of surveillance, Verso, 2020.

Brunon-Ernst, A. (ed.), 2012, Beyond Foucault: New Perspectives on Bentham's Panopticon, Farnham: Ashgate.

Burns T.L., The origins of the National Security Agency, United States Cryptological History, 1990.

Bygrave L.A., Docksey C., Kuner C., The EU General Data Protection Regulation (GDPR): a commentary, 2020.

Cinelli C., Sorveglianza digitale, Sicurezza nazionale e tutela dei diritti umani, in International Legal Order and Human Rights

Caggiano G., Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione.

Calder A., EU GDPR – An international guide to compliance, 2020.

Carbone M.R., Regolamento Chatcontrol ovvero la sorveglianza di massa anche in Europa, La lotta alla pedopornografia è motivo di un regolamento approvato dal Parlamento europeo, che consentirà ai provider dei servizi di messaggistica di effettuare un super controllo sul contenuto delle chat svolte sulle proprie piattaforme. Molte le critiche: primo caso di sorveglianza di massa in UE 09 Lug 2021.

Caretto G., Intercettazioni NSA: lo scandalo del Datagate dal 2013 ad oggi, Startmagazine, economia, 24 febbraio 2016.

Carro G., Masato S., Parla M.D., La privacy nella sanità, Teoria e pratica del diritto, 2018.

Caso NSA, Obama chiese chiarimenti dopo notizie su Brasile e Messico, Libero Quotidiano, 31 ottobre 2013.

Caso Shrems: la Corte di Giustizia dell'Unione Europea invalida la decisione della Commissione sull'adeguatezza della protezione fornita dallo 'scudo UE-USA per la privacy', Data Protection Law, 27 luglio 2020.

Cavallari G., Il diritto all'oblio in seguito al caso Google Spain vs. AEPD e Mario Costeja Gonzales, iusiinitenere, 2018.

Cavicchioli S., Pezzini I., La Tv verità. Da finestra sul mondo a "Panopticon", Collana Rai-VQPT n. 118, Torino, Nuova Eri, 1993.

Champs,E, de., 2015, Enlightenment and Utility: Bentham in French, Bentham in France, Cambridge: Cambridge University Press.

China: Alipay Health Code app shares data with law enforcement, Privacy International, 1st March 2020, da privacyinternational.org

Choi P., Intelligence: NSA: Washington's Best Kept Secret, Harvard International Review, 1983.

Clarcke R.A., Morell M. J., Stone R.G., Sunstein C.R., Swire P., Who guards the guardians? The NSA Report Liberty and Security in a Changing World The President's Review Group on Intelligence and Communications Technologies, Princeton University Press, 2014.

Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica, Garante per la privacy.

Colli G., Introduzione a M. Weber, L'etica protestante e lo spirito del capitalismo, Ed. Rizzoli, 1997.

Colneric. N, Legal opinion on the Chatcotrol commissioned by MEP Patrick Breyer, The Greens/ EFA Group in the European Parliament, 2021
Commission Delegated Regulation (EU) 2022/486 of 21 January 2022 amending Annexes I and III to Delegated Regulation (EU) No 906/2014 supplementing
Committing to Effective Whistleblower Protection, Organisation for Economic Co-operation and Development, OECD Publishing, 2016.

Conforti B., Focarelli C., Le Nazioni Unite, Wolters Klumer, CEDAM, dodicesima edizione, 2020, (pg.178).
Corte di Appello di New York, Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (N.Y. 1902)

Cosimi S., La prima reazione dell'Unione Europea al Datagate, Wired.it, 16 ottobre 2015.

Council of Europe Convention on the Prevention of Terrorism, Council of Europe Treaty Series - No. 196, Warsaw, 16.V.2005.

Crevier D., AI: The Tumultuous Search for Artificial Intelligence. New York, NY: BasicBooks, 1993.

Cuffo A., Snowden: "Microsoft lavorava a stretto contatto con la NSA", Panorama, Sicurezza, 12 luglio 2014.

Datagate, spiati 35 leader mondiali. La Ue: risposta forte agli Stati Uniti, Il Mattino, 24 ottobre 2013.

Datagate. Messico condanna spionaggio NSA, Blitz Quotidiano, 21 ottobre 2013.

De Felice L., Marketing conversazionale. Dialogare con i clienti attraverso i social media e il Real-Time Web di Twitter, FriendFeed, Facebook, Foursquare, 2ª ed., Milano, Il Sole 24 Ore, 2011.

De Scalzi N., Obama e la riforma NSA, Treccani, Atlante Geopolitico, 29 gennaio 2014.

