Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

DIRITTO DELLE NUOVE TECNOLOGIE

Ciclo XXVI

Settore Concorsuale di afferenza: IUS/20
Settore Scientifico disciplinare: 12/H3

LIBERTÀ DI ESPRESSIONE E SORVEGLIANZA GLOBALE

Presentata da: **Dott. Marco Bettoni**

Coordinatore Dottorato
Chiar.mo
Prof. Giovanni Sartor

Relatore
Chiar.mo
Prof. Giovanni Sartor

Correlatore
Chiar.mo
Prof. Giovanni Ziccardi

Esame finale anno 2014

INDICE

INDICE DELLE FIGURE

ABSTRACT

La presente tesi ha come scopo quello di individuare alcune problematiche relative all'esercizio e alla limitazione del diritto alla libertà di espressione nel contesto delle attività globali di sorveglianza e controllo delle tecnologie dell'informazione e della comunicazione. Tali attività, poste in essere da parte degli Stati e da parte degli operatori privati, sono favorite dal nebuloso rapporto tra norme di fonte pubblica, privata e informatica, e sono invece osteggiate dal ricorso, collettivo e individuale, alle possibilità offerte dalle tecnologie stesse per la conduzione di attività in anonimato e segretezza. La sorveglianza globale nel contesto delle privatizzazioni si serve del codice e dell'autonomia privata, così come la resistenza digitale ricorre alle competenze informatiche e agli spazi di autonomia d'azione dell'individuo.

In questo contesto, la garanzia dell'esistenza e dell'esercizio dei diritti fondamentali dell'individuo, tra tutti il diritto alla libertà di espressione e il diritto alla tutela della riservatezza, passa per l'adozione di tecniche e pratiche di autotutela attraverso l'utilizzo di sistemi di cifratura e comunicazioni anonime. L'individuo, in questo conflitto tecnico e sociale, si trova a dover difendere l'esercizio dei propri diritti e finanche l'adempimento ai propri doveri, quando attinenti a particolari figure professionali o sociali, quali avvocati, operatori di giustizia, giornalisti, o anche semplicemente genitori.

In conclusione dell'elaborato si propongono alcune riflessioni sulla formazione della cittadinanza e del mondo professionale, da parte dei giuristi delle nuove tecnologie, all'uso cosciente, consapevole e responsabile delle nuove tecnologie dell'informazione, con lo stimolo ad orientare altresì le proprie attività alla tutela e alla promozione dei diritti umani fondamentali, democratici, costituzionali, civili e sociali.

This thesis aims to identify some issues related to the operation and restriction of the right to freedom of expression in the context of the global surveillance and control of the Information and Communication Technologies. These activities, undertaken by the States as well as by private operators, are fostered by the nebulous relationship between public, private and code norms, and are opposed by collective and individual recourse to the possibilities offered by the technologies themselves for

the conduct of activities in anonymity and secrecy. The global surveillance in the context of privatization uses the code of private autonomy, as digital resistance uses computer skills and the degree of autonomy of action of the individuals.

In this context, the guarantee of the existence and the exercise of fundamental human rights, including the right of everyone to freedom of expression and the right to protection of privacy, through the adoption of self-defence oriented techniques and practices, such as encryption and anonymous communications. The individuals, in this conflict, both technical and social, is having to defend the exercise of their rights and even the fulfilment of their duties, when related to specific professional or social, such as lawyers, justice operators, journalists, or simply parents.

In conclusion, the elaborate propose some reflections on the formation, by the lawyers of new technologies, of the citizenship and the professionals to a conscious, aware and responsible use of new information technologies, so that they may even direct their activities to the protection and promotion of fundamental democratic, constitutional, civil and social human rights.

PREMESSA

"Una volta che abbiamo consegnato i nostri sensi e i nostri sistemi nervosi
alle manipolazioni di coloro che cercano di trarre profitti
prendendo in affitto i nostri occhi, le orecchie e i nervi,
in realtà non abbiamo più diritti.
Cedere occhi, orecchie e nervi a interessi commerciali
è come consegnare il linguaggio comune a un'azienda privata
o dare in monopolio a una società l'atmosfera terrestre"

Marshall McLuhan, Gli Strumenti del Comunicare, 1964

Questa tesi si propone di analizzare il concetto, la natura, il contenuto e i limiti del diritto alla libertà di espressione nel contesto della sorveglianza globale, intesa come complesso di attività di sorveglianza, controllo e repressione poste in essere con l'ausilio, ovvero direttamente sulle, tecnologie di telecomunicazione. La finalità è quella di evidenziare il radicale mutamento in via di accadimento, in particolare, nelle modalità di esercizio e negli strumenti di tutela, alla luce della sottile linea rossa che chi scrive ritiene colleghi tre specifici fenomeni caratterizzati da un alto tasso di interdisciplinarità tra diritto, politica, economia, tecnologie e sociologia: le privatizzazioni di beni e funzioni originariamente di pertinenza delle autorità pubbliche nel più globale contesto dei processi di globalizzazione; il ruolo normativo assunto dal codice informatico sulla scorta del rapporto tra *possibilità* e *liceità*, alla luce in particolare della legittimità dei soggetti che sono nella posizione di scrivere, diffondere o *imporre* l'architettura informatica che ne deriva; le dinamiche di sgretolamento e riaffermazione degli elementi fondanti la sovranità tradizionale dello

stato nazionale, posta in rapporto con ulteriori fonti normative extragiuridiche.

Come anche i più recenti accadimenti della cronaca stanno avendo il merito di porre in rilievo, l'elaborata disciplina normativa della materia, frutto dei processi di consacrazione nei testi costituzionali fondamentali degli Stati e delle organizzazioni regionali, e del contributo sempre crescente degli organi giurisdizionali di legittimità anche e soprattutto costituzionale, si trova di fronte un contesto sociale, economico e tecnologico in rapido mutamento. L'intima essenza dei diritti di libertà e delle loro strumentali garanzie anche giuridiche – si permetta di citare quale esempio lampante il riconoscimento sempre crescente attribuito al diritto al controllo dei propri dati personali, del quale è facilmente sostenibile la natura meramente strumentale a diritti quelli sì di natura fondamentale come il diritto alla libertà d'espressione e alla tutela della vita privata, *rectius*, della riservatezza, degli individui – risente infatti di elementi ambientali idonei a limitarne o escluderne la portata, senza alcun passaggio attraverso gli organi e le procedure, anch'esse consacrate negli stessi testi costituzionali, previsti proprio a complessiva garanzia della correttezza formale e sostanziale dei mutamenti nell'ottica della piena valorizzazione dell'individuo, tanto come singolo quanto come elemento di strutturati e interdipendenti rapporti sociali.

"La società non esiste", un'affermazione ideologica e in assoluto contrasto con tutti i principi fondanti l'organizzazione sociale attraverso lo strumento più efficace che la specie umana ha avuto modo di inventare, il diritto, è un riscontro che la realtà contemporanea ci pone dinnanzi agli occhi con frequenza quotidiana. Applicando infatti quest'affermazione ai rapporti di comunicazione tra gli individui attraverso le tecnologie dell'informazione e della comunicazione non si

fa altro che sottolineare l'elemento centrale del mutamento dei rapporti tra individui e poteri costituiti, così minacciando il perseguimento delle finalità anche politiche e sociali del riconoscimento, a quegli stessi individui, dei diritti fondamentali.

L'obiettivo di questa tesi è modesto. Si intende in questa sede infatti accompagnare chi si accinge alla lettura all'individuazione dei rapporti stretti che intercorrono tra le dinamiche socio-economiche e tecnologiche e l'erosione dei contenuti dei diritti fondamentali fino a non molti anni fa ampiamente riconosciuti e positivamente rivendicati, possibilmente portando all'individuazione di alcuni errori strutturali intrapresi nell'approccio verso i rischi e le potenzialità delle nuove tecnologie, così da limitarne gli effetti negativi e ampliarne quelli positivi.

Un tale obiettivo è perseguito attraverso una strutturazione dell'elaborato in tre capitoli, dedicati rispettivamente (i) alle dinamiche evolutive della società dell'informazione, (ii) agli aspetti più strettamente giuridici relativi al patrimonio giuridico e costituzionale che accompagnano il diritto fondamentale alla libertà di espressione attraverso l'evoluzione delle tecnologie dell'informazione e della comunicazione, e infine (iii) alle pratiche di sorveglianza e di resistenza, condotte dunque su un piano del tutto extra giuridico, che caratterizzano i tempi presenti. Ancor più nel dettaglio, pur meramente introduttivo:

1) il primo capitolo di questo elaborato è dedicato a fornire al lettore gli strumenti necessari ad affrontare il resto dell'elaborato approfondendo le tre prospettive fenomeniche prima anticipate: in primo luogo, la riconducibilità dei più rilevanti fenomeni giuridici, economici e sociali quanto a normazione e *governance* delle *Information and Communication Technologies* (d'ora in avanti ICTs) alle dinamiche proprie della *privatizzazione funzionale*, affermazione questa gravida di

conseguenze non irrilevanti; in secondo luogo, l'inserimento della privatizzazione della censura nella più ampia dinamica della globalizzazione, delle sovranità regionali e locali e della perdita di effettività, quindi di rilevanza, del diritto generato dallo Stato nazionale, a vantaggio dell'affermazione di una pluralità di fonti normative autonome e alternative, pubbliche e private; infine, il delicato ruolo che la tecnologia, traino al tempo stesso di tendenze rivoluzionarie e reazionarie, ricopre nella posizione di fonte privilegiata, e certamente non neutrale né autonoma né tanto meno indipendente, di un nuovo rapporto del binomio possibilità-legittimità, determinante quanto al governo dell'agire umano e, sia ben chiaro, non limitato all'ambito dell'essere digitale. Tale approfondimento è finalizzato ad anticipare e presentare le problematiche che ne derivano in punto di esercizio e tutela del diritto alla libertà di espressione, alla luce della stretta interdipendenza dei fenomeni stessi;

2) il secondo capitolo affonda le proprie radici nella teoria costituzionale e si pone come obiettivo la ricostruzione del concetto e del contenuto del diritto alla libertà di espressione, a partire delle prime elaborazioni dottrinali e positive che hanno visto la luce nell'arco dei secoli per arrivare alle peculiarità che, in una società globale e interconnessa dove assieme allo spazio e al tempo perdono la loro tradizionale connotazione anche distinzioni ritenute oramai acquisite quale, a titolo d'esempio, la netta separazione tra diffusione e comunicazione, ne richiedono una rivisitazione sostanziale. In questa prospettiva rileva il confronto, determinato dalla dinamica globalizzante appena accennata e dal travagliato superamento della fase imperiale propria della seconda metà del secolo scorso, con ordinamenti giuridici ispirati a tradizioni culturali distinte rispetto a quelle alle quali è storicamente associato lo sviluppo e l'affermazione delle teorie dei diritti

fondamentali e dei diritti umani, categorie alle quali è ormai pacificamente ricondotto il diritto alla libertà di espressione;

3) il terzo capitolo è infine dedicato all'approfondimento dei fenomeni, perlopiù transnazionali, della sorveglianza globale e della resistenza digitale. Al primo aspetto si ricondurranno le pratiche di sorveglianza e controllo poste in essere da parte degli Stati a tradizione costituzionale e democratica, aggiornati a quanto in corso di stesura della presente tesi è stato offerto dalle rivelazioni relative al Progetto PRISM e, di grande interesse, alle reazioni istituzionali da parte in particolare degli organi europei. Al secondo aspetto invece saranno ricondotte le nuove ed eterogenee declinazioni della tradizionale etica *hacker* nel mutato e mutevole contesto contemporaneo. Questi moderni attivisti digitali, gli *hacktivists*, stimolano riflessioni sociali e giuridiche, oltre che progresso qualitativo anche informatico, costruiscono e programmano strade alternative per la circolazione dell'informazione, abbattono barriere tecnologiche e segreti istituzionali o, semplicemente, studiano l'architettura informatica che governa il mondo digitalizzato e si relazionano all'ordinamento così in via di costituzione, sulla sottile linea di demarcazione tra estremismo insurrezionalista e rivoluzione libertaria, criminalità informatica e anonimo eroismo digitale.

Alla luce di questo percorso, si proporranno alcune riflessioni sui capisaldi giuridici irrinunciabili, anche nella deriva securitaria di questo XXI secolo, della cultura e del patrimonio europeo, sul rapporto tra libertà, sicurezza, trasparenza e *privacy,* e l'apparente paradosso che sembra sottostare alla promozione delle une tramite le altre, e infinesulla formazione degli individui al ricorso cosciente e consapevole alle possibilità offerte dalle nuove tecnologie di comunicazione.

CAP I – PRIVATIZZAZIONE DELLA CENSURA E SORVEGLIANZA GLOBALE

SOMMARIO: 1. Libertà come conflitto. - 2. Le dinamiche della società dell'informazione e l'*État de droit*. - 3. Sorveglianza, controllo e repressione nel contesto delle privatizzazioni. - 3.1. *Multistakeholder Internet governance model*. - 3.2. (segue) il ruolo degli *Internet Service Providers*. - 3.3. Delega e appropriazione di funzioni pubbliche. - 3.4. Un esempio dalla materialità: la privatizzazione della "piazza" negli USA - 4. Legittimo o possibile: la tecnologia, l'esercizio di diritti e la sorveglianza globale. - 4.1. *Ad impossibilia nemo tenetur* – 4.2. Diritto ed evoluzione tecnologica – 4.3. Diritto e *Liberation Technologies* (rinvio) – 5. Globalizzazione, pluralità delle fonti ed effettività del diritto.

1. Libertà come conflitto

La libertà di espressione affonda le proprie radici nello sviluppo e all'affinamento dell'umana capacità di comunicare attraverso un linguaggio proprio e i più svariati media disponibili nelle diverse epoche storiche. La lunga strada percorsa è ben più consistente del solo aspetto temporale, posto che la comunicazione articolata si è evoluta da qualità propria e distintiva dell'essere umano, oggetto di studio delle scienze antropologiche, a istituto formalizzato del diritto positivo e al tempo stesso rivendicazione politica di un particolare spazio di libertà

individuale e collettiva meritevole di tutela rispetto a ingerenze esterne e garanzia di concrete possibilità di esercizio.

Questa evoluzione è stata all'insegna di conflitti e tensioni non indolori tra diverse istanze che non possono che essere contestualizzate nel periodo storico di riferimento, alla luce dei rapporti sociali e politici vigenti, degli strumenti tecnici disponibili, delle esigenze proprie di individui e gruppi sociali che in quel determinato contesto operano. Risulta però evidente che le potenzialità destabilizzanti dell'ordine politico, sociale ed economico costituito che derivano dal riconoscimento di una generica e universale libertà di esprimere, comunicare, diffondere un pensiero pongano quest'ultima in posizione di conflittualità, aperta o latente, nei confronti delle istituzioni proprie di quell'ordine considerato. Il conflitto tra libertà e autorità sul piano della regolamentazione dell'espressione assume in primo luogo la portata di un conflitto tra istanze reazionarie e conservatrici e istanze rivoluzionarie e riformatrici. Le prime portate avanti da chi, "Papa o Imperatore", detentore di posizioni di potere e dominio, intendeva affermare o estendere i confini di questa supremazia; le seconde erano avanzate da chi, al contrario, tali posizioni intendeva abolirle, ovvero farle proprie, oppure ancora, più semplicemente, limitarle.

Una volta acquisito il valore fondamentale del diritto alla libertà d'espressione, la linea Maginot del conflitto è stata spostata sul piano dell'individuazione delle sue limitazioni, nel rapporto con gli interessi degli Stati e delle Istituzioni. Queste limitazioni alla libertà di espressione a tutela dell'ordine vigente hanno assunto nel tempo e assumono tuttora nei diversi ordinamenti le forme della tutela della sicurezza nazionale, dell'ordine pubblico, socio-economico, politico o religioso. Solo in un momento successivo infatti la portata conflittuale si estenderà alle dinamiche dei rapporti tra libertà distinte, ben riassunte

nella statuizione generale contenuta nell'art. 4 della Dichiarazione dei Diritti dell'Uomo e del Cittadino del 1789, pietra angolare di qualsivoglia discorso sul bilanciamento dei diritti, ove si afferma che

> La libertà consiste nel poter fare tutto ciò che non nuoce ad altri; cosi l'esistenza dei diritti naturali di ciascun uomo non ha altri limiti che quelli che assicurano agli altri membri della società il godimento di questi stessi diritti.[1]

Il riconoscimento di nuovi e diversi diritti, anche di libertà, individuali e collettivi ha generato un numero sempre maggiore di potenziali conflitti, tali quelli che oggi investono il rapporto tra libertà di espressione e proprietà intellettuale, dignità personale, tutela dei minori e delle minoranze. Con lo sviluppo e la diffusione delle tecnologie dell'informazione e della comunicazione, tra le quali spicca in posizione preminente *Internet*, i conflitti tra diritto alla libertà d'espressione e altri diritti o interessi hanno raggiunto picchi qualitativi e quantitativi ancora più elevati, proprio in ragione dell'accresciuta portata territoriale e temporale delle comunicazioni, ora globali e immediate. L'adozione di un linguaggio di rappresentazione e di sistemi di telecomunicazione

---

[1] Il testo integrale in lingua italiana è disponibile all'indirizzo: http://www.dircost.unito.it/cs/docs/francia1789.htm (verificato il 12.05.2014). Il testo originale in lingua francese, che recita "*La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres Membres de la Société, la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la Loi*.", è disponibile sul sito dell'Assemblée Nationale francese all'indirizzo http://www.assemblee-nationale.fr/histoire/dudh/1789.asp (verificato il 12.05.2014)

digitali, caratterizzati da una pervasiva diffusività e da una sostanziale immediatezza temporale, ha spalancato le porte al superamento delle barriere naturalistiche che per secoli hanno scandito temporalmente e spazialmente le comunicazioni a distanza, determinando una crescita esponenziale della circolazione delle informazioni. Alla luce di questa evoluzione anche i diritti e le libertà hanno trovato terreno fertile per una declinazione in senso digitale: le ICTs sono infatti al tempo stesso luogo virtuale di applicazione di diritti tradizionali con modalità e forme peculiari e luogo di declinazione di tali diritti in autonomi istituti propri, e talvolta esclusivi, della virtualità. Sarà sulla scorta di questo significato duale che si approfondirà, successivamente, il rapporto tra diritti e libertà nel contesto digitale, anche alla luce delle richieste di nuovi processi di riconoscimento costituzionale invocate specificamente nei confronti del ciberspazio.

L'assunto fondamentale per comprendere le problematiche relative alla libertà d'espressione nel contesto digitale è dunque l'affermazione della conflittualità che necessariamente deriva dal suo riconoscimento verso non solamente qualsivoglia forma di autorità e di esercizio di potere, sia esso legittimo o illegittimo, politico, economico o religioso, ma anche verso gli altri diritti e libertà fondamentali stesse. L'art. 19 della Dichiarazione Universale dei Diritti dell'Uomo del 1948[2] ben distingue i due fronti problematici ove, nello stabilire che le eventuali limitazioni devono essere poste per legge e devono essere finalizzare alla

[2] Il testo integrale dell'art. 19 della Dichiarazione, disponibile all'indirizzo http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/itn.pdf (verificato il 12.05.2014), recita "Ogni individuo ha diritto alla libertà di opinione e di espressione incluso il diritto di non essere molestato per la propria opinione e quello di cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo a frontiere".

tutela “dei diritti e della reputazione altrui”, ovvero alla tutela “della sicurezza nazionale, dell'ordine pubblico, della sanità o della morale pubbliche”. La conflittualità intrinseca al diritto alla libertà di espressione rileva al punto che quand'anche si intendano affrontare gli specifici conflitti, adoperandosi nel tentativo di elaborare un più equilibrato compromesso ispirato al bilanciamento tra la libertà di espressione e, a titolo d'esempio, la tutela della proprietà intellettuale ovvero il perseguimento della politica criminale a tutela delle dignità dell'onore e della dignità della persone, non è possibile in alcun modo prescindere dalla presa in considerazione delle ricadute quanto a questa peculiare caratteristica. Qualsiasi limitazione della libertà di espressione non può assumere portata tale da escludere gli spazi di critica e conflitto, senza i quali non si potrebbe infatti parlare di libertà.

Di fronte a tale prospettiva, pare di veder riaffiorare, sotto forme nuove, il dibattito sulla linea di confine tra rivoluzione e resistenza e il relativo proposito di inserire il diritto a quest'ultima nelle Carte costituzionali del secondo dopoguerra, tra le quali anche quella italiana. A voler ben guardare, il riconoscimento dei fondamentali diritti di libertà tra i quali spicca proprio la libertà di espressione, è già una porta aperta tanto alla resistenza, quanto alla rivoluzione. La prima, quale difesa dell'ordinamento democratico costituzionale sostanziale rispetto a tentativi di svolte autoritarie o repressive, è conseguenza prettamente giuridica del riconoscimento del diritto alla libertà di espressione, che consiste nella pratica nel riconoscimento del diritto a porre in essere tutte quelle attività propedeutiche a qualsivoglia iniziativa organizzata di tutela dei diritti fondamentali. La seconda, quale rovesciamento, in forma violenta o meno, dell'ordinamento vigente quando la discrasia tra la Costituzione formale e quella materiale sia oramai insanabile, trova anch'essa terreno fertile di realizzazione proprio ove libertà di

esprimersi, quindi di criticare, e comunicare, quindi coordinarsi, abbiamo modo di essere esercitate.

Esempi di libertà di espressione quale forma di esercizio del diritto di resistenza possono essere considerate, in Italia, quelle iniziative della società civile, della stampa, di certe categorie o di persone individuali, finalizzate a contrastare leggi considerate lesive delle stesse libertà di espressione o di stampa, ovvero di altri principi fondamentali quali l'indipendenza del potere giudiziario dal potere politico oppure l'eguaglianza dei cittadini di fronte alla legge, o ancora dei diritti civili con rilievo etico o morale. In questo senso, il diritto alla libertà d'espressione quale forma del diritto di resistenza appare, solo apparentemente in modo paradossale, conservatore, in ragione di un sostanziale approccio volto al mantenimento di uno *status quo* che si considera e si desidera acquisito..

Esempi diversi di libertà di espressione quale elemento propedeutico all'esercizio di una pratica rivoluzionaria, del sommo diritto al rovesciamento del tiranno, o comunque dell'ordinamento vigente, attraverso un uso più o meno intenso della forza, la cui legittimità o illegittimità sarà, in ultima istanza, attribuita dalla vittoria o dalla sconfitta, sono quelli provenienti dall'altra sponda del Mediterraneo. In paesi come l'Egitto e la Tunisia le nuove tecnologie di telecomunicazione hanno sostanzialmente creato uno spazio di libertà di espressione, non riconosciuto dagli ordinamenti politici vigenti, sulla cui base, in un contesto socio-economico critico caratterizzato da sempre più ampia disuguaglianza sociale e sempre più gravi crisi alimentari, è stato possibile costruire l'abbattimento di affermate dinastie autoritarie.