De Vergottini G., La difficile convivenza tra libertà e sicurezza. La risposta delle democrazie al terrorismo, in Rassegna parlamentare, 2004.

Decreto Legislativo 30 marzo 2001, n. 165, Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, vigente al: 8-11-2017.

Deeks A., An International Legal Framework for Surveillance, Virginia Journal of International Law, Vol 55:2.

Della Morte. G, La tempesta perfetta Covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa, SIDIBlog, 2020

Demarest G. B., Espionage in International Law, Denver Journal of International Law & Policy, Volume 24 Number 2 Spring, Article 4, January 1996.

Denley, A., Foulsham M., Hitchen B., GDPR: how to achieve and maintain compliance, 2019.

Di Marco E., Un leak sul Guardian rivela l'incubo del programma Stellar Wind, AgoraVox, 8 giugno 2013.

Di Salvo. P, Whistleblowing e hacking nell'età senza segreti, Luiss University Press, 2019

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), Gazzetta Ufficiale n. L 201 del 31/07/2002.
Direttiva UE 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.

Dozier K., "NSA claims know-how to ensure no illegal spying", Associated Press, 9 giugno 2013.

Dr Reinhard Kreissl, Terrorism, mass surveillance and civil rights, www.vicesse.eu

Dujmovic N., The Significance of Walter Bedell Smith as Director of Central Intelligence, CIA History Staff, Center for the Study of Intelligence, 1950-53.

Dylan H., Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA, RUSI Journal, 03/2018, Volume 163, Fascicolo 2.

Edgar T.H., Beyond Snowden, Privacy, Mass Surveillance, and the Struggle to Reform the NSA, Brookings Institution Press, 29 agosto 2017.

Edward Snowden, 7 anni dopo i giudici gli danno ragione: "Il programma di sorveglianza della Nsa era illegale", il Fatto Quotidiano, 5 settembre 2020.

Lobina E., Il 'capitalismo della sorveglianza' agisce sui nostri desideri tramite il web. Altro che libertà in Il Fatto Quotidiano, (2020).

EU GDPR: A Pocket Guide, second edition di Calder A., 2018, 2nd edition.

EU General Data Protection Regulation (GDPR): An Implementation and compliance guide, fourth edition, di Team, IT Governance Privacy, 2020

European Data Protection Supervisor, Opinion 7/2020 on the proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online

Executive Documents, Proc. No. 7463. Declaration of National Emergency by Reason of Certain Terrorist Attacks, Proc. No. 7463, Sept. 14, 2001, 66 F.R. 48199.

Boehm F., Information sharing and data protection in the area of freedom, security and justice, Berlino, Heildemberg, 2012

Palermo F., La Riservatezza... senza riserve, Diritto pubblico comparato europeo, 2003 The Health Insurance Portability and Accounting Act (HIPAA)

The Children's Online Privacy Protection Act (COPPA)

F.P., Scandalo spyware: Onu, gli esperti chiedono una moratoria sulla vendita di tecnologie di sorveglianza in SIR Agenzia d'Informazione, (2021).

Colombo F., Il potere socievole, Bruno Mondadori Editore, (2013).

Fidler D.P., Office of the Director of National Intelligence and James R. Clapper, Director of National Intelligence, Statements on NSA Cryptological Capabilities, The Snowden Reader, Indiana University Press, 2015.

Fidler D.P., The Snowden reader, Indiana University Press, 2015.

Focarelli C., La privacy: proteggere i dati personali oggi, Universale paperbacks, Il mulino, 2015.

Fonio C., "Oltre il Panopticon? Foucault e la videosorveglianza", Jstor.

Forgang J.D., "The right of the people": the NSA, the FISA Amendments Act of 2008, and foreign intelligence surveillance of Americans overseas, Fordham Law Review, 2009.

Foucault M., Sorvegliare e punire. Nascita della prigione, traduzione di Alcesti Tarchetti, Collana Paperbacks, Torino, Einaudi, 1976,

Fowler A., The most dangerous man in the world: Julian Assange and WikiLeaks' fight for freedom, Melbourne University Press, 2020.

Francel M.T., Rubber-stamping: legislative, executive, and judicial responses to critiques of the foreign intelligence surveillance court one year after the 2013 NSA leaks, Administrative Law Review, 2014.

Friedewald M., Burgess J.P., Bellanova R., Peissl W., edited by Friedewald M., Burgess J.P., Čas J., Bellanova R., Peissl W., Surveillance, Privacy and Security, PRIO New Security Studies, 2017.

Fuchs C., Trottier D., Internet surveillance after Snowden: A critical empirical study of computer experts' attitudes on commercial and state surveillance of the Internet and social media post-Edward Snowden, Journal of Information, Communication and Ethics in Society, 23 novembre 2017.

Mirabelli G., Le posizioni soggettive nella elaborazione elettronica dei dati personali, in Diritto e informatica, 1993

Della Morte G., La tempesta perfetta Covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa in SIDIBlog, (2020).

Gavazzi L., Edward Snowden, PRISM e Datagate, le cose da sapere, Panorama, 2014.

Gawronski M., Guide to the GDPR, 2019
Gazzetta ufficiale dell'Unione europea C 326/47, Trattato sul Funzionamento dell'Unione Europea, versione consolidata, 20.10.2012.

GDPR and Biobanking, edited by Slokenberga S., Tzortzatou O., Reichel J.,

Gearan A., "'No Such Agency' spies on the communications of the world", The Washington Post, 7 giugno 2013.
Geary J., Tracking the trackers: What are cookies? An introduction to web tracking, Battle for the Internet, Cookies and web tracking, The Guardian, da theguardian.com, 2017.

Germania, Datagate: Merkel proporrà a UE la creazione di un network europeo, Notizie Geopolitiche, 16 febbraio 2014.

Giannulli. A, Come i servizi segreti usano i media, Adriano Salani Editore S.p.A. Milano, 2012

Gibson W., Neuromante (Neuromancer, 1984), Milano, Editrice Nord, 1986.

Giudici G., Dalla sorveglianza moderna alla New Surveillance. Il ruolo delle tecnologie informatiche nei nuovi metodi di controllo sociale, tratto dal Centro di documentazione su carcere, devianza, marginalità dell'Università degli Studi di Firenze, da gabriellagiudici.it, 10 ottobre 2013.

Gottlieb E., The Orwell Conundrum, LCCC Library Catalog, 1992.

Green M., Nørgaard L., Cyril B., Mette b., Birkedal B., Early Modern Privacy: Sources and Approaches, MetteIntersections, 2022.

Greenwald G., "NSA taps in to internet giants' systems to mine user data, secret files reveal", The Guardian, London, 6 giugno 2013.

Greenwald G., "The crux of the NSA story in one phrase: 'collect it all': The actual story that matters is not hard to see: the NSA is attempting to collect, monitor and store all forms of human communication" The Guardian, 15 luglio 2013.

Greenwald G., MacAskill E.,"NSA Prism program taps in to user data of Apple, Google and others"., The Guardian, 6 giugno 2013

Greenwald. G, No place to hide sotto controllo. Edward Snowden e la sorveglianza di massa, Rizzoli, 2014

Guldner J., A friend request from the NSA: how intelligence services use social network sites, International Politik, 2014.

Habermas J., The critique of reason as an unmasking of the human sciences: Michel Foucault (F. Lawrence, Trans.) in the philosophical discouse of modernity: Twelve lectures (pg. 238-265), Cambridge, MA: MIT Press, (originariamente pubblicato nel 1985), 1987.

Hallinan D., Leenes R., De Hert P., Leenes R.E., Data protection and privacy: data protection and artificial intelligence, EComputers, privacy and data protection, 2021.

Handley J., PRISM and boundless informant: is nsa surveillance a threat?, American diplomacy, 2013.

Harding L., Snowden. La vera storia dell'uomo più ricercato del mondo, Newton Compton Editori, 17 novembre 2016.

Harris D., Professor Emeritus and Co-Director Human Rights Law Centre, School of Law, University of Nottingham.

Harrison, R., 1983, Bentham, London: Routledge and Kegan Paul.

Hart, H. L. A., 1982, Essays on Bentham: Studies on Jurisprudence and Political Theory, Oxford: Clarendon.

Heembsergen L., Radical transparency and digital democracy: WikiLeaks and beyond, Emerald Publishing Limited, 2021.

Hirsh M., Isikoff M., No More Hide and Seek: Armed with secret new intelligence, including NSA intercepts, America takes the case against Saddam to the world, Newsweek global, 2003.

Homeland Security Act of 2002, Public Law 107–296—NOV. 25, 2002 116 STAT. 2135, Public Law 107–296 ,107th Congress.

How to Protect Your Privacy on Social Media?, Data Privacy Manager, 20/10/2021, in Blog, Data Privacy, da dataprivacymanager.net

Human Rights Instruments, Core Instrument, United Nations Human Rights, Office of High Commissioner.

Saliceti I., La protezione dei dati personali nell'ordine pubblico europeo: tutela della sfera privata e ingerenza dello Stato, in Informatica e diritto, 2008

Iaselli M., Sanzioni e responsabilità in ambito GDPR, Compliance, 2019.
Il capitalismo industriale, La modernizzazione, DeAgostini, Sapere.it

Indrajit S., Louoie C., Beyer J.L., FISA's Section 702 & the Privacy Conundrum: Surveillance in the U.S and Globally, The Henry M. Jackson School of International Studies, University of Washington, 25 ottobre 2017.