2. Le dinamiche della società dell'informazione e l'*État de droit*

Per considerare quindi i profili fondamentali del conflitto tra libertà di espressione e esercizio del potere è quindi necessario muoversi, in primo luogo, dall'identificazione delle dinamiche proprie del potere stesso, non immutabile ma al contrario caratterizzato da un continuo distribuirsi e accentrarsi su soggetti diversi, che accompagna, stimola o frena i cambiamenti della società e ne viene da questi a propria volta influenzato. Le dinamiche ritenute più rilevanti ai fini che qui ci si propone sono tre e investono i settori più mobili dell'affermazione e dell'esercizio del potere:

a) in primo luogo rilevano le dinamiche giuridico-economiche dei rapporti tra pubblico e privato, in particolare alla luce dei fenomeni di privatizzazione, posta l'incidenza fondamentale, addirittura sul diritto alla vita, dell'ispirazione a criteri economici della creazione, dell'acquisizione, della gestione e della distribuzione delle risorse e dei beni, materiali e immateriali. La realtà quotidiana dell'utilizzo delle tecnologie di telecomunicazione ci insegna infatti quanto le libertà siano condizionate dalle scelte, in termini contrattuali oppure tecnologici, degli operatori, per lo più privati, che rendono le nostre comunicazioni possibili. In concreto, la possibilità di vedere una propria forma di espressione del pensiero libera di circolare e permanere sulle reti dipende con una frequenza sempre maggiore dall'adesione a *policies* contrattuali o termini di utilizzo e dalle relative procedure di controllo e decisionali, il tutto elaborato dai citati operatori, e dai *software* di controllo e sorveglianza, preventivi e successivi, da questi implementati. E ciò vale tanto in linea generale e astratta, ossia nella fase di definizione delle finalità, dei limiti all'utilizzo degli strumenti messi a disposizione della generalità delle persone e delle procedure di definizione dei

conflitti, quanto nel momento del realizzarsi di un concreto caso dubbio, ipotesi nella quale la gestione procedurale e, infine, l'assunzione della decisione sulla liceità di un contenuto, in bilanciamento con gli interessi confliggenti, spetta a soggetti non necessariamente nella posizione di legittimi interpreti risolutori di tali conflitti. Ciò rileva, con intensità ancora maggiore, alla luce dell'evoluzione del mercato della società dell'informazione caratterizzato da un accentramento del traffico e dall'affermazione di posizioni dominanti sempre più consistenti nella fornitura di taluni servizi della società dell'informazione, quali strumenti di ricerca delle risorse del *web*, piattaforme di *social networking*, o ancora servizi di *chat* per dispositivi *mobile*. In una società globale e in assenza di un diritto globale la *lex mercatoria* assume posizione e valore predominanti.

b) in secondo luogo rilevano le dinamiche di evoluzione della tecnica, o tecnologia, posto che nella specifica ipotesi qui considerata, la libertà di esprimere un pensiero, le caratteristiche proprie del *medium* ne determinano inesorabilmente, in alcuni casi in via del tutto automatica, non solo la portata ma la stessa sussistenza. Si parla in questa sede della *lex informatica*, ossia del codice informatico quale legge vigente. Questa prospettiva, inscindibilmente legata alla precedente, non si esaurisce nella considerazione della necessità del riconoscimento alla totalità delle persone di un eguale diritto all'accesso ai servizi della società dell'informazione e della difesa del trattamento del traffico degli individui e delle società in condizioni di parità, vale a dire le problematiche del *digital divide*[3] a livello globale e della *network*

[3] Per un approfondimento sul tema, v. ANZERA G. ,COMUNELLO F., *Mondi digitali. Riflessioni e analisi sul Digital Divide*, Milano, Guerini

neutrality[4], ma genera invece problemi sempre più pressanti quando i sistemi di controllo e di rimozione di contenuti diffusi, potenzialmente conflittuali, sia affidata a strumenti automatici, come nel caso delle supposte violazioni del diritto d'autore[5], dell'utilizzo di terminologia volgare o sconveniente[6] o della pubblicazione di contenuti multimediali

---

Associati, 2005, e JAMES J. *Digital Divide Complacency: Misconceptions and Dangers*, in *The Information Society*, 24, 54-61, 2008, Indiana University.

[4] "La *network neutrality* è definita nel modo migliore come un principio di progettazione. L'idea è che una rete informativa pubblica massimamente utile aspiri a trattare tutti i contenuti, siti, e piattaforme allo stesso modo. Ciò permette alla rete di trasportare ogni forma di informazione e di supportare ogni tipo di applicazione. Il principio suggerisce che le reti informative abbiano maggior valore quando è minore la loro specializzazione – quando sono una piattaforma per usi diversi, presenti e futuri", WU T., http://www.timwu.org/network_neutrality.html (verificato il 12.05.2014), professore della Columbia University e autore, tra gli altri lavori sul tema, di *Network Neutrality, Broadband Discrimination*, in *Journal of Telecommunications and High Technology Law*, 2.2, 2003.

[5] Attualmente, sistemi di controllo automatici di contenuti pubblicati in supposta violazione delle prerogative dei titolari di diritti d'autore sono adottati da diversi fornitori di servizi tra i quali Google, in particolare su Youtube attraverso, tra gli altri, il ContentID. Tali sistemi analizzano vari aspetti dei contenuti multimediali, immagini video e musica, confrontandoli con eventuali contenuti registrati, senza limitarsi al complesso dell'opera, ma controllando anche la corrispondenza di piccole parti di quanto dagli utenti pubblicato.

[6] Siti *web*, *blog*, *forum* e *social network* possono provvedere anche in via automatica ad impedire la pubblicazione di terminologie o parole ritenute contrarie alle proprie *policies*. Nella stessa prospettiva, ove si inseriscano successivamente parole nella *blacklist* delle terminologie inadatte, attraverso i *software* che gestiscono i siti le parole vengono oscurate. Anche nell'ambito dei *massive multiplayer online games*, ove il modello di dialogo e comunicazione è riconducibile a quello di una *chat*, è pratica corrente che, nel caso si intenda scrivere una parola volgare, questa venga elaborata dal *software* e "pubblicata" in una forma diversa, composta da caratteri speciali.

contrari a una certa morale[7]. Sul fronte opposto, il radicamento e la diffusione di infrastrutture virtuali alternative in grado di svilupparsi all'interno dell'infrastruttura ordinaria delle tecnologie di telecomunicazione danno origine a fenomeni, quali le *DarkNet*, ove palese diventa il predominio assoluto del fattore tecnologico rispetto a qualunque altro elemento, sia esso sociale, etico o morale, per quanto attentamente disciplinato dal diritto esso possa essere.

c) infine, la terza prospettiva dinamica di rilievo è l'affermazione di una pluralità di fonti del diritto alternative alla tradizionale fonte statale -o comunque pubblica in senso lato- in materia di normazione dei conflitti tra libertà sia nelle ipotesi generali che in episodi concreti, investendo quindi le categorie teoriche tradizionali del diritto e la distribuzione, in primo luogo *de facto* ma anche *de iure*, di competenze tra diversi soggetti. Quest'ultima dinamica attraversa e in un certo senso rappresenta al tempo stesso le fondamenta e la conseguenza di quanto anticipato in punto di ruolo dei soggetti privati e della tecnologia: è infatti sul cedimento e sull'impotenza del diritto nel mondo transnazionale globalizzato che si moltiplicano quelle lacune giuridiche colmate dal ricorso a forme e modi di risoluzione innovativi, e necessariamente extra-giuridici. Se infatti l'ordinamento giuridico non si rivela in grado di disciplinare in modo efficace ed effettivo fenomeni che, pur attraversando ed esplicando i loro effetti in relazione alla popolazione di un determinato Stato, abbiano origine oltre i propri confini nazionali, la funzione regolativa del diritto perde presa, di pari passo, anche all'interno del proprio territorio. Questa dinamica nel

---

[7] È noto l'utilizzo da parte di governi e imprese di *software* per oscurare fotografie e contenuti multimediali che rappresentino scene pornografiche o di nudo.

contesto delle ICTs è predominante, posto che la stessa distinzione tra popolazione, territorio e sovranità sembra perdere di senso se applicata alla virtualità, che ne è caratteristica propria.

Come si avrà modo di approfondire nei paragrafi che seguono, queste tre dinamiche così sommariamente delineate non sono fenomeni a sé stanti che si sviluppano e incidono sul diritto alla libertà di espressione, e sul diritto complessivamente considerato, in modo indipendente e autonomo ma, al contrario, si sostengono e si contrastano l'una con l'altra. È indubbio che queste dinamiche influiscano in modo sostanziale sui confini delle libertà che, per loro stessa natura, sono sì concetti culturali e sociali, in fin dei conti pre-giuridici, ma solo con la loro positivizzazione avvenuta grazie allo sviluppo del costituzionalismo moderno e contemporaneo, e in particolare con la nascita della giustizia costituzionale, hanno raggiunto i loro picchi di estensione quantitativa e profondità qualitativa. In questo senso, seguendo un approccio costituzionalistico sulla scia della teoria di Dworkin, la loro erosione comporterebbe il venir meno delle fondamenta giustificatrici del sistema democratico quale sistema di "governo sottoposto a condizioni"[8], con le conseguenze in punto di legittimazione sociale che ne deriverebbero. Parafrasando Paolo Grossi, il rischio per il diritto è di soccombere o consegnarsi nelle mani di un autoritarismo tecnologico e, per il suo tramite, di un autoritarismo economico[9].

---

[8] Le formula utilizzata è quella del "government subject to conditions", DWORKIN R., *Freedom's Law. The Moral Reading of the American Constitution*, Cambridge, Harvard University Press, 1996, p. 1-38

[9] Secondo l'autore "il rischio per il diritto è di attuare la sua liberazione dall'autoritarismo politico per consegnarsi nell'abbraccio dell'autoritarismo economico, un autoritarismo arrogantissimo", GROSSI P., *Globalizzazione e*

La ragione per la quale, rispetto alle enormi potenzialità positive per la società che derivano dalla diffusione delle ICTs, chi scrive ritiene di dover in primo luogo evidenziare i rischi non è riflesso di uno spirito reazionario, bensì esercizio di quel diritto di resistenza, una parte del quale, come già anticipato, è sicuramente conservatore. E tale conservazione riguarda le esigenze di tutela dello Stato di diritto, non tanto in relazione a quelle concezioni tradizionali caratterizzate da un approccio formale[10] che lo vorrebbero mera modalità di strutturazione dello Stato secondo il diritto, quanto piuttosto alla luce delle teorie dello Stato di diritto materiale e funzionale che legano indissolubilmente tale concetto alle teorie dei diritti umani e dei diritti fondamentali così come ai principi generali delle democrazie costituzionali. Con il riconoscimento dei diritti all'interno di Carte Costituzionali rigide e la previsione di organi di controllo della legittimità costituzionale degli atti legislativi la concezione materiale dello Stato di diritto è stata ricondotta alla formula dello Stato costituzionale di diritto[11]. L'evoluzione del costituzionalismo globale contemporaneo, caratterizzata dal superamento dell'interpretazione dei diritti fondamentali quali statuizioni di carattere programmatico in favore di una considerazione quali norme

pluralismo giuridico, in Q*uaderni fiorentini per la storia del pensiero giuridico moderno*, fasc. 29, Giuffré, Milano, 2000, http://www.centropgm.unifi.it/quaderni/29/quaderno.pdf (verificato il 12.05.2014).

[10] Lo stato di diritto inteso in senso formale prevede la separazione dei poteri e il rispetto del principio di legalità, finalizzati dunque all'assicurare un governo delle leggi, piuttosto che un governo degli uomini. In tale prospettiva, la separazione dei poteri così come delineata da Montesquieu nulla rileva quanto al contenuto delle legislazioni.

[11] Sulla distinzione tra Stato di diritto e Stato costituzionale, si veda ZAGREBELSKY G., *Il diritto mite*, Einaudi, Torino, 1992.

pienamente cogenti[12], dal rafforzamento degli strumenti affidati agli interpreti per la diretta applicazione dei principi costituzionali e, più recentemente, del diritto comunitario, e dall'estensione delle competenze degli organi di giustizia sovranazionali, ha determinato un'incorporazione dei principi democratici e di tutela della persona nello stesso concetto di *état de droit.*

In conclusione, se diamo quindi per acquisito che il sistema democratico-costituzionale e il riconoscimento dei diritti fondamentali della persona, la cui auspicabilità politico-giuridica è in questa sede del tutto fuori di discussione, trovano la propria garanzia di operatività all'interno di un sistema giuridico orientato ai principi caratterizzanti lo Stato di diritto, e in ugual misura riconosciamo l'effetto dirompente di una virtualità e di una globalizzazione capaci di svuotare di significato gli elementi fondanti di tale strumento funzionale, ossia l'identificazione chiara di una popolazione all'interno di un determinato territorio nei confronti dei quali è esercitata la sovranità, allora risulta evidente che le

---

[12] In Italia, il già vivo dibattito dottrinario venne indirizzato in questo senso dalla prima sentenza della Corte Costituzionale, la sent. n. 1 del 1596, che ebbe modo di affermare che "la nota distinzione fra norme precettive e norme programmatiche può essere bensì determinante per decidere della abrogazione o meno di una legge, ma non é decisiva nei giudizi di legittimità costituzionale, potendo la illegittimità costituzionale di una legge derivare, in determinati casi, anche dalla sua non conciliabilità con norme che si dicono programmatiche, tanto più che in questa categoria vogliono essere comprese norme costituzionali di contenuto diverso: da quelle che si limitano a tracciare programmi generici di futura ed incerta attuazione, perché subordinata al verificarsi di situazioni che la consentano, a norme dove il programma, se così si voglia denominarlo, ha concretezza che non può non vincolare immediatamente il legislatore, ripercuotersi sulla interpretazione della legislazione precedente e sulla perdurante efficacia di alcune parti di questa; vi sono pure norme le quali fissano principi fondamentali, che anche essi si riverberano sull'intera legislazione", http://www.giurcost.org/decisioni/1956/0001s-56.html (verificato il 12.05.2014)

ricadute di virtualizzazione e globalizzazione possano incidere sulla sussistenza stessa dei diritti fondamentali della persona e dei principi che oggi ne garantiscono la tutela.

Se infatti oggi sono i tribunali ordinari di merito e di legittimità, i tribunali costituzionali e, in una certa misura, i tribunali internazionali a poter sancire la disapplicazione o finanche l'illegittimità di una norma legislativa, o in taluni casi amministrativa o persino giurisdizionale, che regoli certi aspetti di *Internet* in contrasto al riconoscimento costituzionale di altri diritti fondamentali quale il diritto alla libertà d'espressione, *quid iuris* nel caso dell'implementazione di *policies* transnazionali o infrastrutture informatiche che di fatto conseguano il medesimo effetto, ossia di negare o limitare il diritto alla libertà d'espressione, senza però che esista alcun organo terzo ed indipendente competente in materia?

3. Sorveglianza, controllo e repressione nel contesto delle privatizzazioni

Se, come anticipato in introduzione, è ben pacifico che le questioni relative all'espressione di pensiero sono sorte nel momento stesso in cui l'umanità ha elaborato forme di comunicazione, il ruolo del pubblico, ossia di un entità che esercita potere e autorità nella prospettiva di un interesse generale e collettivo in relazione alla comunità di riferimento, è questione sorta non oltre l'alba immediatamente successiva. Dalla comunicazione interpersonale alle primordiali organizzazioni sociali il passo è stato breve. Con l'evolversi e l'affinarsi delle forme pubbliche di esercizio di tale potere e autorità, è andato a sua volta affermandosi il ruolo centrale del soggetto privato, sia esso un *oikos* dell'antica Grecia o

una corporazione di mercanti operante nella Lega Anseatica[13] o nella Firenze tardo-medievali, al punto che non infrequenti sono stati nella storia i momenti in cui l'ordine sociale, e ancor più economico, ovvero in vari casi quello militare, era conservato oppure modificato da privati eterogeneamente organizzati[14].

L'affermarsi degli Stati moderni, in un primo tempo assoluti, ha segnato l'avvio di un percorso solo apparentemente paradossale: al fianco di un costante restringimento degli spazi di autonomia giuridica dei soggetti privati, necessario sacrificio verso un accentramento dei poteri di governo dell'agire sociale nelle mani delle istituzioni dei neonati Stati nazionali, si sviluppavano teorie e pratiche dell'affermazione di diritti individuali fondamentali, quel liberalismo che sanciva come tali la vita, la libertà e la proprietà. Il paradosso è solo apparente perché è insito nella natura stessa dei diritti di libertà, come si è già avuto modo di anticipare in introduzione, un carattere sovversivo e contestatore. Da qui diviene del tutto logicamente giustificato il fatto che

---

[13] La storia della Lega Anseatica, o *Hansestädte*, nata quale corporazione di mercanti e poi evolutasi quale associazione di città mercantili, è esemplare di un peculiare rapporto tra pubblico e privato in un periodo di lenta dissoluzione dell'ordine giuridico e politico costituito. "La hansa germanica si difierenzia dalle leghe temporanee e occasionali di altri mercanti stranieri per il carattere permanente ch'essa assume, per l'ampiezza del territorio su cui essa estende presto la sua azione, e perché *la solidarietà che si è venuta a stabilire fra i mercanti della bassa Germania in paese straniero finisce per provocare l'unione delle varie città da cui essi provengono*" (enfasi aggiunta) LUZZATTO G., *Lega Anseatica*, in *Enciclopedia italiana Treccani*, vol .III, 1929, pp. 426-428.

[14] Nei siffatti esempi, l'*oikos* quale nucleo fondamentale di conservazione dei rapporti giuridici patrimoniali e familiari e la corporazione operante al servizio delle autorità dei Comuni per le più svariate necessità, dall'approvvigionamento di beni, alla conservazione fino alla difesa del Comune stesso in caso di assedi o minacce di tipo militare.

tali diritti trovino terreno fertile per il loro sviluppo teorico e pratico all'interno di un contesto di nuova definizione di poteri e autorità assolute.

Ed è in questo specifico contesto storico che sono elaborate le fondamenta del pensiero giuridico dei Lumi, così come del costituzionalismo e del liberalismo dei secoli XVIII e XIX: l'art. 19 della Dichiarazione dei Diritti dell'Uomo e del Cittadino del 1789 quale summa degli eterogenei contributi del periodo, e fondamenta ancora attualissima e ineludibile in un qualsiasi dibattito ad oggetto costituzionale, ove si afferma che "ogni società in cui la garanzia dei diritti non è assicurata, né la separazione dei poteri determinata, non ha costituzione". In quell'occasione fu anche positivizzato un altro principio di attualissima rilevanza, ossia l'affermazione secondo cui "la libertà consiste nel poter fare tutto ciò che non nuoce ad altri", sancito dal già citato art. 4 della medesima Dichiarazione. Su tali fondamenta, nel nostro recentissimo passato, si arriverà allo Stato costituzionale di diritto caratterizzato sì dalla garanzia dei diritti fondamentali, ora positivi, ma anche e soprattutto da una divisione dei poteri non limitata alla tripartizione tra potere esecutivo, potere legislativo e potere giudiziario ben immaginata da Montesquieu, bensì allargata alla pratica della supremazia del diritto intesa in primo luogo come supremazia delle Costituzioni, quelle Costituzioni sostanziali dalle quali le garanzie dei diritti siano assicurate, su qualsivoglia altra norma di carattere legislativo o amministrativo che ne dipenda.

Nell'architettura latamente sociale così costruita, i diritti dei soggetti privati sono riconosciuti nella duplice forma del diritto del singolo cittadino, della singola persona, e in certi casi di una pluralità di persone, di conservare in privato ed esercitare in pubblico uno spazio di libertà rispetto a invasioni non autorizzate e di libertà di porre in essere

azioni o attività positive, e del diritto del singolo di operare quale soggetto titolare di uno spazio di libertà di iniziativa economica e di godimento e utilizzo della proprietà acquisita su determinati beni. Entrambi questi aspetti rilevano in punto di relazioni tra pubblico e privato: i diritti di libertà personale hanno natura apertamente conflittuale nei confronti dell'autorità stabilita che, al tempo stesso, in taluni casi, li ha riconosciuti, garantiti e tutelati giuridicamente; i diritti di più stretta natura economica vivono tuttora una tensione conflittuale verso la gestione pubblica tanto in una prospettiva teorica, in primo luogo quella neoliberista, quanto in una pratica quotidiana di esercizio di potere sui beni nella propria disponibilità, posti i limiti quantitativi dei beni. A partire dagli anni '80 del secolo scorso si diffonde capillarmente a livello globale l'ideologia dello *Stato minimo*[15] di fronte ad un settore privato ritenuto più efficiente nell'occuparsi di settori fino ad allora considerate di appannaggio pubblico: la gestione dei trasporti, dei sistemi bancari e monetari, delle infrastrutture idriche ed energetiche, dei sistemi scolastici e dei sistemi sanitari. Proseguendo su questa linea di evoluzione, finanche l'amministrazione dell'ordine pubblico, della giustizia e del sistema carcerario hanno visto funzioni sempre più ampie affidate a privati. Non sorprende quindi che, in tale contesto, la nascita, lo sviluppo e la gestione delle infrastrutture di telecomunicazione digitale, così come fu per le infrastrutture telegrafiche e telefoniche

[15] La raccolta delle impostazione elaborate dagli economisti Milton Friedman e Friedrick von Hayek da parte di pragmatici e influenti politici quali Margareth Thatcher e Ronald Reagan è stata determinante nell'affermazione globale di tale ideologia.

affidate all'*International Telecommunication Union* (ITU)[16], siano stati affidati a soggetti di natura mista pubblico-privata in applicazione del *multistakeholder governance model*.

La teoria economica ha elaborato diverse definizioni e inquadramenti di quanto a cui ci si riferisce usando il temine privatizzazione, distinguendola soprattutto tra privatizzazione sostanziale e privatizzazione formale[17]: con la prima si intende il passaggio della titolarità della proprietà di enti dallo Stato o dagli enti pubblici a soggetti privati, che lo gestiranno secondo le regole del diritto privato[18]; con la seconda invece si fa riferimento al passaggio al regime di diritti privato di un ente che comunque resta di proprietà pubblica[19]. Esistono altre forme diverse o più deboli di privatizzazione, tra le quali la deregolamentazione, ossia la riduzione di vincoli e controlli all'operato di imprese e privati, le liberalizzazioni, ossia l'apertura di monopoli originariamente pubblici alle iniziative private, e la privatizzazione funzionale, nel qual caso pubblico e privato condividono la gestione di certe attività originariamente di appannaggio esclusivo

---

[16] Organizzazione internazionale fondata nel 1865 a Parigi, ora Agenzia delle Nazioni Unite con sede a Ginevra, che si occupa di definire gli standard per l'utilizzo delle onde radio nelle telecomunicazioni, http://www.itu.int/ (verificato il 12.05.2014).

[17] DOSSENA G., *Le privatizzazioni delle imprese. Modalità, problemi e prospettive*, EGEA, Milano, 1990.

[18] Cfr. JAEGER P.G., DENOZZA F., TOFFOLETTO A., *Appunti di di diritto commerciale*. *Impresa e società*, Giuffré, Milano, 2010, p. 52, che definiscono la privatizzazione formale come "l'adozione di una forma giuridica di carattere privatistico [...] in luogo di una di origine e di stampo pubblicistici".

[19] Vedi la definizione "per privatizzazione sostanziale si intende il passaggio della proprietà (o del controllo) di imprese o di settori di imprese da un soggetto pubblico a soggetti privati", *ibidem*.

pubblico, diventano quindi "corresponsabili di settori di attività gestiti in precedenza solo dall'operatore pubblico"[20]. È a quest'ultima tipologia, quella della privatizzazione funzionale, che si fa riferimento, seppur in termini distinti da quelli della sola teoria economica, con l'utilizzo della locuzione privatizzazione della censura e alla quale sembrerebbe essere riconducibile il modello *multistakeholder*[21], che ispira il governo della Rete delle reti.

3.1. *Multistakeholder Internet Governance Model*

Il breve percorso esplicativo appena presentato è preliminare all'analisi dell'evoluzione dei rapporti tra soggetti pubblici e soggetti privati nella gestione di *Internet* e dei dati ivi trasmessi: l'attuale funzionamento del governo delle rete, o *Internet Governance*, riflette tali rapporti. La rete delle reti infatti è ben lungi dall'essere quel luogo ispirato a principi anarco-libertari declamato, o forse meglio auspicato, da parte della dottrina non solo giuridica[22] e di parte della società civile

---

[20] MARTUFI R., VASAPOLLO L., *Le diverse forme di privatizzazione*, http://proteo.rdbcub.it/article.php3?id_article=18#nb2, (verificato il 12.05.2014)

[21] Del resto lo stesso Peter Dengate Thrush, allora presidente del Consiglio di ICANN, ha avuto modo nel 2008 di affermare che "con la creazione di ICANN, la comunità di *Internet* e il governo degli Stati Uniti hanno riconosciuto la necessità di *privatizzare il sistema dei nomi di dominio* per aumentare la concorrenza e la partecipazione internazionale" (corsivo aggiunto), http://www.icann.org/it/news/announcements/announcement-30sep08-it.htm (verificato il 12.05.2014)

[22] Tra tutti, si veda la "Dichiarazione di Indipendenza del Ciberspazio" di John Perry Barlow del 1996, disponibile in lingua italiana all'indirizzo http://www.olografix.org/loris/open/manifesto_it.htm (verificato il 12.05.2014) e in lingua inglese

digitale. Tale immagine, favorita senza dubbio dall'assenza del diritto e di una stabile normazione fino, almeno in Europa, ai primi anni '90 del secolo scorso, e dalla transnazionalità che la caratterizza, venne smentita non solo dall'evoluzione della rete negli anni successivi, che ha visto a fianco dell'economia un ingresso massiccio del diritto nel ciberspazio[23], ma soprattutto dall'architettura stessa del governo di *Internet*. Tecnologia, diritto e imprese possono rappresentare oggi, su *Internet*, insieme, quanto di più lontano da quell'immaginario libertario si sarebbe potuto costruire.

Il governo di *Internet*, da un punto di vista tecnico-normativo e nel senso della definizione qui in seguito riportata, è attualmente gestito da una pluralità di soggetti che svolgono ruoli determinanti nell'assicurarne un funzionamento stabile e continuativo. La stessa definizione di *Internet governance*[24] proposta dal *Working Group on Internet*

---

https://w2.eff.org/Censorship/*Internet*_censorship_bills/barlow_0296.declaration (verificato il 12.05.2014).

[23] Sviluppo dell'economia digitale e normazione giuridica della rete sono andate appunto di pari passo. Sono infatti due le principali ragioni dell'ingresso prepotente del diritto su *Internet*: da una parte le necessità di interesse pubblico da parte dei Governi di perseguire, anche nel contesto digitale, una politica criminale legata ai fenomeni di violazione dei diritti d'autore, pedopornografia, terrorismo e traffico di sostanze stupefacenti; dall'altra l'interesse dei soggetti operanti attraverso *Internet* a veder disciplinato (ma soprattutto protetto) il nascente mondo dell'*e-commerce*. In un secondo momento entrambi questi filoni hanno continuato a crescere, nella prima prospettiva con le sempre più articolate esigenze in materia di esigenze procedimentali nel perseguimento di reati commessi attraverso o su *Internet*, nella seconda prospettiva invece con la necessità di tutela degli interessi dei consumatori e per la tutela delle persone nel trattamento dei dati personali.

[24] La formula di *Internet Governance* è comunque contestata degli stessi operatori, che con frequenza si riferiscono a tale complesso fenomeno con il concetto di *Internet Coordination*, sottolineandone dunque – o rivendicandone – il carattere acefalo e distribuito.

Governance (WGIG)[25] come contenuta nel report conclusivo del *World Summit on the Information Society* (WSIS)[26] promosso dalle Nazioni Unite nel 2005, sancendo che "[l']*Internet governance è lo sviluppo e l'applicazione da parte dei Governi, del settore privato e della società civile, nei propri rispettivi ruoli, di principi, norme, regole, procedure decisionali e programmi condivisi che determinano l'evoluzione e l'uso di Internet*"[27], richiama al ruolo di questa pluralità di soggetti provenienti dai Governi, dal settore privato e dalla società civile. Oltre però le dichiarazioni di principio, il governo di *Internet*, ossia lo sviluppo e l'applicazione di principi, norme, regole e procedure decisionali è quindi affidato a rapporti particolarmente fluidi tra governi, mercato e società. A seconda del livello dal quale si osservano le reti, tale modello, che si descriverà ora brevemente, presenta diversi spunti di riflessione.

---

[25] Il WGIG fu un gruppo di lavoro in seno alle Nazioni Unite avviato a seguito del WSIS di Ginevra del 2003 con lo scopo di predisporre una proposta per il governo di *Internet* da sottoporre al summit seguente svoltosi a Tunisi nel 2005.

[26] Con WSIS ci si riferisce alle due conferenze promosse dalle Nazioni Unite nel 2003 e nel 2005 con le finalità di collegare il problema del *digital divide* e i rischi e le opportunità delle ICTs alla Dichiarazione del Millennio e i relativi obiettivi di sviluppo. Tra i risultati vi è l'attivazione dell'*Internet Governance Forum*.

[27] In originale, "*Internet Governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet"* Report disponibile alla pagina web http://www.wgig.org/docs/WGIGREPORT.pdf (verificato il 12.05.2014)

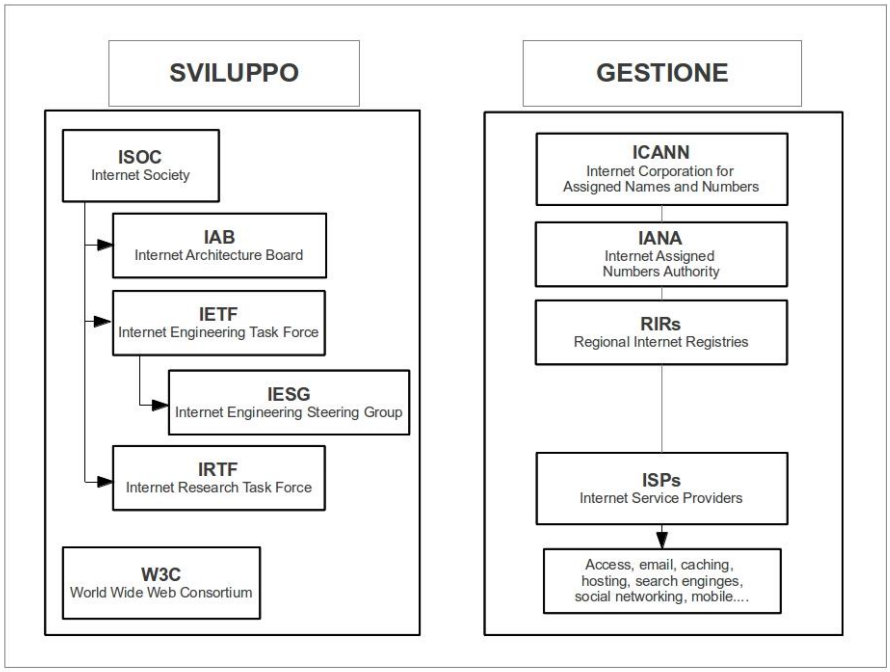

Figura 1: Sviluppo e gestione di *Internet* e del *Web*.

A monte rispetto al web, alle applicazioni e ai servizi che utilizziamo quotidianamente rese disponibili dallo sviluppo delle ICTs, vi è una pluralità di soggetti che studiano, ricercano e sviluppano l'architettura di funzionamento, le tecnologie e i protocolli che abilitano questi stessi servizi, indirizzando l'evoluzione complessiva di *Internet*. Come rappresentato nella figura 1, in tale contesto rilevano in particolar modo le attività delle organizzazioni quali sono l'*Internet Society* (ISOC)[28], finalizzata all'ideazione, allo sviluppo e alla diffusione dei protocolli di funzionamento delle reti, e l'*Internet Corporation for*

[28] L'ISOC è un' organizzazione internazionale di diritto americano per la promozione dell'utilizzo e dell'accesso a *Internet*, la cui finalità sarebbe "promuovere lo sviluppo aperto, l'evoluzione e l'uso di *Internet* per il bene della popolazione di tutto il mondo", http://www.isoc.org (verificato il 12.05.2014).

Assigned Names and Numbers (ICANN)[29], la cui funzione è quella di gestire, nella globalità degli aspetti decisori, l'assegnazione di nomi a dominio e indirizzi IP.

L'ISOC, fondata nel 1992 quale organizzazione no-profit con prima finalità la ricerca dei finanziamenti necessari alle attività delle varie organizzazioni operanti nel campo, è l'organizzazione che ospita e coordina le attività delle più rilevanti entità che operano nello sviluppo tecnico di *Internet*: l'*Internet Architecture Board* (IAB), le cui diverse attività sono comunque rivolte al coordinamento e alla supervisione dei vari soggetti che si occupano di sviluppo degli *standard* e dei protocolli di *Internet*, l'*Internet Engineering Task Force* (IETF) e l'*Internet Engineering Steering Group* (IESG), rispettivamente l'organizzazione finalizzata allo sviluppo degli *standard* di funzionamento di *Internet* e il ristretto gruppo interno allo IETF stesso responsabile in ultima istanza di numerose decisioni, e l'*Internet Research Task Force* (IRTF), le cui attività sono focalizzate verso la ricerca e lo sviluppo delle tecnologie in una prospettiva di lungo periodo.

Quanto alla gestione dei nomi a dominio l'ICANN, organizzazione senza scopo di lucro fondata nel 1998 e stabilita in California, USA, svolge un ruolo centrale nel coordinamento degli spazi riservati agli indirizzi IP e nell'attribuzione dei domini di primo livello (*top-level domain*). L'organizzazione più rilevante che risponde all'ICANN è l'*Internet Assigned Numbers Authority* (IANA), la cui funzione più rilevante è la gestione a livello di radice del *Domain Name System* (DNS), ovvero la gestione della risoluzione dei nomi a dominio nei

[29] Ente internazionale con sede a Los Angeles (USA), https://www.icann.org/ (verificato il 12.05.2014).

corrispondenti indirizzi numerici IP[30]. Al fine di svolgere le proprie attività, l'IANA si serve di organizzazioni di registrazione, i *Regional Internet Registries* (RIRs), geograficamente localizzate (Africa, Asia e Pacifico, Europa e Russia, Nord America, Caraibi e America Latina), che a loro volta si servono di organizzazioni istituzionali o imprese private locali che curano l'attribuzione dei diversi nomi di dominio. Secondo una struttura gerarchica, l'IANA affida un certo numero di indirizzi IP e pacchetti di domini alle RIRs, che a loro volta li distribuiscono alle competenti organizzazioni, autorità nazionali politiche o scientifiche o imprese private, che direttamente o attraverso ulteriori passaggi li mettono infine a disposizione, a pagamento, agli interessati.

Il *World Wide Web Consortium* (W3C)[31], organizzazione internazionale no-profit, svolge un ruolo simile a quello dell'ISOC ma con l'attenzione specificamente rivolta al web. Composta da operatori privati commerciali e no-profit ed enti pubblici, il ruolo del W3C consiste nell'elaborare raccomandazioni per l'adozione di specifiche tecniche di standard e linguaggi di comunicazione che assicurino la conservazione e l'ampliamento delle caratteristiche di apertura e di libertà del *web*.

Vale notare che tale pluralità di soggetti operano in un contesto di interdipendenza marcata di ciascun segmento operativo con l'altro, essendo gli ambiti di cui ciascuno sarebbe responsabile a loro volta

---

[30] Tale controllo avviene dal 1999 ed è stato in diverse forme rinnovato nel 2003, nel 2006 e annualmente dal 2011, su decisione del Dipartimento del Commercio del Governo degli Stati Uniti.

[31] Il sito istituzionale internazionale del W3C è raggiungibile all'indirizzo http://www.w3.org/ (verificato il 12.05.2014)

strettamente correlati. Così l'ICANN e l'ISOC collaborano strettamente e le unità che ne fanno parte si riferiscono le une alle altre per lo svolgimento delle proprie funzioni.

Non essendo finalità del presente elaborato approfondire oltre il necessario la storia e le funzioni delle organizzazioni che si occupano del funzionamento di *Internet*[32], è invece di interesse trarre dall'evoluzione delle stesse, dai loro rapporti con le autorità pubbliche e il diritto e dalla portata delle loro decisioni alcune considerazioni. Questi aspetti rilevano in particolar modo in relazione alla posizione ed il ruolo degli *Internet service sroviders*, sui quali ci soffermerà dettagliatamente più avanti, e alle attività svolte dall'ICANN, la cui legittimità sul piano globale non deriva tanto da una qualche forma di rappresentatività di tipo giuridico, quanto dal combinato tra una posizione fattuale di monopolio della gestione tecnica dei *top-level domain* e del DNS e il consenso politico degli Stati nazionali. Consenso quest'ultimo non più, se mai lo fosse veramente stato, unanime. Le considerazioni riguardo alla concentrazione di attività decisionali relative all'utilizzo del più importante strumento di comunicazione mondiale nell'area di influenza di una sola nazione, gli Stati Uniti, hanno comportato critiche e proposte di modifica dell'organizzazione di modo che, per esempio, questa fosse condotta formalmente sotto il controllo delle Nazioni Unite.

Se le attività di ricerca e implementazione tecnica svolte dalle organizzazioni sotto l'egida dell'ISOC sollevano un minor, e comunque

---

[32] Per approfondimenti sul punto, anche nella prospettiva giuridica di cui si tratta, si veda MUELLER M., *Ruling the root: Internet governance and the taming of cyberspace*, 2004, MIT Press, California.

presente, complesso di contestazioni[33], le attività svolte dall'ICANN hanno infatti risvolti di elevato rilievo sia in ambito economico che in ambito giuridico. Sull'assegnazione di nomi a dominio infatti possono facilmente sorgere controversie in relazione sia alla tutela di marchi e della proprietà intellettuale, sia a tutela del nome delle singole persone. In particolare su quest'ultimo aspetto i tribunali degli Stati nazionali non hanno esitato ad intervenire, ordinando la collaborazione delle autorità di registrazione nazionali, e di riflesso dell'ICANN stessa. In punto di tutela del marchio e della proprietà intellettuale, la *policy per la risoluzione delle controversie sui nomi di dominio uniformi*[34] dell'ICANN richiama la disciplina della *World Intellectual Property Organization* (WIPO)[35], agenzia delle Nazioni Unite competente a riguardo, affidando la risoluzione delle eventuali controversie che dovessero sorgere a riguardo a una procedura arbitrale condotta al proprio interno. Rileva infine come fondamentale la funzione di gestione, sia centralizzata che delegata, del DNS, che a valle trova come penultimi interlocutori, giusto prima degli utenti, i fornitori di servizi di connettività. La funzione svolta dal DNS è infatti di fondamentale rilevanza per l'accessibilità ai contenuti di *Internet* da parte della generalità delle persone. I fornitori di servizi di connettività, ossia gli

---

[33] A tal punto, come si affronterà più avanti, è comunque di interesse la posizione dei soggetti deputati alla determinazione tecnica dell'ambiente virtualizzato nel quale si opera attraverso gli strumenti di telecomunicazione. Tale ambiente infatti influisce determinando, in parte, quali attività, comportamenti o scelte siano effettivamente possibili e quali impossibili. Queste leggi naturali del ciberspazio determinano, in ultima istanza, la portata del nostro agire sociale attraverso le telecomunicazioni.

[34] Consultabile in lingua italiana all'indirizzo web https://www.icann.org/it/help/dndr/udrp/policy (verificato il 12.05.2014).

[35] Il sito della WIPO, http://www.wipo.int/ (verificato il 12.05.2014).

access provider, gli operatori che permettono di connettersi alla rete, intervengono attraverso questo strumento per permettere o bloccare l'accesso a determinati contenuti su ordine delle autorità nazionali, quando questi non siano ospitati su *server* materialmente dislocati all'interno dei confini su cui l'autorità esercita la propria funzione[36].

Tale ricostruzione dell'organizzazione dell'ICANN, così come delle funzioni fondamentali che essa svolge, dev'essere infine messa in relazione con la composizione e l'organizzazione della stessa organizzazione: la natura eminentemente privatistica e la posizione, non solo geografica, orientata nei confronti del sistema politico e giuridico statunitense, dal cui Governo ottiene l'autorizzazione allo svolgimento delle proprie funzioni, ben motiva il sorgere di questioni relative alla rappresentatività e, in punto finale, alla democraticità delle decisioni assunte e delle procedure istituzionalizzate che riguardano l'intera società globale. Volgendo lo sguardo agli operatori responsabili dell'attribuzione dei *top-level domain names*[37], la prevalenza di soggetti privati e portatori di interessi propri, quali *Verisign*, responsabile tra gli altri per i domini .com e .net, è ben radicata.

Esistono in tal senso costruzioni alternative, quale quella avanzata durante il WSIS del 2005 che proponeva la trasformazione dell'ICANN in un'agenzia facente capo alle Nazioni Unite, con l'assoluto controllo

---

[36] Si permetta, sul tema, un rinvio a BETTONI M., *Il sequestro preventivo di siti web tramite ordine agli ISP: osservazioni sui casi Moncler e Vajont.info*, in *Ciberspazio e diritto*, 2012, p. 75 ss.

[37] La lista è accessibile sul sito dell'ICANN all'indirizzo http://www.icann.org/en/resources/registries/listing (verificato il 12.05.2014).

del DNS e al di fuori del monopolio legale degli Stati Uniti[38]. Il dilemma in punto giuridico-politico, precedente rispetto a considerazioni di carattere economico, sorge dall'assenza di un unanime riconoscimento dei diritti fondamentali della persona da parte degli stati che compongono le Nazioni Unite. In sostanza, il conflitto vede da una parte un modello nel quale i principali operatori economici, in assenza di trasparenza, rappresentatività e poteri di controllo democratico, sotto l'egida di un solo specifico Governo, influiscono sulle decisioni tecniche e sostanziali con lo sguardo rivolto, ovviamente, ai propri interessi economici e dall'altra un governo politico internazionale ancora immaturo quanto al consolidamento dei principi propri del costituzionalismo moderno. Il timore suscitato dall'idea di dall'affidare scelte strategiche relative alle ICTs, *in primis Internet*, alle Nazioni Unite, organismo all'interno del quale non è indifferente il peso degli Stati che con minori limiti e maggiore arbitrarietà violano i principi dei diritti fondamentali è, infatti, ben fondato.

3.2. (segue): il ruolo degli *Internet Service Providers*

Proseguendo a valle verso i soggetti locali che permettono alle ICTs di funzionare, attualmente il ruolo preponderante è quello svolto dagli intermediari, i cosiddetti *Internet service providers* (ISP). Rinviando alla ricca dottrina in merito le questioni strettamente giuridiche relative all'individuazione dei soggetti intermediari e delle

[38] E che, per inciso, è stata una delle ragioni del parziale fallimento di quel *summit*.

discipline normative della loro posizione[39], dei loro obblighi e delle loro responsabilità, ciò che si intende svolgere in questa sede è chiarire le ragioni, le finalità, la portata e le implicazioni derivanti dal presente assunto. Un qualsivoglia pensiero che voglia essere espresso con l'ausilio delle ICTs è infatti indissolubilmente legato alla disponibilità di una pluralità di soggetti di dar corso alla circolazione dello stesso. Dal momento stesso in cui questo pensiero fuoriesce dall'intima riflessione personale per riversarsi in un formato digitale nella forma di un contenuto testuale, audiovisivo o comunque multimediale, se la finalità è quella della comunicazione o della diffusione[40] sarà necessaria la collaborazione di una pluralità articolata di soggetti terzi il cui numero dipende dalle modalità scelte dal soggetto interessato.

---

[39] Tra tutti, LUPARIA L.. (a cura di), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Giuffrè, 2012, ma, più risalenti e di interesse, SEMINARA S:, *La responsabilità penale degli operatori su Internet*, in *Diritto dell'Informazione e dell'Informatica*, 1998, pp. 441-458, RICOTTI S., *Fondamento e limiti della responsabilità penale dei Service-providers in Internet*, e *La responsabilità penale dei Service-providers in Italia*, in *Diritto penale e processo*, 1999.

[40] Ma questa circoscrizione della problematica alla circolazione del contenuto già sfuma con la diffusione di terminali in assenza di memoria propria, nel cui caso anche la mera trascrizione in formato digitale incorrerà nelle medesime problematiche.