Informativa sul trattamento dei dati personali ex art. 13 del Regolamento (UE) 2016/679, Ministero del Lavoro e delle Politiche Sociali.

International Covenant on Civil and Political Rights, 1976

Izzo L., Regolamento ChatControl: le nostre mail e conversazioni sotto controllo?, StudioCataldi.it, 27 ago 2021.
Jackson C., Ayshe Namid J., Piano di Adeguamento al Regolamento Generale Sulla Protezione dei Dati (GDPR): Guida aziendale per lavorare in conformità con i requisiti del GDPR, 2020.

Joint Resolution of November 7, 1973, Public Law 93-148, 87 STAT 555, concerning the war powers of congress and the president; 11/7/1973.

Regan J., Cosa si intende per spyware? In AVG, (2020).

Joseph S., Castan M., The International Covenantg on Civil and Political Rights: Cases, Materials and Commentary, Oxford Public International Law, 2013.

Kaplan A. M., Haenlein M., Users of the world, unite! The challenges and opportunities of social media, Business Horizons, Vol. 53, 2010.

Karlstrom E., "Stellar Wind" (NSA warrantless surveillance program begun under Pres. G. W. Bush's President's Surveillance Program (PSP), Gang Stalking, Mind Control, and Cults, Exposing and Defeating Organized Gang Stalking, Mind Control, and Cults, 27 febbraio 2019.

Katz E., Mass Media Effects. In International Encyclopedia of Communications, vol. 2. New York, Oxford University Press, 1989, pp. 492-497.

Kenyon A., Richardson M., New Dimensions in Privacy Law: International and Comparative Law, edited by Kenyon, Andrew T; Richardson M., 2006.

Carboni K., L'azienda che ha sviluppato lo spyware Pegasus è finita nella lista nera degli Stati Uniti,Wired, 2021.

Key Social Media Privacy Issues for 2020, Tulane University, School of Professional Advancement, 2020.

Kirwan M., Mee B.,Clarke N., Tanaka A., Manaloto L., Halpin E.,Gibbons U., Cullen,A., McGarrigle S., Connolly E.B., Bennett K., Gaffney E., Flanagan C., Tier L., Flavin R., McElvaney N.G., What GDPR and the Health Research Regulations (HRRs) mean for Ireland: a research perspective, Irish journal of medical science, 7/2020, Volume 190, Fascicolo 2.

Krzysztofek M., GDPR: General Data Protection Regulation (EU) 2016/679Post-Reform Personal Data Protection Regulation EU 2016/679, 2018.

Kuntze J., The abolishment of the right to privacy?: the USA, mass surveillance and the spiral model, 2018.

Mormile L., Trattamento dei dati personali per finalità pubbliche: il giudice del rinvio arbitro di un difficile bilanciamento, 2003.

La Direttiva UE sul Whistleblowing, Integrity Line, 22 aprile 2022.

La tutela dei dati personali: commentario alla L. 675/1996
Article 8 (right to respect for private and family life, home, and correspondence) of the European Convention on Human Rights

Lagasnerie G., The art of revolt: Snowden, Assange, Manning, Stanford University Press, 2017.

Lanier. J, Dieci ragioni per cancellare subito i tuoi account social, Il Saggiatore, 2018 Lyon. D, La cultura della sorveglianza. Come la società del controllo ci ha reso tutti controllori, Luiss University Press, 2020

Lawner K. J., Post-Sept. 11th International Surveillance Activity - A Failure of Intelligence: The Echelon Interception System & the Fundamental Right to Privacy in Europe, 14 Pace Int'l, (2002).

Laybats C., Davies J., GDPR: Implementing the regulations, Business information review, 06/2018, Volume 35, Fascicolo 2.

Legge 30 novembre 2017, n. 179, Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarita' di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato, entrata in vigore del provvedimento: 29/12/2017.

Leigh D., Harding L., Pilkington E., Booth R., Arthur C., Wikileaks: inside Julian Assange's war on secrecy, Guardian nooks, 2011.

Lemma V., COVID-19: il trattamento dei dati sanitari tra privacy e interesse pubblico, 8 giugno 2020, OMAR osservatorio malattie rare, da osservatoriomalattierare.it

Licata, Spyware e tecnologie di sorveglianza, l'Onu: "Stop alla vendita, servono regole", 12/08/2021, da corrierecomunicazioni.it.