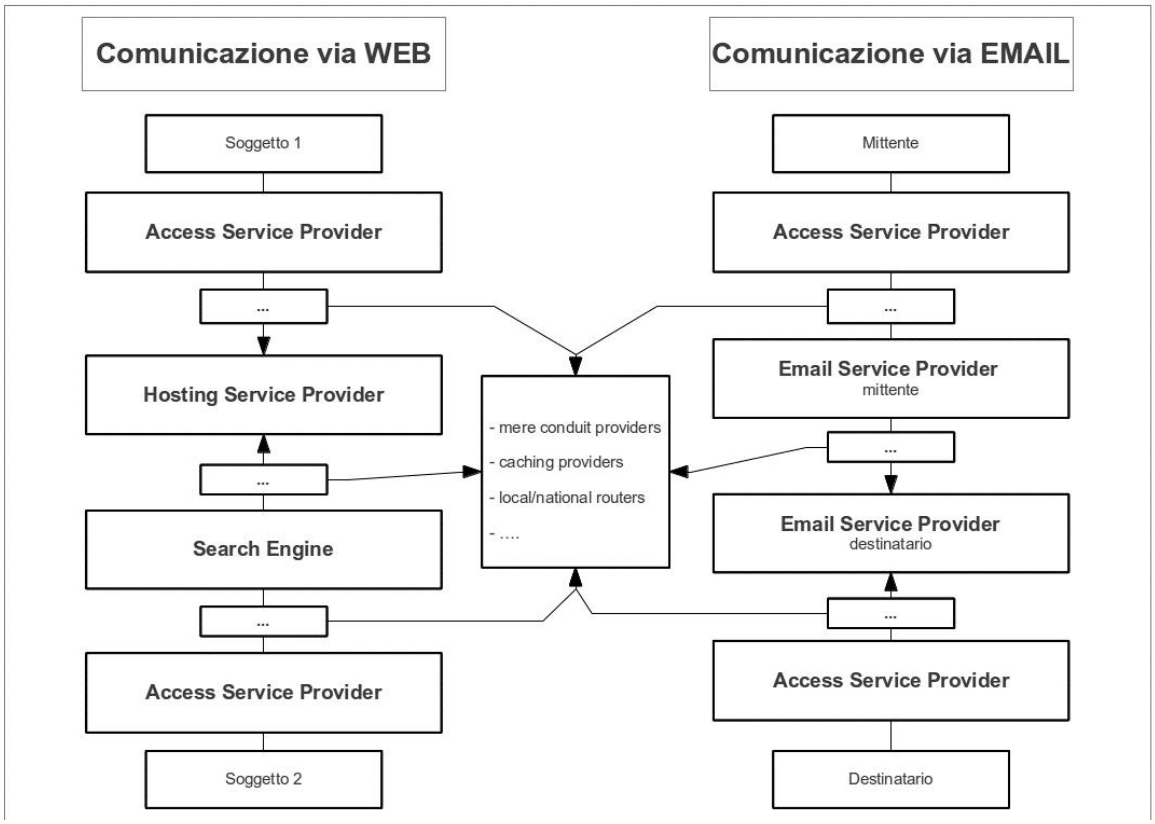

Figura 2: Intermediari nelle trasmissioni *web* ed *email*

Come si riassume nella figura 2, nel caso infatti di volontà di diffondere un contenuto attraverso la sua pubblicazione sul *web* in modo tale da renderlo accessibile alla globalità degli utenti di *Internet* occorreranno, dal punto di vista dell'autore, un soggetto che ci consenta l'accesso alla rete (*access provider*), un soggetto che metta a disposizione uno spazio ove il contenuto possa essere ospitato e quindi raggiunto (un *hosting provider*), la pluralità di soggetti che rendono possibile la trasmissione del contenuto stesso dal punto di origine a

questo spazio virtuale (*mere conduit providers*) e, dal punto di vista di un potenziale destinatario interessato, un soggetto che individui la presenza di questo contenuto sulla rete agevolandone l'accesso (un *information location tool,* quale un motore di ricerca), oltre nuovamente a un fornitore di servizi di accesso e vari fornitori di servizi di trasmissione dei dati. Il numero di questi soggetti può eventualmente ridursi, in virtù di particolari tecnologie che bypassino questo o quel passaggio, come, a titolo d'esempio, nel caso di distribuzione *peer-to-peer*, ove il ruolo dell'intermediario di *hosting* sfuma di fronte ad altre posizioni, quale quella dei soggetti che indicizzano i contenuti stessi o ne trasmettono semplicemente i dati. La platea di soggetti terzi coinvolti potrebbe anche aumentare, in quei contesti regionali o nazionali che aggiungano aggravi e controlli ai dati che passano attraverso determinate frontiere virtuali, a livello di *router* locali, regionali o nazionali.

Nell'ipotesi invece di volontà di comunicare a un numero di soggetti determinati attraverso servizi di posta elettronica o altre modalità di comunicazione diretta, la necessità di collaborazione da parte di fornitori di servizi di *hosting* sarebbe sostituita da quella di fornitori dello specifico servizio utilizzato[41], non vi sarebbe necessità di un servizio di indicizzazione e le altre posizioni resterebbero invece immutate, ciò anche nel caso di un aggravio dei controlli su specifici nodi della rete.

Ugualmente esistono ulteriori possibilità che determinerebbero una

---

[41] Nel caso di un *email service provider* (ESP), la posizione del fornitore si avvicinerà a quella dell'*hosting provider* nell'ipotesi in cui il servizio sia fornito attraverso webmail e al contrario sarà più prossima a quella del *mere conduit provider* nella diversa ipotesi di fornitura del servizio tramite protocolli IMAP /POP3, per la ricezione, e SMTP, per l'invio.

riduzione dei soggetti coinvolti o dell'efficacia di un loro eventuale intervento. Nella prima ipotesi ci si riferisce all'utilizzo di propri dispositivi quali *server* propri permanentemente o temporaneamente connessi alla rete, in modo da sopperire alla necessità di un servizio di *hosting*. Con la seconda ipotesi invece ci si riferisce a modalità di connessione più ricercate, quali l'utilizzo di sistemi di *onion routing*[42], *proxy*[43] o *Virtual Private Networks* (VPN)[44], ovvero di crittografia dei dati trasmessi[45]. Tali tecnologie determinano una maggior difficoltà nell'attività di interposizione sulla base, nel primo esempio, dei soggetti originari o destinatari delle comunicazioni ovvero, nel secondo esempio, sulla base del contenuto delle comunicazioni stesse. Questi ultimi esempi sono esemplificativi della stretta correlazione tra la posizione di soggetti intermediari e le tecnologie disponibili utilizzate dai fruitori dei servizi.

---

[42] Tecnica per la comunicazione anonima attraverso le reti di comunicazioni.

[43] Un programma che si interpone tra un c*lient* ed un *server* facendo da tramite o interfaccia tra i due *host*, in pratica permettendo all'utente di nascondere al sito di destinazione le informazioni relative alla propria localizzazione.

[44] Reti di telecomunicazione private che si poggiano sull'infrastruttura di *Internet* creando però un canale di comunicazione riservato e sicuro.

[45] Queste tecniche, e le riflessioni che ne derivano, saranno affrontate nel CAP III, *Sorveglianza Globale e Resistenza Digitale*, par. 5 e seguenti.

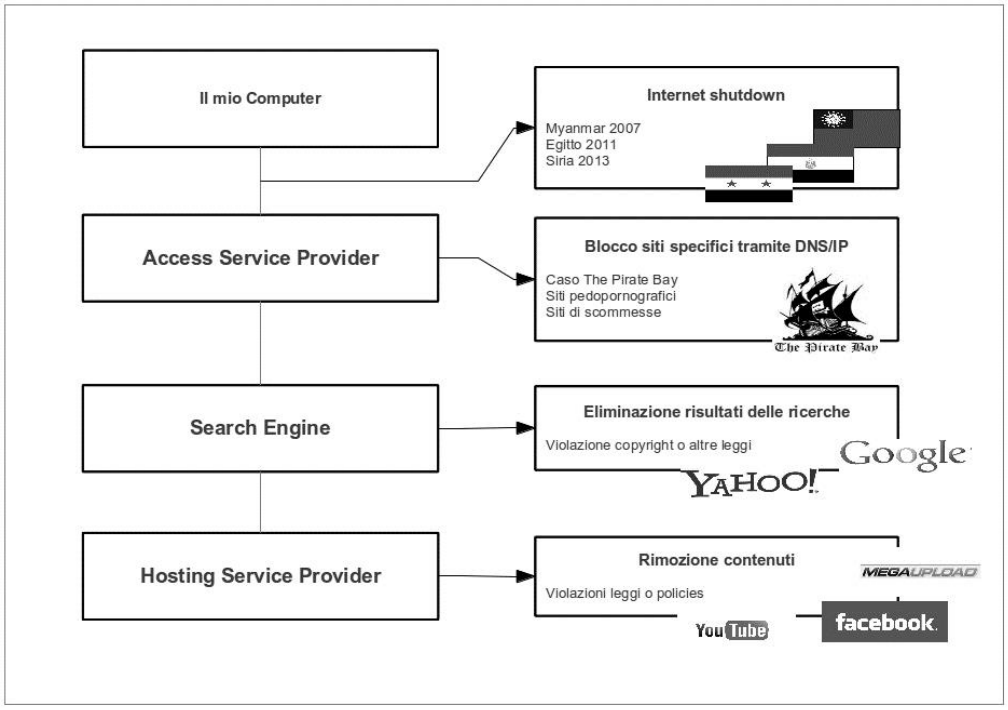

Figura 3 Ipotesi di censura a diversi livelli

Alla luce di tale sommaria ricostruzione, a ciascuno di questi piani corrispondono concrete possibilità di censura e, di riflesso, di violazione dei diversi diritti collegati alla libertà di espressione. Nella figura 3 sono presentati, a titolo d'esempio, alcuni casi noti di limitazione dell'accesso a risorse telematiche in relazione al livello sul quale si è realizzato l'intervento censorio.

Sul piano della *rimozione dei contenuti* sono possibili interventi a livello di *hosting provider* oppure a livello di materialità del *server*. Rientrano nella prima categoria i diversi casi di collaborazione da parte di fornitori quali Youtube o Facebook nella rimozione di contenuti denunciati quali illeciti, sia su autonoma iniziativa dei fornitori di

servizi, sia su segnalazione diretta degli interessati che, infine, su suggerimento o ordine delle autorità. Nella seconda categoria rientrano invece le ipotesi di sequestro materiale del *server*, come avvenne nel caso del sequestro del sito di *streaming* e condivisione *Megaupload* per ragioni di violazione della proprietà intellettuale. In questo caso il sequestro fu possibile grazie alla collaborazione tra le autorità statunitensi e quelle canadesi, dove i *server* si trovavano dislocati fisicamente.

Uno strumento in grado di limitare la circolazione di informazioni suppostamente illecite è quello di *ordinare ai motori di ricerca di non indicizzare* uno specifico contenuto o un argomento in generale. Tra i primi spicca il caso *About Elly* nei confronti di *Yahoo*[46], quando a quest'ultima fu ordinato di rimuovere risultati che rinviavano a copie illecite del film. Tra i secondi rientrano le pratiche di Google, nei diversi paesi dove opera, di eliminare dai propri risultati pagine su indicazione delle autorità, frequentemente correlate a argomenti politici o religiosi sensibili[47]. Degna di nota, benché per ragioni temporali sia impossibile

---

[46] Per un dettaglio del caso, MULA D., *Responsabilità del motore di ricerca nel caso About Elly: fraintendimenti informatici a base di un'ordinanza (revocata) dal contenuto anomalo*, in *Diritto Mercato e Tecnologia*, http://www.dimt.it/2013/09/14/responsabilita-del-motore-di-ricerca-nel-caso-about-elly-fraintendimenti-informatici-a-base-di-unordinanza-revocata-dal-contenuto-anomalo/ (verificato il 12.05.2014) e in *Responsabilità Civile*, in corso di pubblicazione, e per l'ordinanza v. IASELLI M, *Caso "about Elly": non convincono le conclusioni del giudice cautelare*, in Altalex, 9.11.2011, http://www.altalex.com/index.php?idnot=15048 (verificato il 12.05.2014).

[47] Un riepilogo di alcuni casi di censura riportati in relazione ai diversi servizi offerti da Google è disponibile sulla pagina in lingua inglese *Censorship by Google* di Wikipedia, http://en.wikipedia.org/wiki/Censorship_by_Google (verificato il 12.05.2014). Maggior dettaglio è disponibile alla pagina *Censorship of Youtube*, dedicata invece alla soppressione di contenuti del più noto e utilizzato servizio di pubblicazione e diffusione di video al mondo,

proporre in questa sede un approfondimento, è la recentissima sentenza della Corte di Giustizia dell'Unione Europea, decisione C-131-12 del 13 maggio 2014[48], *Google Spain* e *Google Inc.* c. *Gonzalez* e Autorità spagnola per la protezione dei dati personali, che comporterà la possibilità, per i cittadini, di richiedere la rimozione dei link a pagine che li riguardino. Pur essendo tale possibilità sottoposta a condizioni, il risultato presumibile nel breve periodo sarà un aumento dell'opera di censura nella proposizione dei risultati dei motori di ricerca, attraverso formulari di richiesta in tal senso, il cui esito, sarà da vedere, potrebbe essere determinato in via automatica.

Quando la prima possibilità è, per diverse ragioni, preclusa, uno Stato può intervenire a livello di *access providers*, pubblicando una *blacklist* di siti oppure ordinando il *blocco all'accesso* verso un sito specifico tramite interdizione della risoluzione del DNS. La prima ipotesi è, in Italia, rappresentata perlopiù dalle *blacklist* di siti di scommesse online e di siti con contenuti pedopornografici. Il caso più noto di intervento della giurisprudenza per l'interdizione della risoluzione di un sito è ciò che accadde con *The Pirate Bay*, per ragioni

http://en.wikipedia.org/wiki/Censorship_of_YouTube (verificato il 12.05.2014), e al report di *Open Net Initiative Youtube Censored: a recent history*, https://opennet.net/youtube-censored-a-recent-history (verificato il 12.05.2014). Un interessante articolo, LOPEZ-TARRUELLA (a cura di), *Google and the Law* in *Information Technology and Law Series* V. 22, 2012

[48] La decisione è disponibile al sito della Corte di Giustizia dell'Unione Europea, http://curia.europa.eu/juris/documents.jsf?num=C-131/12 (13.05.2014). Sul diritto all'oblio, si veda PIZZATTI F. (a cura di), *Il caso del diritto all'oblio*, Giappichelli, Torino, 2013, e MAYER-SCHONBERGER V., *Delete. Il diritto all'oblio nell'era digitale*, EGEA, Milano, 2010.

di violazione della proprietà intellettuale[49].

Infine, sempre a livello di *access providers*, è possibile che si intervenga, in situazioni particolari, al fine di prevenire e bloccare la generale funzionalità di *Internet*. Questa ipotesi, l'estremo atto, è avvenuto in alcuni specifici contesti, quali, tra altri, il Nepal nel 2005[50], la Birmania nel 2007[51], l'Egitto nel 2011[52] - si veda per questo episodio l'illuminante rappresentazione visiva tramite grafico di ciò che accadde al traffico su *Internet* della rete egiziana tra il 27 e il 28 marzo del 2011 (figura 4) – e la Siria nel corso del 2012, del 2013 e del 2014[53].

---

[49] Per la sent. 49437 del 23 dicembre 2009 della Corte di Cassazione, e relativa nota di ALU F., *Caso "The Pirate Bay": la parola della Cassazione su file sharing e peer-to-peer*, del 11.02.2010, si veda in *Altalex*, http://www.altalex.com/index.php?idnot=48812 (verificato il 12.05.2014)

[50] Si veda il report di *Open Net Initiative* dedicato al Nepal, https://opennet.net/research/profiles/nepal (verificato il 12.05.2014).

[51] L'*Internet blackout* in Birmania/Myanmar nel 2007, in occasione della rivolta dei monaci buddhisti, è esaminato nel report di *Open Net Initiative*, *Pulling the Plug: A Technical Review of the Internet Shutdown in Burma*, alla pagina https://opennet.net/research/bulletins/013 (verificato il 12.05.2014).

[52] In merito al *blackout* della rete in Egitto, tra i citati esempi il più noto e seguito, si veda su *Open Net Initiative*, *Egypt's Internet Blackout: Extreme Example of Just-in-time Blocking*, https://opennet.net/blog/2011/01/egypt%E2%80%99s-*internet*-blackout-extreme-example-just-time-blocking (verificato il 12.05.2014), e sul sito dell'*Electronic Frontier Foundation*, *Egypt's Internet Blackout Highlights Danger of Weak Links, Usefulness of Quick Links*, https://www.eff.org/deeplinks/2011/02/egypts-*internet*-blackout-highlights-danger-weak (verificato il 12.05.2014).

[53] Per un'introduzione su *Internet* e i relativi *blackout* in Siria, http://en.wikipedia.org/wiki/*Internet*_censorship_in_Syria (verificato il 12.05.2014).

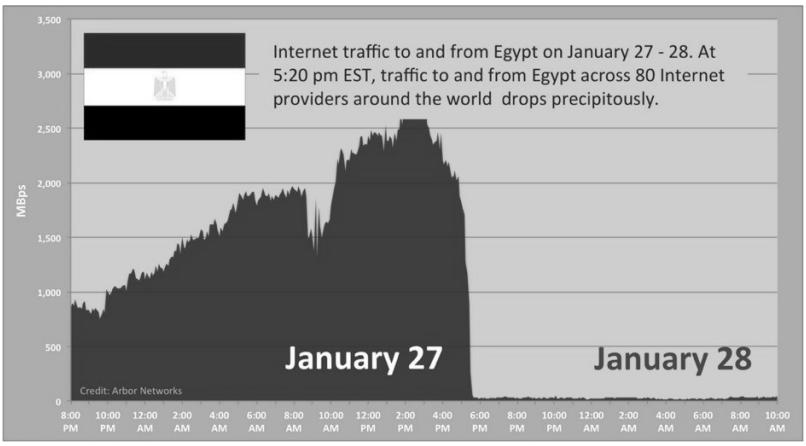

Figura 4 *Internet* blackout in Egitto, 2011.

Nelle ipotesi di intervento da parte di uno Stato sui fornitori di servizi, siano essi *information retrieval tools*, *hosting* o *access provider*, sia per la rimozione di un contenuto o di un risultato di ricerca sia per la fornitura di accesso a specifiche persone o alla globalità degli abitanti di un determinato Stato o regione, sono possibili due diversi scenari: o l'ISP è nel diretto controllo e proprietà dello Stato, come nel caso dell'*Internet shutdown* della Birmania nel 2007, nel qual caso la scelta adottata viene operata senza passaggi mediati, oppure l'ISP è privato, come nella medesima ipotesi ma nell'Egitto del 2011, e lo Stato ne ordina la collaborazione nelle forme e nei modi del proprio ordinamento. Collaborazione che, come ben si può immaginare, non soggiace necessariamente a regole di partecipazione democratica o di particolare trasparenza procedimentale.

3.3. Delega e appropriazione delle funzioni pubbliche

Il panorama fin qui delineato nelle sue declinazioni contemporanee può essere compreso attraverso l'osservazione di due dinamiche diverse che attengono il rapporto tra pubblico e privato nella gestione delle risorse economiche e nell'esercizio delle funzioni sociali non limitatamente al contesto delle ICTs: da una parte la tensione alla delega da parte delle istituzioni pubbliche, su propria iniziativa, di determinate funzioni all'ambito privato e, dall'altra, l'appropriazione da parte dei privati di ambiti e spazi ove agire in autonomia, così come il consapevole allargamento di quelli già loro affidati.

La *delega di funzioni ai privati* trova le proprie fondamenta in tre motivazioni di carattere politico-economico che, per quanto riguarda l'ordinamento italiano, sono state sancite dalla legge 241/1990: il perseguimento degli obiettivi di efficienza, efficacia ed economicità dell'azione amministrativa. Tali obiettivi, assunti come paradigmi in relazione ai quali valutare l'operato delle istituzioni pubbliche, hanno costituito la base giuridico-teorica giustificatrice della necessità di ricorrere a soggetti terzi rispetto agli apparati amministrativi dello Stato per l'esercizio delle proprie funzioni. Tale discorso, se traslato nei termini che qui ci interessano, ossia l'inquadramento del fenomeno dell'elevata influenza dei soggetti privati sull'intero ambito delle telecomunicazioni, poggia sull'inconfutabile considerazione che questi hanno nella propria disponibilità la gestione delle infrastrutture di telecomunicazione. Come si è appena delineato, ciò avviene a partire dalle diverse piattaforme *web* con il quale le persone possono interagire (*blog*, *social network*, *chat*, motori di ricerca, *webmail*), passando per la definizione dei protocolli di trasmissione e la gestione di tipo privatistico dell'attribuzione dei nomi a dominio, per arrivare fino, nella gran

maggioranza dei casi, alla materiale proprietà delle linee di trasmissione, siano esse composte da cavi ovvero reti *wi-fi* o satellitari.

L'espressione di un proprio pensiero all'interno del quadro così delineato finisce in balia di una pluralità di soggetti terzi a partire dall'istante stesso nel quale, assunta una forma digitale, viene indirizzato al di fuori del piccolo territorio virtuale, rappresentato dal nostro dispositivo, del quale ci sentiamo *dominus* incontrastati. Si pensi inoltre alla portata degli strumenti di *cloud computing* in tale prospettiva: abbandonando la disponibilità materiale di *software* di elaborazione dei dati prima e di *hardware* per la loro memorizzazione poi, l'utente stesso, non più titolare di diritti simil-proprietari ma ora fruitore di servizi a lui forniti da terzi, anticipa la frontiera di tale perdita di controllo dal momento della trasmissione del pensiero in forma digitale al momento stesso della sua digitalizzazione[54]. Quella stessa, già ridotta, porzione di territorio virtuale all'interno della quale si opera la trasposizione di espressioni di pensiero in dati digitali è quindi, nel caso dei servizi di *cloud computing*, così come nelle ipotesi di ricorso a dispositivi mobili o fissi aziendali o ancora se fosse utilizzato il *computer* messo a disposizione in un *Internet café*, affidata ad altri.

Da questo panorama deriva l'ovvia considerazione che tale pluralità di soggetti fornitori di servizi o comunque gestori delle

---

[54] Tale dinamica è efficacemente spiegata e riassunta in DE FILIPPI P., MCCARTHY S., *Cloud computing: legal issues in centralized architectures*, in *Neutralidad de la red y otros retos para el futuro de Internet*, p. 225, dagli Atti del VII Congresso Internazionale su *Internet*, Diritto e Politica, svoltosi il 12 e il 13 luglio 2011 presso l'*Universitat Oberta de Catalunya*, disponibili all'indirizzo
http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8341/7/IDP_7.pdf
(verificato il 12.05.2014), secondo i quali "*there is a trend fueled by the shift of control from end-users towards increasingly centralized services providers*".

infrastrutture *software* e *hardware* che permettono la circolazione dei dati, avendo disponibilità diretta della materialità dei beni coinvolti, risultino i più accreditati al fine di svolgere attività di sorveglianza e prevenzione, e ancor più di controllo e repressione. Tali operazioni infatti, richiedendo interventi diretti sulle infrastrutture di trasmissione così come sui dati ivi circolanti, possono ben essere condotte direttamente da quegli stessi soggetti in modo certamente più efficiente, efficace ed economico di quanto non potrebbe fare lo Stato, attraverso il ricorso alle strutture generalmente preposte allo svolgimento di tali attività. Chi meglio dell'amministratore di un sito di *hosting* o *webmailing*, o del delegato preposto a tali attività, può infatti intervenire per rimuovere un contenuto illecito, o anche solo scoprirne l'esistenza, individuarne la posizione e segnalarlo alle autorità competenti?

Di fronte all'ovvietà di tale osservazione il giurista o anche il cittadino che veda il diritto quale strumento al servizio di un ordine ispirato a principi di giustizia, equità e trasparenza, ossia a quella supremazia del diritto funzionale ad un sistema democratico costituzionale garante dei diritti fondamentali della persona, non può non notare che l'apparente buon senso che l'ammanta altro non sia che una elevata dose d'ingenuità, feconda di effetti indesiderati potenzialmente distruttivi. La definizione dei confini tra diritti e interessi contrastanti, così come le procedure per l'accertamento in concreto di eventuali illegittimità, rappresentano il fulcro, dalla prospettiva giuridica, dell'esistenza stessa di questi diritti. Come si avrà modo di approfondire in seguito[55], la disciplina dei limiti alla libertà di espressione è ben definita, benché complessa, e le decisioni da assumere in tale

[55] V. CAP II, *Libertà di espressione e diritti digitali*.

complessità, alla luce delle potenzialità lesive di qualsivoglia forma di limitazione, devono rispondere a requisiti particolarmente stringenti[56]. Ancor più pressante risulta la necessità di svolgere l'attività di bilanciamento nelle sedi competenti, caratterizzate dal più elevato tasso di trasparenza, terzietà e imparzialità, oltre che dalla garanzia della possibilità di partecipazione, nelle ipotesi di inquadramento dei nuovi diritti specificamente sorti nel contesto digitale: il diritto all'oblio[57], il diritto all'anonimato[58] e il diritto di accesso a *Internet* e alle informazioni, quali nuove declinazioni rispettivamente del diritto alla dignità personale, del diritto alla riservatezza e alla protezione dei propri dati personali e del diritto alla libertà di espressione.