Lombardi C., Edward Snowden ha ottenuto il permesso di residenza permanente in Russia, Wired.it, 26 ottobre 2020.

Lubin A., Espionage as a Sovereign Right under International Law and its Limits, Maurer School of Law: Indiana University, 2016.

Zaninello L., Pegasus: lo spyware che sorveglia politici, giornalisti e attivisti dal 2016, 19/07/2021, da tomshw.it.

Mastrodonato L., Contro gli spyware qualcosa si muove in Europa e all'Onu in WIRED, (2021).

Lyon D., L'occhio elettronico. Privacy e filosofia della sorveglianza, Milano, Feltrinelli, 1997.

Lyon D., La cultura della sorveglianza, come la società del controllo ci ha reso tutti controllori, introduzione di Gabriele Balbi e Philip Di Salvo, traduzione di Chiara Veltri, Luiss Guido University Press, 2018.

Lyon D., La società sorvegliata. Tecnologie di controllo della vita quotidiana, con prefazione di Stefano Rodotà, Milano, Feltrinelli, 2002.

Lyon. D, La società sorvegliata. Tecnologie di controllo della vita quotidiana, Feltrinelli, 2003

Bonfanti M.E., Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti, 2011

Manuel E., William G., L'uomo che inventò lo Sprawl, 17/03/2021, da tomshw.com.

Marchetti R., Mulas R., Cyber Security Hacker, terroristi, spie e le nuove minacce del web, 2017, Luiss University Press.

Martorana M., Barberisi A., Pizzetti F., GDPR e Decreto Legislativo 101/2018, 2019.

Marx K., Engels F., Il Capitale (Das Kapital), 1ª ed. Original 1867, 1885, 1894 1ª ed. Italiana 1886.

McCarthy T., The critique of impure reason: Foucault and the Frankfurt School. In Ideals and illusions: On reconstruction and deconstruction in contemporary critical theory (pp. 43-75), Cambridge, MA: MIT Press., 1991.

McCorduck P.,Machines ,Who Think (2nd ed.), Natick, MA: A. K. Peters, Ltd, 2004.

McLaughlin J., NSA intelligence-gathering programs keep us safe, The Washington Post, 2014.

Mechtenberg L., Muehlheusser G., Gerd R.A., Whistleblower protection: Theory and experimental evidence, European economic review, 2020.

Meyers J., Orwell, EBSCO E-Book, 2010.

O'Flaherty M., Freedom of Expression: Article 19 of the International Covenant on Civil and Political Rights and the Human Rights Committee's, General Comment No 34, Human Rights Law Review, Volume 12, Issue 4, December 2012, Pages 627–654, Published: 12 December 2012.

Miller J., The passion of Michel Foucault. New York: Doubleday, 1993.

Miller R. A., Privacy and power: a transatlantic dialogue in the shadow of the NSA-affair, Washington and Lee University, Virginia, Cambridge University Press, 2017.

Milo C., Russian Diplomatic Espionage in Italy the Biot Affair and International Law, The italian review of international and comparative law 1 (2021) 171-180.

Moretti S., La Convenzione Europea dei Diritti dell'Uomo compie 70 anni, Questione di Giustizia, 2020.

Mosca G., Datagate, AT&T ha aiutato l'Nsa a controllare il traffico internet, Wired.it, 17 agosto 2015.

Moss J., Wilson G., "1984" in Literature and Its Times, GVRL E-book, 1997.

Mozur P., Zhong R., Krolik A., In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags, The New York Times, published March 1, 2020, updated July 26, 2021, da nytimes.com

Munro I., Whistleblowing and the politics of truth: Mobilizing 'truth games' in the WikiLeaks case, SAGE journals, 16 dicembre 2016.

Murray J., Whistleblower Laws: What You Need to Know, How the Whistleblower Law Protection Process Works, The Balance Small Business, 29 aprile 2021.

Nakashima E., "Bush Order Expands Network Monitoring: Intelligence Agencies to Track Intrusions", The Washington Post., 26 gennaio 2008.

Nascimbene B., Unione europea: trattati, L'Europa in movimento, 2017, Quarta edizione.

Natali T., Cos'è il Safe Harbour, l'accordo per la protezione dei dati online?, Eu news, 1 febbraio 2016.

National Security Agency and the U.S. Department of Homeland Security Form New Partnership to Increase National Focus on Cyber Security Education", NSA Public and Media Affairs, 22 aprile 2004.

National Security Agency/Central Security Center, nsa.gov.

Naughton J., 'The goal is to automate us': welcome to the age of surveillance capitalism, in The Observer, 20 January 2019.