L'altra faccia della medaglia di questo fenomeno di privatizzazione delle attività di sorveglianza, controllo, prevenzione e repressione di forme di espressione attraverso *Internet* è l'*appropriazione di funzioni tipicamente pubbliche da parte dei soggetti privati* in relazione alla posizione appena descritta che questi ricoprono. Questa assunzione di funzioni di sorveglianza da parte di soggetti privati nasce e si sviluppa

---

[56] Come si vedrà meglio nel prosieguo, nell'ambito del diritto europeo spicca l'art. 52 della Carta dei diritti fondamentali dell'Unione Europea, ove afferma, sul modello della Convenzione Europea dei Diritto dell'Uomo, i principi di necessità, proporzionalità e ragionevolezza ai fini della limitazione dei diritti: "eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui"

[57] V. *supra*, nota 48.

[58] Tra tutti, in italiano, FINOCCHIARO G., *Diritto all'anonimato. Anonimato, nome, identità personale*, CEDAM, Padova, 2008. Per i profili sociali e tecnici, vedi CAP III, *Sorveglianza Globale e Resistenza Digitale*, par. 5 e ss.

quale esercizio di facoltà riconducibili al diritto di proprietà per trascenderne in via del tutto fattuale i limiti, così d'avvicinarsi sensibilmente più all'atto di imperio di tipo pubblicistico. Procedendo attraverso alcuni esempi, si possono ricondurre a tale dinamica l'approvazione e l'implementazione di *policies* sul modello delle condizioni generali di contratto finalizzate a definire la liceità o meno di taluni utilizzi dei servizi forniti ed eventualmente i procedimenti di risoluzione di controversie, ovvero la definizione sommaria di casi non originariamente previsti attraverso il rinvio di clausole aperte o attraverso il mero esercizio di autorità, ovvero ancora la scelta di escludere soggetti da servizi offerti o di cancellare contributi pubblicati in virtù della semplice preferenza in un senso o nell'altro e della possibilità materiale di compiere tale azione. Tali attività decisorie saranno esplicite e trasparenti quando apertamente rivendicate e basate su *policies* portate a conoscenza e accettate consapevolmente dal fruitore di servizi, come nel caso di affermati operatori transnazionali fornitori di servizi su larga scala o di operatori della stampa soggetti a discipline particolari. Potranno invece svolgersi in forma del tutto implicita e sulla base delle mere possibilità di fatto di svolgere operazioni censorie nel caso, estremamente diffuso, della creazione e gestione di spazi personali e non professionali, quali *blog*, *forum* o pagine *web*, aperti ai contributi della comunità.

Quest'ultima distinzione tra sussistenza o meno di *policies* che esplicitamente prevedano casi, ragioni e modalità di risoluzione delle controversie non tragga però in inganno quanto a potenzialità lesive dei diritti fondamentali, in particolare del diritto alla libertà di espressione, delle persone. La mera esistenza di regolamentazioni dei termini di utilizzo dei servizi messi a disposizione non preclude in alcun modo la sussistenza di violazioni dei diritti fondamentali delle persone. Al

contrario i termini stessi ben possono rappresentare una cristallizzazione normativa di tale mancato rispetto. Il risultato di un simile gioco delle tre carte consiste infatti nello spostare i termini della questione dall'illiceità di clausole contenute nei termini stessi per contrasto con le statuizioni dei diritti fondamentali alla legittimità o meno del consenso prestato dal fruitore dei servizi ivi regolati. Quest'ultima problematica, fondamentale per stabilire sussistenza e validità della manifestazione di volontà di un soggetto in ambito contrattuale con le conseguenti ricadute in termini di applicabilità o meno di quanto *ivi* previsto, nulla rileva sotto il profilo, anche questo sostanziale, della conformità della sottostante regolamentazione privata alla luce dell'ordinamento giuridico nazionale e sovranazionale.

Tornando infatti agli esempi poc'anzi presentati, l'esistenza o meno di termini di utilizzo, nella parte in cui sia loro riconosciuta validità giuridica, può fondare eventuali richieste risarcitorie in termini civilistici nelle ipotesi di scorretto utilizzo da parte del fruitore o di mancata prestazione da parte del fornitore. Saranno invece le pratiche effettive da giudicare assunto quale paradigma il complesso di norme imperative dell'ordinamento giuridico di riferimento, tra le quali non è più rinviabile una piena assunzione delle previsioni costituzionali nazionali, sovranazionali ed internazionali.

In questa direzione sono numerosi i contributi, non solo dottrinali, all'elaborazione di carte dei diritti pensate proprio in relazione alle peculiarità delle ICTs o di modelli specifici riguardanti le responsabilità degli intermediari. Rinviando ai relativi capitoli l'approfondimento del dettaglio di alcune di questi contributi, si può tra i primi evidenziare la

Carta dei Diritti Umani e principi per Internet[59], modellata sulla Dichiarazione Universale dei Diritti dell'Uomo, e la proposta di un *Bill of Rights in Cyberspace*[60]. Tra i secondi invece le proposte di riforma della Direttiva UE sul commercio elettronico.

3.4. Un esempio dalla materialità: la privatizzazione della "piazza" negli USA

Prima di giungere a conclusione di questo breve percorso finalizzato all'inquadramento del fenomeno della privatizzazione della censura nella società dell'informazione, sia permesso un *excursus* su un fenomeno del tutto assimilabile e con simili conseguenze in termini di esercizio dei diritti fondamentali. Si intende riferirsi alle conseguenze dell'evoluzione degli spazi sociali in numerose metropoli mondiali architetturalmente concepite di modo da ridurre, o persino escludere, l'esistenza di spazi comuni di proprietà pubblica a favore di spazi privati aperti al pubblico. Al posto di piazze e strade e parchi, luoghi per eccellenza deputati al libero esercizio pubblico dei diritti di libertà da parte della cittadinanza, intere comunità hanno visto sostituirsi sale di attesa, sottopassaggi o pontili e spazi di ristoro usufruibili in termini di servizio da parte dei consumatori che vi transitano. Questo modello, che parrebbe a prima lettura da parte di una persona cresciuta nello spazio

---

[59] Il testo della Carta, elaborate in seno all'*Internet Rights and Principles Coalition*, è disponibile all'indirizzo http://*internet*rightsandprinciples.org/site/charter/ (verificato il 12.05.2014).

[60] Tra le diverse, http://buzzmachine.com/2010/03/27/a-bill-of-rights-in-cyberspace/ (verificato il 12.05.2014).

comune europeo più vicina a film di fantascienza o distopie letterarie, è applicato in una pluralità di città americane e non mancano giuristi, perlopiù costituzionalisti accorti, che sollevino la questione di quale spazio rimanga, in un simile contesto giuridico-architettonico, per l'esercizio dei fondamentali diritti di libertà dei cittadini. Tale fenomeno è stato ben affrontato da Joel BAKAN, costituzionalista canadese, che nella sua importante opera *The Corporation: the pathological pursuit of profit and power*, ha modo di affermare:

> La "strada" - termine che denota non solo le strade ma anche gli altri spazi pubblici quali le piazze – occupa uno spazio centrale nell'immaginario democratico. È uno spazio pubblico urbano, un luogo dove le persone si incontrano e aggregano, dove conducono battaglie, protestano, marciano, picchettano, gridano attraverso megafoni, fanno circolare varie forme di informazione, e semplicemente godono della loro libertà di essere in pubblico. L'idea della libertà di parola prende molto del suo potere evocativo dalla strada, sia attraverso immagini dei manifestanti in piazza Tienanmen, *soapbox* oratori allo Speaker's Corner all'Hyde Park di Londra, o le marce per i diritti civili e del lavoro attraverso le strade di periferia.[61]

---

[61] "The "street" - a term that denotes not only streets but uther public places such as plazas and town squares -occupies a central place in the democratic imagination. It is a public urban space, a place where people meet and congregate, where they rally, protest, march, picket, shout through megaphones, convey various forms of information, and simply enjoy their freedom just to be in public. The idea of freedom of speech draws much of its evocative power from the street, whether though images of protesters in

Se infatti è indubbio che, posti certi limiti distinti da Stato a Stato, ben sia ancora possibile fermarsi in una piazza qualunque di Milano, Parigi o Berlino ad esprimere pubblicamente le proprie idee attraverso la parola o la diffusione di materiali stampati, tale libertà è in dubbio o persino formalmente negata in quegli spazi privati aperti al pubblico sottoposti a regolamentazioni finalizzate all'ordinaria circolazione di merci, consumatori e capitali. Le ragioni di tale negazione, ben documentata nell'opera citata, risiedono in quel carattere necessariamente conflittuale che caratterizza il diritto alla libertà di espressione, così come gli altri diritti fondamentali di libertà, e che porta il suo riconoscimento ad un irrinunciabile margine di instabilità politica e sociale. Instabilità che è ben necessaria ad un ordinamento che rifugga la fossilizzazione all'interno di soluzioni precostituite e immutabilmente stabilite a disciplinare un presente che si vorrebbe riproposto in eterno, ma che al contrario è comprensibilmente mal vista, ed il più possibile esclusa, dagli operatori ispirati dal conseguimento di profitto sul consumo.

I tunnel e i passaggi sopraelevati urbani, così come i centri commerciali suburbani, sono luoghi disegnati e utilizzati per l'interazione pubblica ma di proprietà di grandi imprese private, generalmente corporazioni internazionali, che controllano cosa succeda e chi possa accedervi. Le guardie di sicurezza e i sistemi di sorveglianza sono onnipresente perché, come ha evidenziato un commentatore, "i proprietari devono mantenere un'atmosfera proficua allo svolgimento di

---

Tiananmen Square, soapbox orators at Speakers' Corner in London's Hyde Park, or civil rights and labor marches through downtown streets", BAKAN J., *The Corporation: the pathological pursuit of profit and power*, Simon & Schuster, 2004, p. 130.

attività commerciali, che ha bisogno della proibizione di quei soggetti del pubblico e di quelle attività percepite come pregiudizievoli a questo obiettivo"[62] - come, per esempio, picchettatori, manifestanti, attivisti che volantinano, e senzatetto. Siccome centri commerciali, tunnel e passaggi sopraelevati sono, si ribadisce, proprietà privata, l'esercizio dei diritti alla libertà di parola e assemblea può essere molto più facilmente limitato in questi luoghi piuttosto che nella proprietà pubblica.[63]

Richiamando un altro studio[64], Bakan sottolinea che questa tendenza è in atto anche nei contesti abitativi, con lo sviluppo di enclavi residenziali dotate di mura, cancelli, spazi aperti e *regolamenti interni*, di proprietà privata, che al tempo della redazione dell'opera avrebbero ospitato circa quattro milioni di cittadini statunitensi.

Questi rappresentano, nelle parole dell'opera citata, "una tendenza all'allontanamento dall'accresciuto controllo governativo sull'utilizzo del

---

[62] HOPKINS J., *Excavating Toronto's Underground Streets: In Search of Equitable Rights, Rules and Revenue*, in *City Lives and City Forms*, University of Toronto Press, 1996, p- 63

[63] "Urban tunnels and skywalks, along with suburban malls, are places designed and used for public interaction but controlled by private owners, generally large corporations, which control what happens and who can be on their premises. Security guards and surveillance equipment are ubiquitous because, as one commentator points out, "The proprietors must mantain an atmosphere conductive to business, which necessitates prohibiting those members of the public and activities they perceive as detracting from this objective" - such as, for example, picketers, protesters, leafleters, and homeless people. Because mall, tunnels, and skywalks are private property, citizens' exercise of rights to free speech and assembly can be more easily curtailed in these places than on comparable public property", BAKAN J, cit., pag.131.

[64] Lo studio a cui fa riferimento e da cui coglie le citazioni è MASSARONN ROSS M., SMITH L., PRITT R., The *Zoning Process: Private Land-Use Controls and Gated Communities: The Impact of Private Property Rights Legislation, and Other Recent Developments in the Law, Urban Lawyers*, v. 28, 1996, p. 802-803.

territorio e sulla fornitura di servizi da parte del Governo verso una dipendenza sempre maggiore sui controlli privati e sui servizi forniti dai privati", e "forniscono *una nuova e potente strada per escludere persone e attività non gradite*".[65]

Tali architetture urbane, benché in quantità molto più limitate, esistono e si diffondono anche nell'Europa continentale e nelle nostre periferie. Ma di maggior interesse per quanto qui rileva è l'estrema somiglianza di questo fenomeno di privatizzazione del territorio materiale, di sottrazione di tale territorio dall'ordinario governo pubblico, alla tendenza all'affidamento e alla crescita e allo sviluppo di territori virtuali ove l'unica normazione relativa ai diritti di accesso e di utilizzo dei servizi è affidata alle scelte, di natura privatistica e tendenzialmente insindacabili, degli operatori privati. Questi ultimi, verso gli Stati e le autorità, si limitano a fornire informazioni ed eseguirne gli ordini di identificazione, blocco dell'accesso e conservazione dei dati, senza che vi sia più controllo della legittimità delle proprie pratiche di vero e proprio governo.

---

[65] "*The represent, in , in the words of one study, "a trend away from governmental control over land use and governmental provision of services and toward an increased reliance on privately created controls and privately supplies services", and "provide a new and more potent way to exclude unwanted persons and uses*", BAKAN J., cit., p. 131-132.

4. Legittimo o possibile: la tecnologia, l'esercizio dei diritti e la sorveglianza globale

La seconda dinamica più rilevante è la crescita del peso della tecnologia, del codice informatico, sulla risoluzione di istanze giuridiche contrapposte e, in ultima analisi, sul governo della società. Il codice informatico, nella contemporanea società dell'informazione digitale, diventa regola che disciplina l'agire, umano e non, con una forza cogente ben superiore a quella delle norme di fonte giuridica. Com'è stato lucidamente analizzato[66], la diffusione globale di *Internet* a metà degli anni '90 del secolo scorso ha suscitato un'ondata di entusiasmo liberale e libertario pari, se non superiore, a quello della di poco precedente caduta dell'Unione Sovietica. "L'affermazione per il ciberspazio non era solo che il Governo *non avrebbe dovuto* regolare il ciberspazio – era che il Governo *non avrebbe potuto* regolare il ciberspazio"[67], afferma Lessig richiamando lo spirito di quegli anni. La citata Dichiarazione di indipendenza del Ciberspazio di Barlow, pubblicata nel 1996, è esemplare sotto questo aspetto, quando così si esprime: "Governi del Mondo, stanchi giganti di carne e di acciaio, io vengo dal Cyberspazio, la nuova dimora della Mente. A nome del futuro, chiedo a voi, esseri del passato, di lasciarci soli. Non siete graditi fra di noi. Non avete alcuna

---

[66] LESSIG L., *Code v2.0*, Basic Books, New York, 2006, http://codev2.cc/download+remix/Lessig-Codev2.pdf (verificato il 12.05.2014).

[67] "*The claim for cyber-space was not just that government would* not regulate *cyberspace—it was that government* could not regulate *cyberspace*", LESSIG L., *ivi*, p. 3.

sovranità sui luoghi dove ci incontriamo"[68]. La forza dirompente della rete è vista e vissuta nelle sue più ampie potenzialità: il rifiuto stesso del modello di potere organizzato sull'esercizio di autorità.

Lessig anticipa però le prospettive infauste dello sviluppo di *Internet*, alla luce del suo primo decennio di vita globale. Il ciberspazio è naturalisticamente preposto, già dal nome individuato[69], alla realizzazione del controllo globale[70]. Individuando il fenomeno dell'affidamento al codice informatico e al commercio, con le dinamiche e gli interessi propri coinvolti, un ruolo preponderante nello sviluppo di *Internet*, Lessig centrò il punto e anticipò, con grande chiarezza, le problematiche oggi così pervasive. Il ciberspazio, nella sua più ampia e comprensiva definizione, è il terreno sul quale si sviluppano istanze divergenti: le reti di telecomunicazione riempiono di significato e allargano la portata del diritto alla libertà di espressione, di parola, di stampa, di ricerca delle informazioni, sono quindi in sostanza il più efficace ed effettivo strumento di trasmissione delle istanze costituzionalmente legittime di esercizio dei diritti fondamentali della persona, pur al tempo stesso rivelandosi prezioso strumento al servizio delle più moderne forme di criminalità o terrorismo, realtà per le quali la

---

[68] BARLOW J. P., *Dichiarazione di indipendenza del Ciberspazio*, 1996, al sito http://w2.eff.org/Censorship/*Internet*_censorship_bills/barlow_0296.declaration (verificato il 12.05.2014).

[69] Il termine nasce dalla fusione tra *cybernetics* e *space*. Il primo fu definito quale "studio scientifico del controllo e della comunicazione negli animali e nelle macchine", WIENER N., *Cybernetics, or Communication and Control in the Animal and the Machine*. MIT Press, Cambridge, 1948

[70] "*Left to itself, cyberspace will become a perfect tool of control*", LESSIG L., cit., pag. 4

ricerca di modalità sia per le comunicazioni private che per le rivendicazioni pubbliche rappresenta un elemento strutturalmente necessario; d'altro canto, le modalità di funzionamento tecnologico delle reti rendono disponibili sia una pluralità di strumenti e tecniche di anonimato e segretezza, sia di strumenti e tecniche di sorveglianza e controllo sull'attività e sulle informazioni personali della generalità delle persone. Attività e informazioni che possono essere acquisite dalle autorità sia perché volontariamente, ma spesso incautamente, pubblicate e diffuse dalle stesse persone coinvolte o da conoscenti o terze parti[71], sia in ragione di raccolta di dati e informazioni sulla navigazione e sulle preferenze svolte dai soggetti privati fornitori di servizi, sia infine in esito ad attività generali di sorveglianza, indagine e archiviazione, in conformità[72] o meno[73] con le discipline vigenti nei paesi di riferimento.

---

[71] Si pensi alla mole di informazioni personali di ogni genere che quotidianamente vengono diffuse dai diretti interessati, specie giovanissimi, o da loro conoscenti, attraverso i *social network*. Informazioni spesso riconducibili al concetto di dati sensibili per la tutela delle quali abbiamo alle nostre spalle quasi due decenni di legislazioni comunitarie e nazionali

[72] La totalità degli ordinamenti giuridici prevede reparti specializzati delle autorità amministrative e giudiziarie per il perseguimento di reati portati a compimento attraverso *Internet* e procedure legislative che disciplinano tali attività. In Italia la Polizia Postale svolge le proprie attività di indagine in conformità alle leggi sostanziali e procedimentali dell'ordinamento italiano. In Russia è prevista, sotto determinate condizioni non particolarmente stringenti, la possibilità di un controllo generale delle comunicazioni per finalità di prevenzione di attività terroristiche (legge federale 35-Z, 11.3.4) del 2006) e di attività estremiste di supporto o giustificazione al terrorismo (legge federale 114-FZ del 2002, modificata nel 2008).

[73] Oltre al recentissimo caso del Progetto PRISM, di cui si dirà meglio più avanti, al CAP III, *Sorveglianza Globale e Resistenza Digitale*, sono numerosi i casi di sorveglianza generalizzata condotta da soggetti privati o da autorità pubbliche al di fuori del recinto di legalità, quand'anche quest'ultimo sia particolarmente permissivo. In ambito privato, nel 2006 Vodafone in Grecia e

In ragione di considerazioni simili a quelle che motivano l'affermazione dell'importanza del ruolo dei soggetti privati, anche la *lex informatica* ha assunto una posizione di supremazia tale da incidere profondamente sull'ambito di azione e sulla portata del diritto. Al rapporto tra illiceità e liceità proprio della categorizzazione del diritto va gradatamente sostituendosi il rapporto tra possibilità e impossibilità di tipo tecnico-informatico. Gli ambiti di applicazione da cui trarre esempio di questa evoluzione sono i più disparati: le misure tecnologiche di protezione nell'ambito della gestione dei diritti derivanti dalla tutela della proprietà intellettuale su di un'opera multimediale, nel cui caso le azioni fisicamente esercitabili dai licenziatari su una certa opera vengono regolamentate a livello di codice, da parte dei licenzianti, in ragione dei termini della licenza stessa e, forse, delle previsioni legislative in materia di libere utilizzazioni; la separazione del codice sorgente dal codice oggetto, attraverso la pratica della compilazione, nell'ambito della gestione dei diritti relativi all'utilizzo di programmi per elaboratore, nel qual caso gli ambiti di operatività e soprattutto le modalità di esercizio dei propri diritti sono definite a monte dal licenziante senza che il licenziatario possa persino conoscerne l'effettiva portata; il cd. "sequestro preventivo" di *server* situati all'estero tramite ordine di inibizione della risoluzione di nomi a dominio agli ISP, nel cui caso, non potendo intervenire sulla materialità dei *server*, i *service providers*, su ordine dell'autorità giudiziaria, provvedono a modificare il funzionamento del DNS per inibire lo scambio di dati tra soggetti operanti in quel determinato territorio e il *server* così segnalato; e ancora, la gestione della circolazione dei propri dati personali in

Telecom in Italia furono travolte da scandali relativi a controlli e intercettazioni di politici e giornalisti dei paesi.

Internet, regolata non dalle pur stringenti norme europee e nazionali sul trattamento dei dati, in particolare sul consenso e sul trasferimento dei dati al di fuori dell'Unione Europea, bensì dal funzionamento di profili tecnici della rete, tra i quali *cookies*, *logs*, indirizzi IP, *geotagging* e metadati in genere[74].

Questi esempi servono anche a comprendere la stretta interdipendenza tra dominio privatistico e forza cogente della *lex informatica*. Su *Internet* le norme, siano esse leggi statali o *policies* private, devono ricorrete al codice per la loro implementazione, sia questa considerata dalla prospettiva di intervento preventivo al fine di promuovere o proibire un determinato comportamento, sia questa considerata dalla successiva necessità di provvedere su specifiche attività, individuarne gli autori, definirne gli elementi temporali o spaziali, elaborarne gli elementi probatori.

4.1. *Ad impossibili nemo tenetur*

Il ragionamento sul rapporto tra possibilità e illiceità è un discorso di fondo della dottrina giuridica. Come ricorda il brocardo latino assunto a fondamenta degli ordinamenti giuridici moderni, tale da considerarsi un principio proprio del contemporaneo Stato di diritto, "*ad impossibilia nemo tenetur*", ossia nessuno può essere obbligato all'impossibile. Una simile considerazione parrebbe ovvia di fronte al buon senso, ma in ogni caso l'affermazione di tale principio ha avuto risvolti determinanti nel mondo del diritto, avendo infatti fissato un limite naturale, e quindi

[74] Per il dettaglio su questi strumenti, v. CAP III, par. 2.

esterno, rispetto all'operatività delle regole giuridiche. Nessun senso avrebbero norme che stabilissero l'obbligo per i non udenti di non udire,, piuttosto che il divieto di teletrasportarsi. Ma al di là degli esempi deliberatamente eccessivi[75], tale principio trova applicazione nella totalità delle azioni quotidiane, tanto da aver meritato, nel nostro ordinamento giuridico come negli ordinamenti di altri Stati nazionali, una pluralità di specifiche previsioni normative che al concetto di impossibilità fanno riferimento, quali la possibilità dell'oggetto di un contratto e il concetto di forza maggiore, affini a quanto di qui si tratta, che permeano rispettivamente l'intero sistema civilistico, tanto da poter determinare la nullità di un accordo tra le parti o la risoluzione per impossibilità sopravvenuta, e il sistema penalistico, tanto da incidere sull'imputabilità di un soggetto per un reato. A seguito dell'esclusione dal mondo del diritto, dalla gestione del rapporto tra essere e dover essere, tutto quanto sia impossibile, risulta meglio definito l'ambito all'interno del quale possa operare un sistema giuridico completo e coerente con l'ambiente stesso che intende operare. L'assenza di previsioni incompatibili con il concetto di possibilità è uno degli indici di quella certezza del diritto e coerenza sistematica dell'ordinamento necessari affinché di Stato di diritto si tratti. È quindi in questo contesto, nel reame delle possibilità umane, che la società organizzata in istituzioni può validamente darsi regole, norme e leggi che stabiliscano divieti, obblighi, poteri, facoltà o diritti.

L'idea di escludere dalla normazione ciò che, alla luce delle leggi

---

[75] E ricordando comunque che eccessivi appaiono solo alla luce dei principi etici, giuridici e morali che abbiamo acquisito dall'età dei Lumi, posto che in diverse epoche storiche e contesti locali o culturali, finanche contemporanei, tale confine al mondo del diritto e, quindi, in ultima istanza, al potere, non fosse e non sia riconosciuto.

naturali, da noi immutabili, risulti fisicamente impossibile, è però un principio tanto più valido quanto definito e tendenzialmente immutabile è il confine tra possibilità e impossibilità. Non ha finora determinato infatti il venir meno della validità di tale principio l'ordinario sviluppo tecnologico, sociale ed economico della società umana. Se infatti anche solo cento anni fa un eventuale ordine di comparizione emesso nei confronti di una persona residente oltreoceano con la previsione di un termine di dieci giorni ben avrebbe travalicato il regime delle possibilità, un uguale ordine emesse oggi potrebbe al massimo essere considerato una forzatura, ma sicuramente non sarebbe riconducibile alla pretesa dell'impossibile. Ciò che ha permesso una sostanziale sopravvivenza, con annessa straordinaria utilità, del principio di cui si tratta è che lo sviluppo della società umana è stato accompagnato da un pari aggiornamento del diritto, in grado quindi di aggiornarsi via via che il discorso tecnico, la tecnologia, apriva nuovi spiragli di possibilità dove prima regnava l'irraggiungibilità.

Ma *il rapporto tra il binomio possibilità e impossibilità e il binomio liceità e illiceità nel contesto digitale* avviene in termini del alternativi e diversi rispetto al contesto dei rapporti tra tali concetti nel funzionamento della realtà materiale. Rispetto a quest'ultima, dall'umanità vissuta e sulla cui materialità di fondo, così come sulle cui regole fisiche che ne regolano l'esistenza non è possibile ancora intervenire, eccetto qualche rara punta di avanzamento scientifico, la virtualità delle reti di telecomunicazione determina che la loro stessa esistenza, le regole di funzionamento, ossia le leggi naturali del ciberspazio altro non siano che risultati pratici di scelte tecniche integralmente operate da persone umane. Come si è visto in precedenza, il sistema di *governance* di *Internet* ben mostra tale rapporto tra soggetti umani e determinazione delle regole tecniche di funzionamento delle

reti[76]. Sia che si tratti di protocolli di trasmissione, sia che si tratti di *software* per lo scambio di *email* o per lo svolgimento di attività di *social networking*, il ciberspazio è disciplinato da proprie leggi naturali stabilite, in ultima istanza, dall'uomo stesso. In questa prospettiva non rileva tanto il fatto che tali soggetti umani siano o meno riconducibili a concetti di istituzioni pubbliche o meno[77]. Ciò che rileva infatti è l'influenza originaria dell'umano sulla fonte delle leggi naturali dell'ambiente in cui noi persone operiamo. Nel primo caso, quello della realtà materiale, tali leggi derivano da un fattore esterno e da queste non possiamo, se non entro limiti molto stretti, allontanarci: l'interezza delle sfaccettature dell'esplicarsi della persona umana, della società e delle società umane è inevitabilmente vincolata all'intero di un sistema di regole sostanzialmente non modificabile. Diverso è invece il rapporto tra determinazione umana e regole di funzionamento dell'ambiente che ci circonda nella costruzione della virtualità: in questo caso è infatti una pluralità di soggetti che ha determinato e determina tuttora l'evoluzione strutturale delle reti di telecomunicazione, implementando appunto un protocollo piuttosto che un altro, ovvero intervenendo su di un qualsiasi codice affinché ne sia cambiata la natura o la funzione, così da modificare l'ambiente in cui altri soggetti operano e comunicano.

---

[76] V. *supra*, par. 3.2.

[77] Sebbene questo, come si è visto in precedenza, sia particolarmente rilevante sul piano della garanzia e del riconoscimento dei diritti fondamentali.

4.2. Diritto ed evoluzione tecnologica

Alla luce di questa distinzione, il principio giuridico richiamato, così come altri aspetti degli ordinamenti, vacilla sotto il peso dell'incessante sviluppo scientifico della società globale. La frequenza temporale con la quale le barriere dell'impossibilità sono travolte e nuovi ed estesi spazi di possibilità aperti ed offerti all'umanità è tale che il diritto, sistema di per sé orientato a un funzionamento di tipo conservativo ed eventualmente a un'evoluzione fondata sulle riforme, piuttosto che sulle rivoluzione, arranca, e arretra. E siccome la necessità di fissare limiti all'esercizio o all'accesso a certe possibilità è criterio d'ispirazione di qualsiasi sistema di regole, ove non arriva il diritto intervengono gli altri operatori della gestione dell'umano agire: il mercato, la società o la tecnologia stessa. Riprendendo però il discorso già avviato, sono stati presentati in precedenza i dubbi sull'affidabilità delle dinamiche del mercato al fine di soddisfare le esigenze di equità sociale ed uguaglianza rappresentate dalla concezione funzionale dello Stato di diritto. Se sul ruolo della società si intende approfondire in seguito, la tecnologia quale strumento di regolamentazione dei rapporti umani presenta problematiche in certi casi non dissimili da quelle evidenziate in relazione al ruolo dei privati.

Nella prospettiva del discorso sul sempre più rapido abbattimento delle barriere dell'impossibilità, i due settori applicati che operano in questo senso con maggior incidenza sono senza dubbio quello delle scienze mediche e quello delle scienze informatiche. L'affermarsi della discipline della bioetica e della natura fortemente interdisciplinare di tale materia di approfondimento altro non è che la reazione delle dottrine ad

un diritto che arriva in ritardo, e quando arriva non sa bene dove andare. Le applicazioni concrete delle scoperte scientifiche in ambito medico che aprono immensi spazi di nuove possibilità sono ormai numerosissime e investono ambiti più che sensibili: nuove possibilità in relazione al concepimento e alla creazione e alla modificazione genetica della vita; nuove possibilità in relazione alla gestione della morte, della vecchiaia e del dolore; nuove possibilità in relazione alla gestione quotidiana della vita umana, alla gestione e al superamento dei limiti fisici rappresentati dagli elementi che compongono il nostro corpo e dal loro sviluppo, con l'ausilio delle applicazioni in campo medico delle scoperte della robotica; nuove possibilità di intervento sul patrimonio genetico di piante e animali così da modificarne tratti e caratteristiche.

Di fronte a queste evoluzioni il tentativo del diritto, affiancato dall'etica e dalla filosofia, non è solo quello di ricomporre i bilanciamenti tra diritti e interessi diversi nel mutato contesto scientifico contemporaneo, ma dovrebbe essere quello di elaborare nuovi paradigmi, o presentare sotto una nuova prospettiva i paradigmi originari, affinché siano termine di paragone durevole nel contesto contemporaneo di rapida evoluzione. Non diversamente dev'essere guardata la sfida lanciata al diritto dalla rivoluzione digitale: affermare nuovi paradigmi che mantengano viva la supremazia del diritto non quale fine in sé stesso, ma quale storicamente acclarato mezzo capace di mantenere in vita spazi di autonomia e di libertà più elevati di qualsiasi altro sistema di regole.

Dinnanzi dunque a una tecnologia in grado di condizionale l'esistenza stessa dei diritti fondamentali della persona, persino in punto di mera trasposizione del proprio pensiero in una forma materiale, benché digitale, è necessario riprendere l'ancora attuale, pur risalente a più di vent'anni fa, affermazione dal filosofo del diritto Bobbio "il

problema di fondo relativo ai diritti dell'uomo non è oggi tanto quello di giustificarli, quanto quello di proteggerli. È un problema non filosofico, ma politico"[78]

4.3. Diritto e *Liberation Technologies*

Quest'ultimo aspetto relativo alla peculiarità del ruolo della *lex informatica* in relazione ai conflitti tra diritti in qualche modo collegati con le ICTs riguarda l'aspetto contrapposto all'utilizzo a fini di sorveglianza e controllo: l'infrastruttura e le modalità di funzionamento delle reti di telecomunicazione servono, a chi abbia competenze sufficienti, proprio ad aggirare in maniera più che efficace le normative e le loro applicazioni. Con uno sforzo da comparare al rischio dal quale un soggetto intenda difendersi, è possibile provvedere, sul piano tecnologico, a rimuovere le tracce che lasciamo quando operiamo sulla rete, a travalicare confini materiali e digitali imposti dalle autorità, oltrepassando quindi quel territorio a cui originariamente eravamo legati, a esercitare in forme nuove diritti fondamentali suscettibili di limiti nel contesto quotidiano della realtà materiale.

Se tale aspetto sarà approfondito in conclusione di questo elaborato[79], valga per ora sottolineare come lo spostamento dell'incontro tra istanze confliggenti sul piano tecnologico non è esclusivamente predestinato a determinare la nuova supremazia di governi autoritari ovvero di monolitiche multinazionali, bensì porta in sé tutti gli elementi,

---

[78] BOBBIO N., *L'età dei diritti*, Einaudi, Torino, 1990

[79] V. CAP III, *Sorveglianza Globale e Resistenza Digitale*, par. 5 e ss.

come l'esperienza quotidiana già mostra con chiarezza, necessari alla formazione e all'operatività efficace di gruppi sociali o individui le cui azioni sono finalizzate alla difesa di campagne politiche e sociali e, in estrema conclusione, dei diritti umani fondamentali minacciati dagli interconnessi autoritarismi contemporanei, economici, tecnologici e politici.

5. Globalizzazione, pluralità delle fonti ed effettività del diritto

Delineati i tratti fondamentali dell'influenza del mercato e della tecnologia sul mondo del diritto, si eleva da sé l'elemento caratterizzante l'epoca contemporanea che convoglia tale influenza. Secondo Ulrich Beck, parlando di globalizzazione ci si riferisce all'"evidente perdita di confini dell'agire quotidiano nelle diverse dimensioni dell'economia, dell'informazione, dell'ecologia, della tecnica, dei conflitti transculturali e della società civile, cioè, in fondo qualcosa di familiare e nello stesso tempo inconcepibile, difficile da afferrare, ma che trasforma radicalmente la vita quotidiana, con una forza ben percepibile, costringendo tutti ad adeguarsi, a trovare risposte"[80]. È la perdita dei confini, quel territorio quale elemento geografico del diritto nazionale, dell'agire umano nei suoi più svariati ambiti di esplicazione che caratterizza il fenomeno, al quale un'ampia letteratura ha dedicato la

[80] BECK. U., *Che cos'è la globalizzazione? Rischi e prospettive della società planetaria*, Carocci, Roma, 1999. p. 39

propria attenzione[81]. Questo dissolvimento dell'elemento territoriale è di immediato riscontro nei due settori sin qui affrontanti: il mercato è transnazionale e globale, gli attori che vi operano pensano e scelgono globalmente, alla luce di valutazioni economiche, giuridiche e sociali condotte sulla scorta delle analisi costi/benefici, i cittadini consumano prodotti e si servono di servizi la cui origine trascende il territorio della propria vita o lo Stato di appartenenza; le comunicazioni sono globali, la pubblicazione su un sito *Internet* raggiunge qualsiasi, salvo rare eccezioni, angolo del mondo, al pari delle comunicazioni via email o VoIP, e così la socialità abbraccia soggetti fisicamente distanti nel tempo di un istante.

Dinnanzi a questa evoluzione, le scelte degli Stati nazionali perdono quella posizione di supremazia nell'influire sulle scelte degli operatori economici o sulle stesse persone. L'approvazione di una disciplina più stringente in materia di protezione dei lavoratori o in materia fiscale, in luogo di raggiungere il ricercato risultato, da un lato, di migliorare le condizioni di lavoro di questa o quella categoria e, dall'altro, di sottoporre i profitti di una certa tipologia di attività a una nuova disciplina contributiva accrescendo quindi la quantità di risorse disponibili per la collettività, possono determinare la scelta di

---

[81] V., tra gli altri, BAUMANN Z., *Dentro la globalizzazione. Le conseguenze sulle persone*, Laterza, Roma-Bari, 1998, KLEIN N., *No Logo*, Baldini e Castoldi, Milano 2001, STIGLIZ J., *La globalizzazione che funziona*, Einaudi, Torino, 2006, e, da una prospettiva eminentemente giuridica, TEUBNER G. *La cultura del diritto nell'epoca della globalizzazione*, Armando, Roma, 2005, CASSESE S., *Il diritto globale. Giustizia e democrazia oltre lo stato*, Einaudi, Torino, 2009, FERRARESE M. R., *Il diritto al presente*, Il Mulino, Bologna, 2002 e FERRARESE M. R., *Le istituzioni della globalizzazione. Diritto e diritti nella società transnazionale*, Il Mulino, Bologna, 2000

delocalizzazioni altrove, con conseguente perdita di lavoro ed entrate fiscali. Se le politiche promosse dalla *World Trade Organization* (WTO) nei diversi Stati nazionali hanno semplificato e favorito, con l'apertura dei mercati cd. "in via di sviluppo" agli operatori internazionali, le pratiche di delocalizzazione fisica con incidenza sugli aspetti occupazionali e di diritto del lavoro, sono le ICTs e il loro utilizzo nel contesto dell'economia dematerializzata e della finanza globale che hanno permesso la piena realizzazione di quella libera circolazione di capitali, non più fisicamente ma virtualmente identificati, al di fuori della portata delle autorità tributarie nazionali.

Questo elemento investe la totalità degli ambiti oggetto di studio del diritto delle nuove tecnologie: la criminalità informatica trascende i confini nazionali, la disciplina della tutela dei dati personali si arricchisce dell'inestricata matassa di giurisdizioni coinvolte in un trattamento che interessa indefinite pluralità di nazioni, e tale destino travolge anche la disciplina del commercio elettronico o della tutela della proprietà intellettuale. Gli operatori di tutti questi ambiti, siano essi soggetti desiderosi di portare a compimento attività illecite o entità che scelgono questo o quell'ordinamento per le proprie attività economiche all'esito di un'analisi costi-benefici in termini di diritto applicabile, si muovono sostanzialmente prescindendo dall'esistenza dei confini nazionali geografici, ovvero con l'accortezza di dissolvere il proprio operato spezzettando le attività nel più ampio e confuso numero di giurisdizioni[82].

In termini giuridico-politici, il problema che si pone da queste

[82] Seguendo, *mutatis mutandis*, le costruzioni societarie a scatola cinese finalizzate ad eludere i controlli su assetti proprietari, conflissi di interesse, normative antiriciclaggio, fiscali e tributarie dei paesi in cui si opera.

considerazioni è che "la globalità moderna non ha il suo diritto comune, non ha una giurisdizione internazionale, non ha dispositivi di amministrazione e di polizia internazionale ovvero non ha fondato il concetto e i dispositivi di una sovranità internazionale globale o transnazionale"[83]. Di fronte ad un mercato ed una società globalizzate in pochi decenni le risposte istituzionali affrontano ancora, e non senza difficoltà evidenti, la fase di coordinamento regionale, mentre il ruolo globale delle Nazioni Unite, o delle agenzie e organizzazioni internazionali settorialmente specializzate quali il WTO per il commercio, il WIPO per la tutela della proprietà intellettuale, l'ISOC e l'ICANN per la gestione di *Internet*, è ben lungi dal rappresentare quel punto di difficile equilibrio per il governo dell'agire umano rappresentato dagli Stati su scala nazionale, anzi risente di un rilevante influsso della cultura imperiale del XX secolo.

Come si aveva avuto modo di chiarire nelle pagine precedenti, tale necessità di rappresentanza istituzionale di tipo giuridico non è fine a sé stessa, ma giustificata dalle considerazioni in materia di garanzie formali e sostanziali proprie di un ordinamento pubblico rispetto agli ordinamenti extra-giuridici. In contrapposizione a tale modello vi è l'intervento dei soggetti privati e, usando nuovamente le parole di Bakan, il pressante problema sociale rappresentato dal fatto che "il mandato legalmente definito della corporazione è di perseguire, senza sosta o eccezione, il proprio interesse, disinteressandosi delle conseguenze

---

[83] L. VECCHIOLI, *Il rischio della sovranità globale. Riflessioni a partire da Ulrich Beck*, G. Giappichelli editore, Torino, 2004, p. 34.

frequentemente dannose che possa causare agli altri"[84].

In un rilevante saggio sui media Marshall McLuhan, sociologo canadese, già nel 1966, a proposito del sistema audiovisivo e telefonico, ebbe modo di scrivere che "Archimede disse una volta: 'Datemi un punto di appoggio e solleverò il mondo'. Oggi ci avrebbe indicato i nostri mezzi di comunicazione elettronici dicendo 'Mi appoggerò ai vostri occhi, alle vostre orecchie, ai vostri nervi e al vostro cervello, e il mondo si sposterà al ritmo e nella direzione che sceglierò io. Noi abbiamo ceduto questi 'punti d'appoggio' a società private". Continua McLuhan, "una volta che abbiamo consegnato i nostri sensi e i nostri sistemi nervosi alle manipolazioni di coloro che cercano di trarre profitti prendendo in affitto i nostri occhi, le orecchie e i nervi, in realtà non abbiamo più diritti. Cedere occhi, orecchie e nervi a interessi commerciali è come consegnare il linguaggio comune a un'azienda privata o dare in monopolio a una società l'atmosfera terrestre"[85].

A fronte di una pluralità di soggetti economici ben organizzati su scala transnazionale, che a disposizione hanno un sistema tecnologico di telecomunicazioni decentralizzato e dunque ben calibrato sulle loro esigenze e il cui fine è il perseguimento del proprio mero interesse al ritorno economico, lo Stato, luogo istituzionale di perseguimento del sostanzialmente contrapposto interesse collettivo, non ha gli strumenti per adempiere, efficacemente, alla propria missione. Il sistema normativo in cui si trova a operare diventa plurale. A tale pluralismo non

---

[84] "*The corporation's legally defined mandate s to pursue, relentlessly and without exception, its own self interest, regardless of the often harmful consequences it might cause to others*" BAKAN J., cit., p. 2.

[85] MCLUHAN M., *Gli strumenti del comunicare*, Il Saggiatore, Milano, 1966, p. 79

corrispondono più divisioni verticali tra diversi ordinamenti giuridici nazionali basate sui relativi confini territoriali, ma una complessa stratificazione di divisioni orizzontali che interessano, transnazionalmente, i diversi soggetti coinvolti, e consistono dunque nella *lex mercatoria*, nella *lex informatica*, nel diritto e nella politica internazionali e nelle nuove norme sociali globali. All'analisi dell'influenza di questo pluralismo sul diritto alla libertà d'espressione e sulla visione sociale di tale libertà sono specificamente dedicati i successivi capitoli di questo elaborato, a partire dai profili costituzionali nazionali e internazionali dei diritti coinvolti e dei nuovi diritti digitali, verso le pratiche effettive di sorveglianza globale e di resistenza digitale, per arrivare dunque all'individuazione del paradosso insito al discorso socio-libertario delle Liberation Technologies e al ruolo della formazione, giuridica e non, all'uso cosciente delle nuove tecnologie.

CAP II – LIBERTÀ DI ESPRESSIONE E DIRITTI DIGITALI

SOMMARIO: 1. Universalismo dei diritti umani. - 2. Tipi di Costituzione, sistemi politici e diritti umani fondamentali. - 3. Disciplina giuridica del diritto alla libertà di espressione. – 3.1. Le fonti tradizionali del diritto alla libertà di espressione. – 3.2. I limiti alla libertà di espressione nella Costituzione italiana e nella giurisprudenza Costituzionale. – 4. Le fonti alternative dei diritti digitali. – 4.1. Il codice informatico. – 4.2. L'autonomia privata – 4.2.1. – La proprietà privata e i social network. – 4.2.2. La proprietà intellettuale e la diffusione della cultura – 4.2.3. (segue) i principi costituzionali in materia di libertà di espressione e il ruolo del giudice nell'attività di bilanciamento. Il caso Hadopi – 5. "Collateral murders": il bilanciamento improprio dei diritti e degli interessi. – 6. I limiti e la rete transnazionale: la prospettiva critica.

1. Universalismo dei diritti umani

L'idea dell'esistenza di diritti fondamentali propri della totalità delle persone ha raggiunto la più marcata affermazione con la proclamazione della Dichiarazione Universale dei Diritti dell'Uomo, approvata dalle Nazioni Unite il 10 dicembre del 1948[1]. Tale

[1] Il cui testo è consultabile in lingua italiana all'indirizzo http://www.ohchr.org/en/udhr/pages/language.aspx?langid=itn (verificato il 12.05.2014).

dichiarazione, risultato di un percorso motivato dalla considerazione, ripresa nel Preambolo, che "il disconoscimento e il disprezzo dei diritti umani hanno portato ad atti di barbarie che offendono la coscienza dell'umanità", ha rappresentato l'adesione da parte della neonata comunità internazionale all'approccio universalistico di quella filosofia e quell'etica del diritto che, nei secoli precedenti, avevano contribuito ad affermare l'esistenza di diritti naturali, giusti e inalienabili propri di ogni essere umano, di ogni persona, in quanto tale. Se ciascuno dei diritti ivi enunciati è frutto di un'evoluzione storica propria e diversa dagli altri, da ricercare in relazione alle specifiche carte dei diritti, leggi o convenzioni via via adottate dalle diverse società nell'arco della storia umana già dall'età antica, è con la Dichiarazione del 1948 che questo complesso di diritti viene considerato appannaggio dell'intera comunità umana, senza esclusioni di genere, nazionalità, etnia o età. Non a caso i primi due articoli della Dichiarazione sanciscono rispettivamente il principio di eguaglianza nella nascita di ogni individuo "in dignità e diritti"[2] e un elenco di motivi specifici, frequentemente addotti a ragione di discriminazione, sulla base dei quali non è possibile effettuare distinzioni a tale fine. Tale principio dell'eguaglianza umana, architrave dell'universalismo dei diritti umani, deve operare a prescindere dalle caratteristiche o idee della persona, ossia "senza distinzione alcuna, per ragioni di razza, di colore, di sesso, di lingua, di religione, di opinione politica o di altro genere, di origine nazionale o sociale, di ricchezza, di nascita o di altra condizione", e soprattutto a prescindere dal territorio cui appartiene, "sia indipendente, o sottoposto ad amministrazione

[2] Art. 1 della Dichiarazione, "Tutti gli esseri umani nascono liberi ed eguali in dignità e diritti. Essi sono dotati di ragione e di coscienza e devono agire gli uni verso gli altri in spirito di fratellanza".

fiduciaria o non autonomo, o soggetto a qualsiasi limitazione di sovranità". Intenzione dell'Organizzazione delle Nazioni Unite, erede dell'infausta esperienza della Società delle Nazioni e prima realtà sovranazionale con aspirazioni globali e universali della storia dell'umanità, era, con questa Dichiarazione, fissare "il fondamento della libertà, della giustizia e della pace nel mondo", "evitare che l'uomo sia costretto a ricorrere, come ultima istanza, alla ribellione contro la tirannia e l'oppressione", e "promuovere il progresso sociale e un miglior tenore di vita in una maggiore libertà"[3].