Navacci M., Regolamento chatcontrol, cosa prevede e perché rischia di violare i diritti privacy, In votazione al Parlamento europeo il regolamento chatcontrol, che prevede una deroga alla Direttiva ePrivacy al fine di consentire ai provider di controllare i messaggi che transitano sulle piattaforme per individuare contenuti pedopornografici: un obiettivo lodevole, ma che mina i diritti di tutti gli europei, 6 luglio 2021.

Navarrete Mr I., Buchan R., Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions, Cornell International Law Journal, Volume 51, Number 4 Winter 2019, Article 4.

Newport F., Americans Disapprove of Government Surveillance Programs, 12 giugno 2013.

Nixon Library, War Powers Resolution of 1973 July 27, 2021, da nixonlibrary.gov.

Notaro S., Le novità del Regolamento Europeo "ChatControl, 27 settembre 2021, e-lex.it.

NSO Group, Cyber intelligence for global security and stability, About Us, da nsogroup.com.

Occhipinti S., App Immuni, via libera dal Garante della privacy, IP, IT e Data Protection, Altalex,da altalex.com, 2020.

Orizzonti Politici, Organizzazione delle Nazioni Unite (ONU), Eleonora Ferrari, 16 luglio 2020.

Orlowski J., The Social Dilemma, 2020.

Orwell G., 1984, Foreward by Thomas Pynchon, Afterword by Erich Fromm, 1948, Mondadori.

Paccagnella L., Sociologia della Comunicazione, Bologna, Il Mulino, 2010, p. 84.

Palombino F.M., Introduzione al diritto internazionale, GLF Editori Laterza, 2019.

Panetta A., Iannini A., Alpa G., Circolazione e protezione dei dati personali, tra libertà e regole del mercato: commentario al Regolamento UE n. 2016/679, 2019.

Panetta A., Iannini A., Alpa G., Circolazione e protezione dei dati personali, tra libertà e regole del mercato: commentario al Regolamento UE n. 2016/679, 2019.

Pecere P., L'età del capitalismo della sorveglianza in Il Tascabile, (2020)
Pegasus. La Francia apre un'inchiesta, in Messico spiato anche il presidente

Pelino E., Alagna I., Bolognini L., Codice della disciplina privacy, Codici commentati Giuffrè, 2019.

Pelino E., Alagna I., Bolognini L., Codice della disciplina privacy, Codici commentati Giuffrè, 2019.

Pellicani L., La genesi del capitalismo e le origini della modernità, Soveria Mannelli (CZ), Rubbettino Editore, 2013 (I Ed., 1988).

Peonidis, F., 2009, "Bentham and the Greek Revolution: New evidence", Journal of Bentham Studies.

Perspectives on Privacy: Increasing Regulation in the USA, Canada, Australia and European Countries, 2015, edited by Dieter D., Russell L., Weaver Perspectives on Privacy: Increasing Regulation in the USA, online information review, 06/2015, Volume 39, Fascicolo 3.

Pividori, Competenza Rationae Materiae, Dossier: la Corte Penale Internazionale, Centro di Ateneo per I Diritti Umani "Antonio Papisca", Universita degli Studi di Padova.

Pocar F., Baruffi M.C., Commentario breve ai trattati dell'Unione Europea, Breviaria juris, 2014, 2. ed.
Protocolo Facultativo ao Pacto Internacional sobre os Direitos Civis e Politicos, dhnet.org.

Punto Informatico, App Immuni: così controlleremo il contagio (2021).

Radsan A. J., The Unresolved Equation of Espionage and International Law, Michigan Journal of International Law, Volume 28, Issue 3, 2007.

Rafter D., Tracking cookies: What are tracking cookies and how do they work?, NortonLifeLock, May 6, 2021, Privacy, Norton, da us.norton.com

Reese S.D., The Framing Project: A Bridging Model for Media Research Revisited, in Journal of Communication, 57, 2007, pp. 148-154.

Regolamento Chatcontrol, l'UE verso la sorveglianza di massa per prevenire la pedopornografia, 2 Ago 2021.

Regolamento UE 2016/679 del Parlamento Europeo e del consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

Regulation (EU) No 1306/2013 of the European Parliament and of the Council as regards the calculation methods of public intervention expenditure.

Regulation of Investigatory Powers Act 2000 UK Public General Acts, legislation.gov.uk.

Report of the Special Rapporteur on the promotion and protection of the right of freedom of opinion and expression: Surveillance and human rights, 2019
Resolution 2178, Threats to international peace and security caused by terrorist acts, Security Council Distr.: General 24 September 2014, Resolution 2178 (2014), adopted by the Security Council at its 7272nd meeting, on 24 September 2014.