La Dichiarazione cristallizza un insieme di diritti umani fondamentali: il diritto all'eguaglianza, formale e sostanziale (artt. 1 e 7); i diritti alla vita, alla dignità e alla sicurezza (artt. 3, 4 e 5); i diritti di libertà, ossia alla libertà di pensiero e credo religioso, alla libertà di espressione e alla libertà di associazione, all'inviolabilità del proprio domicilio e della propria corrispondenza e alla libertà di movimento (artt. 18, 19, 20, 12 e 13). Tra tali diritti sono compresi inoltre i diritti politici, i diritti economico-sociali e i principi dell'*habeas corpus* e del giusto processo. Nella piena consapevolezza che la libertà, in una società composita, si possa pienamente riconoscere solo in presenza di limiti, la Dichiarazione sancisce che, tali limitazioni debbano essere poste, dalla legge, per due soli ordini di motivi: tra i primi la necessità di bilanciare gli stessi tra loro nel rapporto con altre persone; tra i secondi la necessità di rapportarli a un interesse generale, qui declinato nelle "giuste esigenze della morale, dell'ordine pubblico e del benessere

[3] Preambolo della Dichiarazione universale dei diritti dell'uomo, 1948.

generale in una società democratica" (art. 29[4]). Infine, come norma di chiusura, l'art. 30 stabilisce che i principi e i diritti enunciati in precedenza non possano in alcun modo e da parte di alcuno, sia esso "Stato, gruppo o persona" essere interpretati nel senso di consentire attività indirizzate alla negazione dei diritti e delle libertà stesse[5].

Le ragioni storiche della necessità di una proclamazione così solenne non risiedono solamente nel rifiuto delle esperienze della prima metà del XX secolo, che era stata caratterizzata, con le due guerre mondiali e la pluralità di conflitti su scala regionale e locale che l'avevano attraversata, dalle più profonde e sistematiche degradazioni dell'essere umano, ma anche e soprattutto dalla sentita necessità di tentare di portare alla globalità degli esseri umani quella tutela giuridica che aveva permesso evoluzioni importanti, ma fino a quel momento limitate alle esperienze di specifici Stati o paesi, nel riconoscimento e nella considerazione della dignità della persona.

Correttamente, si era individuato un nesso inscindibile tra i diritti fondamentali di libertà, i principi dello Stato di diritto costituzionale quali strumento di garanzia per l'esercizio dei diritti stessi senza costrizioni e senza il timore di abusi del regime politico vigente e il generale rispetto della dignità e della vita umana. Nel senso

---

[4] Art. 29 della Dichiarazione: "Nell'esercizio dei suoi diritti e delle sue libertà, ognuno deve essere sottoposto soltanto a quelle limitazioni che sono stabilite dalla legge per assicurare il riconoscimento e il rispetto dei diritti e delle libertà degli altri e per soddisfare le giuste esigenze della morale, dell'ordine pubblico e del benessere generale in una società democratica".

[5] Art. 30 della Dichiarazione: "Nulla nella presente Dichiarazione può essere interpretato nel senso di implicare un diritto di un qualsiasi Stato, gruppo o persona di esercitare un'attività o di compiere un atto mirante alla distruzione di alcuno dei diritti e delle libertà in essa enunciati".

contrapposto, si era evidenziato come le concezioni assolutistiche dello Stato, quali tra tutte l'ideologia nazional-socialista, non avrebbero potuto che comportare, con la negazione dei diritti sostanziali e dei principi dello Stato di diritto, un annullamento della persona umana in sé considerata. Alla luce di queste riflessioni si ritenne di dover indirizzare la neonata comunità internazionale verso un'estensione sul piano globale della concezione secondo la quale la persona umana è e sarebbe dovuto essere fine in sé, e mai un mezzo.

La nozione di diritto della persona, inviolabile e inalienabile, proprio di *ogni* individuo era infatti in realtà limitata alle elaborazioni teoriche di religiosi, filosofi e giuristi, tra i quali il ruolo più rilevante è stato svolto dal pensiero giusnaturalista. "Le prime formulazioni storiche dei diritti come diritti naturali prendevano le mosse dal concetto di uguaglianza naturale di tutti gli esseri umani e, di conseguenza, dalla considerazione di tutti come titolari"[6]. Le esperienze giuridiche, ossia il riconoscimento nel diritto positivo di diritti, libertà o principi fondamentali del diritto, per esempio in ambito penale, erano invece state ad allora limitate ad esperienze nazionali, quali la Magna Charta inglese del 1215 e la Dichiarazione d'Indipendenza degli Stati Uniti d'America del 1776, con successiva Costituzione e, in particolare, i relativi Emendamenti. Anche la stessa Dichiarazione dei diritti dell'uomo e del cittadino del 1789, nata dalla Rivoluzione francese, sebbene possa probabilmente essere considerato il testo formale più antico comprensivo di un'universale teoria dei diritti umani, in ragione del solenne principio sancito dall'articolo 1 ove si afferma che "gli

---

[6] PECES-BARBA G., *Teoria dei diritti fondamentali*, Giuffrè, Milano, 1993, p. 144.

uomini nascono e rimangono liberi e uguali nei diritti", presentava in realtà notevoli tratti discriminatori in piena contraddizione con l'universalismo professato.

In primo luogo, la Dichiarazione era ben limitata, nella sua rilevanza pratica, ad uno specifico paese di riferimento; e soprattutto, in secondo luogo, la Dichiarazione stessa escludeva dai propri destinatari le donne, tanto che, due anni dopo, nel 1791, fu pubblicata all'indirizzo dell'Assemblea Costituente francese la Dichiarazione dei diritti della donna e della cittadina[7], testo che fu dalla Convenzione rifiutato. Allo stesso modo, l'esperienza della Dichiarazione del 1789 mostrava pecche quanto all'elencazione dei diritti ivi contenuta: tra tutti, la proprietà privata, riconosciuto come diritto "inviolabile e sacro" all'art. 17[8].

L'obiettivo proclamato dalla Dichiarazione universale delle Nazioni Unite del 1948 è quindi quello di fungere, come rivendicato nella conclusione dello stesso preambolo, da " ideale comune da raggiungersi da tutti i popoli e da tutte le Nazioni", da perseguire "con l'insegnamento e l'educazione, il rispetto di questi diritti e di queste libertà" e "mediante misure progressive di carattere nazionale e internazionale, l'universale ed effettivo riconoscimento e rispetto". Un approccio pragmatico ovvio alla luce della debolezza dell'organizzazione internazionale, della profonda divisione politica della comunità globale. Questo approccio ne marcherà tuttavia un valore meramente

---

[7] Per la ricostruzione di questa interessante, e poco nota, vicenda, si veda la pagina dedicata sul sito di Wikipedia, http://fr.wikisource.org/wiki/D%C3%A9claration_des_droits_de_la_femme_et_de_la_citoyenne (verificato il 12.05.2014).

[8] Per le critiche al riconoscimento di un valore assoluto preminente alla proprietà privata, vedi *infra*, par. 4.2. e ss.

programmatico tale da, in assenza di quegli strumenti vincolanti e coercitivi che avevano fatto, in parte, la fortuna di alcune delle precedenti esperienze, confinarne effettivamente il valore a una mera dichiarazione di buone volontà, riconducibile a pieno titolo alle norme di *soft law*[9].

Alla luce di queste debolezze, ma comunque nella prospettiva promossa dalla Dichiarazione stessa, sarà infatti nuovamente sul piano nazionale, locale o comunitaristico e sul piano del diritto internazionale che il cammino dei diritti umani fondamentali riprenderà il proprio corso, e questi raggiungeranno l'apprezzabile estensione odierna. Sarà sul piano internazionale che verranno promulgate la Convenzione internazionale sui diritti civili e politici[10] e la Convenzione internazionale sui diritti economici, sociali e culturali[11] del 1966 ed entrate in vigore nel 1976. Entrambe queste convenzioni furono adottate nella forma di trattato internazionale vincolante, così come i due protocolli opzionali sull'instaurazione del Comitato per i Diritti Umani[12]

---

[9] A proposito del concetto di *soft law*, vedasi MOSTACCI E., *La soft law nel sistema delle fonti: uno studio comparato*, CEDAM, Padova 2008, e l'interessante VOLANTE R. (a cura di), *Soft law e hard law nelle società postmoderne*, Giappichelli, Torino, 2009.

[10] Testo integrale in lingua inglese disponibile all'indirizzo http://www.un.org/Pubs/CyberSchoolBus/treaties/civil.asp (verificato il 12.05.2014).

[11] Testo integrale in lingua inglese disponibile all'indirizzo http://www.un.org/Pubs/CyberSchoolBus/treaties/economic.asp (verificato il 12.05.2014).

[12] Testo integrale in lingua inglese disponibile all'indirizzo http://www.un.org/Pubs/CyberSchoolBus/treaties/pro_civil.asp (verificato il 12.05.2014).

del 1966 e sull'abolizione della pena di morte[13] del 1989.

A fianco di questa lenta progressione della comunità internazionale globale verso l'adozione di documenti e procedure sempre più vincolanti in materia, i passi più rilevanti saranno compiuti dai alcuni singoli Stati, intenti nell'immediato secondo dopoguerra ad affrontare nuovi processi costituenti. Tali processi furono caratterizzati, in particolare, dall'adesione alla teoria delle supremazia delle Costituzioni, o almeno di una norma fondamentale[14], una *grundnorm*[15], rispetto agli atti inferiori, tradotta in forme di controllo della conformità costituzionale degli atti gerarchicamente inferiori[16] e in procedure complesse di revisione costituzionale[17], e dal riconoscimento precipuo dei diritti umani fondamentali fissati anche nella Dichiarazione delle Nazioni Unite. Questo piano, proprio in ragione dell'effettività della giurisdizione degli Stati all'interno dei propri territori e sulle proprie popolazioni, porterà agli avanzamenti più tangibili in particolare nel campo dell'applicazione dei principi fondamentali dello Stato di diritto e

---

[13] Testo integrale in lingua inglese disponibile all'indirizzo http://www.un.org/Pubs/CyberSchoolBus/treaties/pro_aim.asp (verificato il 12.05.2014).

[14] Quale, per esempio, la *Grundgesetz* della Repubblica Federale Tedesca, consultabile in lingua inglese sul sito del Bundestag, https://www.btg-bestellservice.de/pdf/80201000.pdf (verificato il 12.05.2014).

[15] KELSEN H., *Lineamenti di dottrina pura del diritto*, a cura di R. Treves, Torino: Einaudi, 1952, e, diverso il modo di valutazione ma non il punto relativo al rapporto gerarchico tra norme, sempre KELSEN H., *La dottrina pura del diritto*, Torino, Einaudi, 1966.

[16] ZAGREBELSKY G:, MARCENO V., *Giustizia costituzionale*, Il Mulino, Bologna, 2012.

[17] PACE A, *La naturale rigidità delle costituzioni scritte*, Cedam Padova, 1995

del principio di eguaglianza, così come dei diritti politici e dei diritti di libertà. Se in un primo momento questo approccio era limitato agli Stati del cosiddetto blocco occidentale, con i processi di decolonizzazione prima e la caduta del muro di Berlino poi, questa diffusione su base nazionale di buona parte dei diritti umani fondamentali continua a espandersi, e altresì a nutrire il terzo livello di promozione, ossia quello comunitaristico caratterizzato dall'operato comune di Stati affini per posizione geografica e regime politico o economico.

È su quest'ultimo piano che si svilupperanno e tuttora si stanno sviluppando le evoluzioni più significative nel campo della promozione e della protezione dei diritti umani fondamentali. I primi passi sono sicuramente stati mossi, in questa direzione, dalle *due Europe*: la prima, rappresentata dal Consiglio d'Europa, organizzazione internazionale istituita nel 1949 che già nel 1950 adottò la Convenzione Europea per la salvaguardia dei diritti dell'Uomo e delle libertà fondamentali (CEDU), il cui contenuto ricalcò fedelmente parte della Dichiarazione universale delle Nazioni Unite e previde inoltre l'istituzione della Corte Europea dei Diritti dell'Uomo, competente a valutare e sanzionare le violazioni da parte degli Stati membri; la seconda invece che affonda le proprie radici nelle prime Comunità Europee e che ora è rappresentata dall'Unione Europea, si è progressivamente allargata oltre i sei Stati fondatori ed è oggi dotata di una Carta dei diritti fondamentali, con gli strumenti finalizzati a garantirne l'applicazione. Queste due Europe, con la loro interazione, contribuiscono a fare del Vecchio Continente, ad oggi, la punta probabilmente più avanzata quanto a estensione qualitativa e quantitativa della portata dei diritti umani fondamentali. In questa prospettiva, anche le altre realtà comunitarie che sono andate nascendo

ed affermandosi in altre regioni, quali l'Associazione delle Nazioni del Sud-Est Asiatico (ASEAN)[18], la Lega Araba[19] e la Comunità delle Nazioni del Sud America (UNASUR)[20], hanno intrapreso percorsi che, benché caratterizzati da peculiarità tutt'altro che irrilevanti nella visione concettuale e pratica dei diritti umani, possono considerarsi non dissimili.

2. Tipi di Costituzione, sistemi politici e diritti umani fondamentali

Al fine di poter affrontare il merito della tutela dei diritti fondamentali nel contesto globale, si ritiene necessario osservare alcune peculiarità critiche dei risultati dei processi di costituzionalizzazione intrapresi sul piano nazionali, a partire dalle distinzioni teoriche tra tipi di Costituzione, passando per l'individuazione degli elementi distintivi e

---

[18] L'ASEAN, benché buona parte degli Stati membri non abbia carattere né democratico né costituzionale, nel senso che si vedrà nel prosieguo, ha adottato nel novembre 2012, a Phnom Phen, una propria Dichiarazione dei Diritti Umani, consultabile in lingua inglese all'indirizzo http://www.asean.org/news/asean-statement-communiques/item/asean-human-rights-declaration (verificato il 12.05.2014).

[19] Dopo una prima versione del 1994, la Lega Araba ha adottato una propria Carta, l'*Arab Charter of Human Rights*, consultabile all'indirizzo dell'Università del Minnesota, http://www1.umn.edu/humanrts/instree/loas2005.html?msource=UNWDEC19001&tr=y&auid=3337655 (verificato il 12.05.2014). Avendo questa carta numerosi riferimenti a principi religiosi e discriminatori, profonde solo state le critiche rivolte nei confronti delle disposizioni contenuto e professate.

[20] Pur non avendo l'UNASUR ancora adottato una propria Carta, è del 2013 la decisione dell'istituzione di un corpo permanente finalizzato alla trasposizione all'interno dell'Organizzazione della Convenzione Americana sui Diritti Umani, adottata in seno all'Organizzazione degli Stati Americani nel 1979.

gli elementi comuni dei diversi regimi politico-costituzionali.

La Costituzione, quale atto normativo fondamentale che definisca i rapporti tra soggetti e poteri, è infatti oggi tratto caratteristico della globalità degli Stati contemporanei. La dottrina costituzionalistica[21] distingue modelli di costituzione a seconda della loro procedura di revisione, della loro lunghezza, del loro carattere orale o scritto, e dell'incorporazione o meno dei diritti dell'individuo all'interno del corpo principale del testo. La classificazione più rilevante è quella che sottolinea che parlare di costituzione può comportare il riferirsi a fenomeni ben diversi tra loro: da una parte la *costituzione in senso formale*, ossia le regole stabilite di principio in uno o più atti specifici; dall'altra la *costituzione materiale*, ossia l'effettiva vitalità di quelle stesse regole all'interno della comunità di riferimento, come esse siano applicate o disapplicate, come siano le stesse integrate da prassi, costumi, in particolare quando il trascorrere del tempo e i mutamenti politici, sociali ed economici ampliano la discrasia presente tra realtà e tutte le forme di normativa fissa, in definitiva la costituzione vivente; un terzo fenotipo di *costituzione è quella in senso sostanziale*: la dottrina che distingue la costituzione materiale da quella sostanziale caratterizza quest'ultima, ispirandosi ai principi al giusnaturalismo e al costituzionalismo del secondo dopoguerra, per la sua aderenza a principi superiori validi di per sé. Ritornando a ritroso nel tempo, come si è avuto modo di anticipare in precedenza, le radici di questo referente del termine costituzione si può trovare nella summa dell'esistenza di una

---

[21] Tra gli altri, ZAGREBELSKY G., *Manuale di diritto costituzionale, I, Le fonti del diritto*, Utet, Torino, 1988, MORTATI C., L*a costituzione in senso materiale*, Giuffré, Milano, 1942, D'ANDREA A., GUIGLIA G., ONIDA V., *L'ordinamento costituzionale italiano*, Torino, Utet, 1990.

garanzia dei diritti e della separazione tra poteri dello Stato, tra i quali è ora considerato anche il sistema di giustizia costituzionale la cui funzione è, appunto, quella di valutare la conformità degli atti inferiori a quella norma fondamentale.

Alla luce di questa sommaria distinzione, la precedente affermazione in punto di costituzionalizzazione da parte di tutti gli Stati contemporanei risulta necessariamente riferita al senso materiale del termine costituzione. Qualsiasi organizzazione sociale, e ovviamente tra queste rientrano gli Stati e le autorità sovrane su territori contestati, è dotata di una costituzione in senso materiale, in quanto esiste, se non per iscritto, almeno una pratica concreta dell'esercizio del potere e della gestione dei rapporti tra i soggetti istituzionali, politici, sociali e individuali coinvolti. Discorso analogo si può anche condurre nel caso ci si riferisca al senso formale della costituzione: in questo senso, benché non sia assoluta, è comunque ampiamente maggioritaria la presenza di atti normativi fondamentali negli Stati contemporanei.

Diverso invece è l'esito di un confronto fra i testi costituzionali contemporanei alla luce dell'interpretazione sostanziale del termine costituzione, quindi nella prospettiva della garanzia dei principi dello Stato di diritto e dei diritti fondamentali della persona. In questo caso, il panorama comparatistico offre soluzioni molto diverse tra loro, in grandi linee classificabili secondo due ordini di distinzioni:

a) esistono costituzioni che garantiscono la divisione dei poteri e costituzioni che non la garantiscono. In punto di divisione dei poteri non è univoco il rapporto che potere legislativo, potere esecutivo, potere giudiziario e altri poteri di garanzia debbano avere tra di loro affinché di separazione effettiva si tratti. Le stesse costituzioni formali addotte a modello di giustizia e civiltà hanno elaborato, in tema di rapporti tra poteri, forme di Stato e di governo, modelli molto diversi tra loro, in

certi casi propendendo verso una supremazia del potere legislativo, come la Costituzione italiana o quella spagnola, in altri verso una supremazia del potere esecutivo, come nel caso inglese e ungherese, in altri ancora verso forme mediate in modo distinto con propensione verso la supremazia di uno o dell'altro, o ancora di tipo presidenziale, come quella americana, o semi-presidenziale, come nella Costituzione francese gaullista. Anche il rapporto nei confronti dell'autonomia e dell'indipendenza del potere giudiziario varia da paese a paese, spaziando dalla funzione anche normativa dei giudici fino ad una parziale dipendenza al potere esecutivo. Ciò che sicuramente funge da discrimine nella concezione contemporanea della divisione dei poteri è la presenza di un istituzione adibita al controllo della legittimità costituzionale degli atti e la sua non corrispondenza esclusiva con gli organi di derivazione politica, esecutivo e legislativo in particolare.

b) *esistono costituzioni che garantiscono i diritti umani fondamentali e costituzioni che non garantiscono i diritti umani fondamentali*. Sotto questo punto di vista la distinzione è più complessa e meno netta rispetto alla precedente. Pur considerando, ovviamente, a pieno titolo tra gli ordinamenti che proteggono i diritti umani fondamentali quelli che prevedono la tutela dei diritti in testi giuridici diversi rispetto alla Costituzione formale, è opposto e diffuso il caso di enunciazione di quegli stessi diritti e principi nella più totale assenza di strumenti giuridici concreti per il loro esercizio e la loro tutela[22].

[22] Valga richiamare quanto riferito supra, nota 19, in merito alla sussistenza di numerose critiche alla Carta dei Diritti Umani della Lega Araba, ovvero ancora quanto si dirà di seguito sulla Costituzione della Repubblica Socialista del Vietnam, e discorso analogo può essere condotto con riferimento a numerose carte costituzionali nazionali.

È intenzione soffermarsi e tenere in maggior rilievo la seconda di queste due distinzioni, individuando quindi in questa sede gli indici rilevanti al fine di valutare un ordinamento quale ispirato o meno alla dottrina dei diritti umani e a quell'ideale di cui parla la Dichiarazione universale dei diritti dell'uomo delle Nazioni Unite. Tra gli indici suscettibili di ingenerare giustificati dubbi quanto alla riconducibilità di un certo testo costituzionale alla citata dottrina, si possono in particolar modo evidenziare:

a) *l'assenza di procedure e criteri di limitazione dei diritti*. Come più volte ribadito, un diritto, e questo vale in particolar modo per i diritti di libertà, può essere pienamente garantito ove siano stabilite le ragioni e le procedure per la sua limitazione, ovvero, com'è agilmente percepibile in campo di diritti sociali, delle procedure di individuazione del corrispondente dovere, sia esso di astensione oppure di intervento. Il diritto alla libertà d'espressione può essere sancito in via generale ed astratta, ma è nelle formule quali quella contenuta nei commi dal secondo al sesto dell'art. 21 della Costituzione italiana, che stabilisce le procedure di sequestro per la stampa e il limite del buon costume[23], ovvero nel comma 2 dell'art. 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo[24], che stabilisce le tre condizioni,

---

[23] Discorso diverso e distinto, frutto proprio delle possibilità dischiuse dalle ITCs e dalla società dell'informazione, è quello della validità di una distinzione tra espressione e informazione.