Ressese P., Gli Usa non garantiscono la protezione dei dati personali. Da Ue si può bloccare il trasferimento, Eu news, 6 ottobre 2015

Resta. G, La sorveglianza elettronica di massa e il conflitto regolativo USA/UE, Romatrepress, 2019
European Court of Human Rights, case of Big Brother Watch and others v. UK, 2021

Riccio G., Scorza P., Belisario E., GDPR e normativa privacy: commentario, Commentari (IPSOA, S.p.a.), 2018.

Risen L., Poitras L., "N.S.A. Collecting Millions of Faces From Web Images", The New York Times, 31 maggio 2014.

Risen M., House Intelligence Chairman Considering NSA Reform Legislation, U.S. news & world report, 2013.

Risoluzione del Parlamento europeo sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sulla vita privata dei cittadini dell'Unione europea (2013/2682) (RSP).

Robeldo P., Edward Snowden: avere ragione, sette anni dopo, The Good Lobby, 11 settembre 2020.

Colella R., Patriot Act: il concetto di 'wartime' che schiaccia i diritti costituzionali in Il Fatto Quotidiano (2021).

Rodden J., The Cambridge Companion to George Orwell, Cambridge, UK; New York: Cambridge University Press, 2007.

Rodotà S., Tecnopolitica. La democrazia e le nuove tecnologie dell'informazione, IIa edizione Bari-Roma, Laterza, 2004.

Rorty R., Moral identity and private autonomy: The case of Foucault, in Essays on Heidegger and others. Cambridge: Cambridge University Press, 1991.

Rosenbach M., Stark H., Stock J., "Prism Exposed: Data Surveillance with Global Implications", 10 giugno 2013.

Rosenblum N., 1978, Bentham's Theory of the Modern State, Cambridge, MA: Harvard University Press.

Rodotà S., Elaboratori elettronici e controllo sociale, Bologna, 1973 A. Torre, Costituzioni e sicurezza dello stato, Rimini, 2013

Saetta B., Privacy negli Usa, Normativa, 7 Settembre 2016 Ultima modifica:4 Giugno 2021, protezionedatipersonali.it

Saetta B., Whistleblowing e privacy, Protezione Dati Personali, 29 dicembre 2021.

Sala M., Privacy: guida alla lettura del Regolamento (UE) 2016/679 sulla protezione dei dati e del Codice Privacy, 2018.

Samtani S., Kantarcioglu M., Chen H., A Multi-Disciplinary Perspective for Conducting Artificial Intelligence-enabled Privacy Analytics, 2021.

Scheuerman W.E., Whistleblowing as civil disobedience: The case of Edward Snowden, SAGE journals, 8 giugno 2014.

Schweda S., UK Surveillance Under Judicial Scrutiny: GCHQ Intelligence Sharing with NSA Contravened Human Rights, But Is Now Legal, European Data Protection law review, 2015

Semple, J., 1993, Bentham's Prison: A Study of the Panopticon Penitentiary, Oxford: Clarendon Press.

Siobhan G., "NSA killed system that sifted phone data legally", Baltimore Sun, Tribune Company (Chicago, IL), 17 maggio 2016.

Smith K. A., Mass Media and Children: Concerns about Harmful Effects Increased with Each New Medium. In History of Mass Media in the United States: An Encyclopedia, 1998, pp. 349-350.

Snowden E. J., Permanent Record, Pan Macmillan, pubblicato il 17 settembre 2019, data corrispondente all'entrata in vigore della Costituzione Americana, il 17 settembre 1787.

Snowden, Nsa fa spionaggio industriale, Redazione ANSA, 26 gennaio 2014.

Soffientini M., Caccialupi M., Privacy: protezione e trattamento dei dati, PSOA Manuali, 2018.

Solanas A., Martínez-Ballesté A., Advances in artificial intelligence for privacy protection and security, Intelligent information systems, 2010.

Solombrino E., La app Immuni vista dal lato della privacy, Privacy, Risk Management360, Network Digital 360, 21 settembre 2021, da riskmanagement360.it

Starnoni, A., Chatcontrol, nel 2022 la decisione definitiva dell'Ue sulla sorveglianza delle conversazioni private, Il controllo di massa delle chat per combattere gli abusi sui minori potrebbe presto diventare realtà, Mashable Italia, 9 Gennaio 2022.

Steinhoff W.R, George Orwell and the Origins of 1984, LCCC Library Category, 01/01/1975.

Stoddart J., Chan B., Joly Y., The European Union's Adequacy Approach to Privacy and International Data Sharing edited by Rothstein M., A; Knoppers B.M., The Journal of law, medicine & ethics, 03/2016, Volume 44, Fascicolo 1.

Stone. O, Snowden, 2016

Suffia G., Effetti geopolitici del Datagate: appunti e spunti per la geopolitica della sorveglianza globale, Cyberspazio e Diritto, Mucchi Editore, 2015.

Surace M., Dalla sorveglianza moderna alla New Surveillance: il ruolo delle tecnologie informatiche nei nuovi metodi di controllo sociale in ADIR-L'altro diritto (2005).

Tamburri D., Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation, An Information systems (Oxford), 07/2020, Volume 91.

Tan S., China's Novel Health Tracker: Green on Public Health, Red on Data Surveillance, Center for Strategic and International Studies, CSIS, May 4, 2020, da csis.org

Taylor P., A Commentary on the International Covenant on Civil and Political Rights, The UN Human Rights Committee's Monitoring of ICCPR Rights, Cambridge University Press, 2020.

Testo approvato dal Parlamento Europeo: Uso di tecnologie per il trattamento di dati personali ai fini della lotta contro gli abusi sessuali sui minori online (deroga temporanea alla Direttiva 2002/58/CE)

The History of Facebook: From BASIC to Global Giant, Brandwatch, January 25th 2019, Josh Boyd, da brandwatch.org

The New Yok Times, In Coronavirus fight, China gives citizens a Color Code with Red flags, 2021

The United States, Department of Justice: Privacy Act of 1974, Overview of the privacy Act, Updated on April 30, 2021.

The Vision, La pandemia ha giustificato nuove forme di sorveglianza di massa. Anche più di quante pensiamo, (2020).

The Wassenaar Arrangement at a Glance, Arms Control Association, Daryl Kimball, Executive Director, 2022, da armscontrol.org

Meo T., L'azienda Nso ha impedito ad alcuni clienti di usare il suo spyware Pegasus in WIRED, (2021).

Tosi E., Codice della privacy: tutela e sicurezza dei dati personali, I codici vigenti, 2018, Undicesima edizione.

Treccani, Il caso Snowden e le conseguenze diplomatiche del Datagate, Atlante Geopolitico, 2014.

Two years after Snowden: protecting human rights in an age of mass surveillance.

UE Directive 95/46 Safe Harbour European Court of Justice, Schrems decision, 2015

Universal Declaration of Human Rights, 1948

Usa, sentenza Snowden: “Dopo 7 anni mai avrei immaginato di trionfare in Usa”, Redazione Bloglive, 4 settembre 2020.

Venkataramanan N., Data privacy: principles and practice, 2017.
Viktor Orbán using NSO spyware in assault on media, data suggests, Shaun Walker in Budapest, 18/07/2021. The Guardian.

Walsh P.F., Miller S., Rethinking ‘Five Eyes’ Security Intelligence Collection Policies and Practice Post Snowden, Taylor & Francis Online, 22 gennaio 2015.

Wang J., China: The QR Code System - a battle between privacy and public interests?, Lex.Atlas: Covid-19, 6 May 2021, da lexatlas-c19.org

Wassenaar Arrangement, NTI Building a Safer World, Nuclear, Conventional Weapons and Dual-Use, 14 luglio 2020, da nti.org

Weber M., L’etica protestante e lo spirito del capitalismo (Die protestantische Ethik und der Geist des Kapitalismus), 1904-1905

What American intelligence & especially the NSA have been doing to defend the nation, Vital speeches of the day, 2006.

Wise D., "Espionage Case Pits CIA Against News Media", The Los Angeles Times, 18 maggio 1986.

Yurttagul H., Whistleblower protection by the Council of Europe, the European Court of Human Rights and the European Union: an emerging consensus, Springer, 2021.

Harari Y.H., the world after coronavirus, this storm will pass. But the choices we make now could change our lives for years to come, March 20, 2020, Financial Times.

Zacaria S., Martorana M., Sorveglianza di massa nel Regno Unito, condanna della CEDU, Uno sguardo in Europa alla luce della recente sentenza della Corte europea dei diritti dell'uomo: vittoria della privacy come diritto umano, altalex.com.

Zagrebelsky V., Chenal R., Tomasi L., Manuale dei diritti fondamentali in Europa, il Mulino, seconda edizione, 2016.

Zorzi Galgano N., Persona e mercato dei dati: riflessioni sul GDPR, Le monografie di Contratto e impresa, serie diretta da Francesco Galgano, 2019.

Zuboff S., Möllers N. e Wood D., Surveillance Capitalism: An Interview with Shoshana Zuboff, in Surveillance & Society, vol. 17, n. 1/2, 31 marzo 2019.

Zuboff. S, Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri, Luiss University Press, 2019