[24] Il comma 2° recita "l'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, per la sicurezza nazionale, per l'integrità territoriale o per la pubblica sicurezza, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, per la protezione della reputazione

legalità, legittimità e proporzionalità, affinché tale diritto possa essere limitato, o ancora il già citato art. 19 della Dichiarazione Universale dei Diritti dell'Uomo. Tale approccio soddisfa la necessità di un'efficacia rinforzata, nel tempo e nel rapporto tra fonti, rispetto alle contingenti decisioni marcatamente politiche che potrebbero susseguirsi in modo altalenante. Sotto questo punto di vista può essere necessario tenere a mente che i confini tra diritti in conflitto fra loro, pur mancando nelle previsioni esplicite dei testi di natura costituzionale, potrebbero essere elaborati con sufficiente determinazione dalle giurisprudenze costituzionali nazionali o sovranazionali, intervenute in soccorso di legislatori recalcitranti o scarsamente interessati. Diversamente, l'assenza di tali formule dinnanzi a una dichiarazione di mero principio quale quella contenuta nell'art. 69 della Costituzione del Vietnam, che stabilisce che "ognuno è titolare della libertà di espressione e di stampa"[25], così come un rinvio alla legge in assenza di criteri di comparazione, potrebbero ben essere assunti a indici di elevata arbitrarietà in fase interpretativa, e quindi di facile negazione, del diritto stesso[26].

b) *l'assenza di procedure che permettano al cittadino di accedere*

---

o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario".

[25] Il testo della Costituzione della Repubblica Socialista del Vietnam del 1992 è disponibile in lignua inglese all'indirizzo web http://www.vietnamlaws.com/freelaws/Constitution92%28aa01%29.pdf/ (verificato il 12.05.2014).

[26] Si noti che proprio la citata Costituzione del Vietnam del 1992 all'art. 23, nello stabilire il diritto alla proprietà privata, indica anche le ragioni e le procedure basilari attraverso le quali tale diritto possa essere limitato o negato. La diffusione, nell'ambito dei diritti economici, di formule che esplicitino i possibili limiti è tale da rendere impensabile che l'assenza di ulteriori indicazioni quanto ai diritti di libertà sia frutto di una scelta casuale.

a una giustizia indipendente per la tutela dei propri diritti. In parallelo al ruolo svolto dai tribunali costituzionali quanto a competenze degli organi di uno Stato, l'assenza di tali organi, l'esclusione dalle loro competenze delle materie dei diritti, la corrispondenza tra gli organi di controllo costituzionale e gli organi politici dello Stato o, nel caso di una di queste situazioni, l'impossibilità di sollevare violazioni costituzionali dinnanzi al giudice ordinario o infine la dipendenza diretta di questo dagli organi politici sono forti indicatori di una probabile assenza, nel diritto vivente, di una concreta tutela di tali diritti.

c) *la presenza di preminenti principi etici, religiosi, politici, economici o sociali* non dettagliati e di ispirazione dei testi costituzionali. Un elemento che accomuna la pluralità di Stati denunciati quali ostili alla garanzia e protezione dei diritti umani fondamentali è la presenza, per ragioni eminentemente culturali e politiche, di principi superiori collettivi di matrice perlopiù religiosa o politica, talvolta ma non necessariamente esterni al testo costituzionale e soprattutto da questo non dettagliatamente declinati, ai quali in ultima istanza andrebbero ricondotte l'interpretazione e l'applicazione delle norme di legge ai casi concreti. L'ambiguità e la vaghezza degli ideali ispiratori di uno Stato, ideali che nella pluralità delle costituzioni, essendo carte solenni, sono proclamati nei preamboli, è indice della presenza di ragioni arbitrarie che possono portare a limitare o escludere i diritti collettivi e individuali, politici e di libertà. In particolare risaltano appunto i dettami religiosi negli ordinamenti che fanno esplicitamente riferimento a fonti religiose, testi sacri o autorità, quale criterio di interpretazione del contenuto del testo stesso, e le ideologie politiche ed economiche che, in quanto tali, derivano il loro contenuto dall'indirizzo politico del momento.

d) *la presenza di organi dello Stato, competenti nell'esercizio delle*

*funzioni proprie, la cui composizione non sia determinata dalla costituzione stessa o da un atto equiparabil*e. Questo indice, che si ricollega in realtà per la maggior parte al precedente, accade in quegli Stati ove la competenza sulla valutazione di una legge, ma ancor più sulla decisione della risoluzione di un caso concreto, spetti a organi religiosi o organizzazioni politiche del tutto esterne alla costituzione formale e dotate di proprie autonome e indipendenti regole organizzative e formative. Sia essa un consiglio, per l'appunto, religioso ovvero un partito unico dello Stato, la delega a tali elementi esterni dell'attività di bilanciamento è indice di elevate probabilità di violazione dei diritti umani fondamentali.

Il ricorso a tali indici per osservare i fenomeni costituzionali nei diversi paesi della comunità internazionale pone, ad avviso di chi scrive, una pesante ipoteca sull'approccio, più che diffuso, orientato a distinguere gli ordinamenti giuridici e politici sulla base della novecentesca divisione del mondo in due blocchi contrapposti, quello occidentale democratico-costituzionale e quello orientale autoritario e ostile allo Stato di diritti e ai diritti di libertà. Questo approccio infatti, pur avendo un proprio valore da un punto di vista storico e sociologico[27], può involontariamente generare un indebito e inopportuno senso di superiorità al momento dell'approccio agli ordinamenti giuridici distanti dai nostri. Indebito in primo luogo in ragione del fatto che, come si avrà modo di vedere, sebbene la divisione dei poteri sia più marcata e

[27] È fuori di dubbio infatti che l'origine di tali principi sia correttamente attribuita a paesi geograficamente "occidentali", così come l'affermazione che la profondità e l'articolazione di questi stessi principi siano in stadio più avanzato in questi stessi paesi. Allo stesso modo taluni paesi hanno avuto modo di denunciare apertamente la teoria dei diritti umani quale strumento d'impero appartenente all'ideologia occidentale.

assistita da organi di garanzia costituzionale, i diritti fondamentali subiscono anche nell'Occidente limitazioni e vincoli alla luce di principi ideologici trasposti negli ordinamenti giuridici attraverso pratiche poco trasparenti; inopportuno in quanto, e anche di questa statuizione di approfondirà più avanti, in numerosi casi è proprio dall'Occidente che vengono diffusi, a livello globale, modelli e tecnologie di limitazione dei diritti fondamentali dell'individuo.

Risulta a questo punto più proficuo, nell'ottica che è qui di interesse, tentare un raggruppamento degli ordinamenti giuridici non tanto alla luce di una classificazione per grado di aderenza ai principi dello Stato di diritto, attività pur meritevole e destinata a fornire esiti piuttosto sorprendenti, quanto invece alla luce dei preminenti interessi suscettibili di porsi quale valida base per un effettiva limitazione del diritto alla libertà di espressione, anche nel contesto digitale. Pur avendo infatti ciascuno Stato e ciascuna cultura giuridica un proprio retroterra culturale e sociale distintivi, vi sono tratti che accomunano Stati diversi, spesso in aree geografiche contigue, alla luce delle ragioni che giustificano o ispirano l'assenza di una normativa efficace di tutela dei diritti umani fondamentali, in particolar modo i principi dello Stato di diritto, i diritti politici e i diritti di libertà, tra i quali assume rilievo in questa sede il diritto alla libertà di espressione, così nel contesto materiale come in quello digitale.

In questa prospettiva è possibile individuare diritti e interessi che ricevono una tutela elevata a livello globale, riconosciuti quindi dalla totalità degli ordinamenti giuridici e raggruppamenti di diritti e interessi preminenti invece all'interno di specifiche culture giuridiche. Tra i primi vi sono indubbiamente tutti quei fenomeni riconducibili alla sicurezza nazionale, alla stabilità dell'ordine politico-costituzionale e sociale costituito: che si tratti della tutela dell'ordinamento democratico-

costituzionale protetto in Europa da espressioni apologetiche nei confronti di passati o presenti regimi autoritari ovvero di tutela dell'ordine politico-sociale proprio dei sistemi ispirati all'ideologia socialista, il concetto di tutela dell'ordine costituito è un criterio di limitazione dei diritti mirato all'autoconservazione del sistema diffuso nel mondo intero e caratterizzato da un elevato tasso di opacità delle procedure poste in essere a riguardo. Tra i secondi invece si possono individuare i principi di ispirazione religiosa che permeano una pluralità di ordinamenti giuridici di stampo teocratico: in questi paesi, che spaziano per l'appunto da Stati considerati appartenere al blocco occidentale così come a quello orientale a seconda del momento e tra i quali si può iscrivere buona parte dei paesi del Vicino e del Medio Oriente, la protezione dell'etica e della morale religiosa, frequentemente declinate nel concreto a partire da fonti eteronome rispetto agli ordinamenti giuridici statali, è principio cardine e superiore nei confronti del quale porre in relazione diritti individuali e collettivi.

3. Disciplina giuridica del diritto alla libertà di espressione

In questo contesto caratterizzato da un pluralismo giuridico che la dottrina giuridica e sociologica moderna aveva già ben identificato, la diffusione delle tecnologie dell'informazione e della comunicazione a livello globale ha comportato un contatto molto ravvicinato tra queste diverse culture giuridiche, tale da determinare la necessità di considerare l'esistenza dei diritti nel contesto digitale alla luce dei tratti comuni o difformi degli ordinamenti nazionali o regionali così come delle fondamenta dell'ordinamento giuridico internazionale, dell'economia transnazionale e dell'infrastruttura tecnologica vigente. La domanda da porsi è se in un contesto sociale e giuridico plurale e frazionato, in taluni

casi in ragione di distanze culturali profondamente radicate nelle popolazioni di riferimento, lo sviluppo e la presenza di un territorio virtuale comune possa incidere sullo sviluppo e sulla diffusione di diritti comuni alla collettività globale che in tale territorio si muove, e da quali fonti tali diritti possano essere fatti discendere.

Al fine di rilevare gli eventuali tratti comuni dei diritti digitali, si intende in questa sede ricercare le origini e le fondamenta dei diritti fondamentali tradizionali, la loro declinazione del contesto digitale e infine l'influenza del codice informatico e dell'autonomia privata sull'effettività delle norme giuridiche in materia.

3.1. Le fonti tradizionali del diritto alla libertà di espressione

Rinviando al primo paragrafo dedicato all'universalismo della teoria dei diritti umani per il breve inquadramento storico della questione e ai contributi dottrinali più rilevanti a riguardo[28], in questa sede ci si intende concentrare sulle fonti del diritto alla libertà di espressione nell'età contemporanea nelle democrazie costituzionali nazionali e in particolare prendendo a paradigma di riferimento lo sviluppo delle due Europe.

La libertà di espressione, come si è avuto modo di dire, è architrave del sistema dei diritti umani e degli ordinamenti dello Stato costituzionale di diritto contemporanei. Il diritto alla libertà di

[28] CHELI E., *La Costituzione italiana tra storia e politica*, Il Mulino, Bologna, 2012; PALADIN L., *Per una storia costituzionale della Repubblica Italiana*, Il Mulino, Bologna, 2004, OSTREICH G., a cura di G. Gozzi, *Storia dei diritti umani e delle libertà fondamentali*, Roma, Laterza, 2001.

espressione, formula che richiama non solo l'esistenza di uno spazio di libertà da ingerenze esterne dirette a precluderlo o annullarne la portata ma soprattutto la necessità di condotte positive delle autorità e degli attori sociali affinché venga garantito tale spazio di libertà, riveste tale ruolo centrale per un duplice ordine di ragioni.

In primo luogo il diritto alla libertà di espressione, come *diritto del tutto autonomo*, è orientato alla tutela dell'esistenza di spazi di relazione interpersonale suscettibili di essere il veicolo di manifestazioni del proprio pensiero[29], o di espressioni, la cui libertà da sorveglianza, controllo o limitazione è garanzia della piena esplicazione dello sviluppo personale, intellettuale, culturale e sociale della persona umana. In questo senso la libertà di espressione è autonomamente considerata un valore, a prescindere tanto dal contenuto dell'espressione quanto dal rapporto tra esercizio della libertà stessa e altre esternalità positive che potrebbero essere generate. La caratteristica della capacità di esprimersi attraverso una comunicazione articolata, particolarmente sviluppata nella persona umana, rileva di per sé in quanto intrinsecamente radicata nella fondamentale e umana necessità di rapporti sociali. In questo senso del contenuto o delle modalità dell'espressione il diritto potrebbe ben disinteressarsi, riservando il proprio intervento all'astensione da pratiche di limitazione preventiva dell'espressione e all'eventuale intervento, solo successivo, per la sanzione di espressioni che in concreto ledano un diritto o interesse altrui di pari grado. In relazione a questa prospettiva, richiamando il pensiero degli studiosi che per manifestazione del pensiero "intendono qualsiasi espressione di opinioni, convinzioni,

[29] In questo senso la formula utilizzata all'art. 21 della Costituzione italiana pone in risalto proprio il rapporto tra elaborazione mentale dell'individuo e manifestazione esteriore della stessa attraverso diversi mezzi di diffusione.

atteggiamenti, sentimenti, emozioni, esortazioni, narrazione e interpretazione di avvenimenti di qualsiasi natura", è stata proposta una sintesi nel concetto di "«rendere manifesti ad altri» tutto ciò che ha origine e/o conseguenza nella sfera psichica di un dato soggetto, e per volontà del soggetto stesso"[30]. La stessa Corte ebbe modo di ricondurre la libertà di espressione alla tutela dell'inviolabilità dei diritti fondamentale, affermando infatti che l'art. 21 "colloca la predetta libertà tra i valori primari, assistiti dalla clausola dell'inviolabilità (art. 2 della Costituzione), i quali, in ragione del loro contenuto, in linea generale si traducono direttamente e immediatamente in diritti soggettivi dell'individuo, di carattere assoluto"[31].

In secondo luogo, il diritto alla libertà di espressione rileva come elemento strutturalmente e concettualmente precedente, come *condicio sine qua non, rispetto alla globalità dei diritti* riconosciuti. Eccezion fatta per il diritto alla vita, il diritto all'integrità della propria persona e il diritto all'inviolabilità della propria libertà personale, la libertà di espressione è elemento necessario dell'esercizio di tutti i diritti di libertà previsti dalle catalogazioni nazionali e internazionali contemporanee. Non è possibile neanche immaginare, in assenza di uno spazio di libertà di espressione, l'esercizio concreto degli altri diritti di libertà, quali la libertà di associazione, la libertà religiosa, la libertà di di stampa. Allo stesso modo, non potrebbero avere un contenuto concreto le libertà sociali, quali insegnamento, ricerca, cultura, associazionismo sindacale,

---

[30] FOIS S., *Informazione e diritti costituzionali*, in *Rivista di diritto dell'informazione e dell'informatica*, 2000, pag. 250 .

[31] Corte Costituzionale italiana, sent. n. 112 del 1993, http://www.giurcost.org/decisioni/1993/0112s-93.html (verificato il 12.05.2014).

ovvero i diritti politici, ove non fosse riconosciuto uno spazio di libertà di espressione, comunicazione e diffusione di idee e pensiero. Tutte queste libertà, "non potrebbero sussistere o risulterebbero svuotate di effettivo contenuto"[32]. Da questo secondo punto di vista, la Corte Costituzionale italiana ebbe modo di definire la libertà di espressione come "pietra angolare dell'ordinamento democratico"[33], così come la Dichiarazione dei diritti dell'uomo e del cittadino del 1789 la definisce come "uno dei diritti più preziosi dell'uomo".

In questa prospettiva è di interesse individuare le più rilevanti fonti legislative che attualmente disciplinano la libertà di espressione, la cui origine, come ben appare evidente, è risalente a prima ancora che l'idea stessa di *Internet* come oggi lo conosciamo prendesse forma nell'immaginario scientifico. Le tradizionali fonti giuridiche che sanciscono e garantiscono il diritto alla libertà di manifestazione del pensiero, e ne stabiliscono al contempo i principi cardine in materia di sua limitazione, sono di natura internazionale, comunitaria, costituzionale e legislativa.

Tra le fonti di natura internazionale, possiamo operare una *summa divisio* tra le fonti cosiddette di *soft law*, di orientamento senza efficacia cogente diretta, e quelle invece dotate di efficacia vincolante e direttamente invocabili qualora vi siano supposte violazioni di questo spazio di libertà. Fonte di origine internazionale di orientamento è la citata Dichiarazione Universale dei Diritti dell'Uomo: per le ragione

---

[32] CORRIAS LUCENTE G., *Internet e manifestazione del pensiero*, in *Rivista di diritto dell'informazione e dell'informatica*, 2000, pag. 598

[33] Corte Costituzionale italiana, sent. n. 84 del 2 aprile 1969 in Giur. Cost, 1969, pag. 1175, http://www.giurcost.org/decisioni/1969/0084s-69.html (verificato il 12.05.2014).

storiche e politiche sopra espresse, alla Dichiarazione del 1948 non sono stati affiancati percorsi finalizzati al controllo dell'effettiva implementazione del proprio contenuto all'interno degli ordinamenti giuridici nazionali degli Stati firmatari o aderenti alla Dichiarazione stessa. Diversa invece è stata la scelta operata in sede di stipulazione di convenzioni internazionali, tra le quali spicca la Convenzione internazionale sui diritti civili e politici del 1966, che all'art. 19 sancisce e disciplina proprio la libertà di espressione[34]. Tale articolo sancisce al primo comma la libertà delle proprie opinioni, al secondo comma la libertà di "cercare, ricevere e diffondere informazioni e idee" senza rilevanza di contenuto, frontiere o mezzi, e al terzo comma fissa i principi da rispettare per la disciplina della restrizione della stessa libertà, ossia il principio di legalità e il principio di necessità alla luce del bilanciamento con diritti e interessi di altri e con la tutela "della sicurezza nazionale, dell'ordine pubblico, della sanità o della morale pubbliche". Con l'approvazione di tale Convenzione e l'istituzione del Comitato dei diritti umani è stata raggiunta la maggior estensione possibile in seno all'Organizzazione delle Nazioni Unite della tutela,

---

[34] L'art 19 recita: "*Ogni individuo ha diritto a non essere molestato per le proprie opinioni.*

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.

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 espressa mente 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".

ossia il riconoscimento del diritto alla libertà di espressione all'interno di un testo vincolante e alla luce di una procedura di segnalazione delle violazioni aperta non solo alle parti contraenti, gli Stati, ma anche ai soggetti che da parte di uno Stato contraente ritengano di aver subito violazione di uno dei diritti ivi indicati. Purtroppo, a fianco di tale procedura non è stato previsto, in seno alla Convenzione del 1966, alcuno strumento sanzionatorio, così che tale sistema si presenta comunque come insufficiente al perseguimento degli scopi prefissati e, benché formalmente vincolante, sia quindi sostanzialmente più vicino a un testo a carattere orientativo non dotato di forza cogente verso le parti contraenti.

Profondo contributo è inoltre arrivato dalla due Europe. La prima, ossia il Consiglio d'Europa, organizzazione di carattere internazionale, ha dato origine alla Convenzione Europea dei Diritti dell'Uomo del 1950 e portato all'istituzione della Corte Europea sui Diritti dell'Uomo incaricata di vigilare sulla sua attuazione. La seconda, composta in primo tempo dalle diverse Comunità Europee e giunta ora all'Unione Europea, con i propri trattati fondativi, le proprie competenze normativa, la Carta dei Diritti Fondamentali approvata a Nizza nel 2000 e integrata nel sistema dei trattati comunitari con il Trattato di Lisbona del 2007.

3.2. I limiti alla libertà di espressione nella Costituzione italiana

La libertà ha un contenuto effettivo quando assistita da una

disciplina dei propri confini[35], "d'altra parte, il concetto di limite è insito nel concetto di diritto, nel senso che, nell'ambito dell'ordinamento, le varie sfere giuridiche devono di necessità limitarsi reciprocamente, affinché queste possano coesistere nell'ordinata convivenza civile"[36]. Tale affermazione è stata già chiarita in precedenza, ha portata generale avendo riguardo per la totalità delle libertà individuali o collettive e così pure dei diritti e ha dunque valore portante con riferimento stretto alla libertà di espressione.

La stessa Costituzione prevede, al comma 6 dell'art. 21, il limite esplicito del buon costume. Al di là di tale previsione espressa, la libertà di manifestazione del pensiero nell'ordinamento costituzionale italiano trova limiti ulteriori, "purché questi siano posti dalla legge e trovino fondamento in precetti e principi costituzionali, espressamente enunciati o desumibili dalla Carta costituzionale"[37]. A seguito dell'ampia

---

[35] Questo principio è stato affermato, nel contesto italiano, in numerosissime sentenze della Corte Costituzionale già dalla prima che questo organo di garanzia suprema della Costituzione ha avuto modo di emettere. Tra le varie più datate, le sentenze nn. 1 del 1956, 121 del 1957, 38 del 1961, 48 del 1964, 49 del 1965, 129 del 1970, 138 del 1985; ordinanze nn. 97 del 1965 e 106 del 1974, tutte disponibili sul sito http://www.giurcost.it (verificato il 12.05.2014)..

[36] *I diritti fondamentali nella giurisprudenza della Corte Costituzionale*, Relazione predisposta in occasione dell'incontro della delegazione della Corte costituzionale con il Tribunale costituzionale della Repubblica di Polonia, Varsavia,30-31 marzo 2006, p. 33.

[37] C. Cost., sent. n. 100 del 1981, v. anche sent. 9 del 1965, ove la Corte afferma che "la libertà di manifestazione del pensiero é tra le libertà fondamentali proclamate e protette dalla nostra Costituzione, una di quelle anzi che meglio caratterizzano il regime vigente nello Stato, condizione com'è del modo di essere e dello sviluppo della vita del Paese in ogni suo aspetto culturale, politico, sociale. Ne consegue che limitazioni sostanziali di questa libertà non possono essere poste se non per legge (riserva assoluta di legge) e devono trovare fondamento in precetti e principi costituzionali, si rinvengano essi esplicitamente enunciati nella Carta costituzionale o si possano, invece,

giurisprudenza della Corte Costituzionale sui limiti della libertà di manifestazione del pensiero, può trovare limitazioni nei seguenti diritti o interessi:

1) il *buon costume*. Ai sensi del comma 6 dell'art. 21 "sono vietate le pubblicazioni a stampa, gli spettacoli e tutte le altre manifestazioni di pensiero contrarie al buon costume. La legge stabilisce provvedimenti adeguati a prevenire e reprimere le violazioni". Questo è l'unico limite esplicitamente previsto dalla Carta alla libertà di espressione, il cui contenuto concettuale è comunque andato evolvendosi e mutando nel tempo, posto il carattere indeterminato dello stesso e il ricorso al medesimo concetto da parte di branche dell'ordinamento giuridico diverse, quali il diritti civile[38] e il diritto penale[39]. La Corte

---

trarre da questa mediante la rigorosa applicazione delle regole dell'interpretazione giuridica".

[38] Ai sensi dell'art. 2035 c.c. "chi ha eseguito una prestazione per uno scopo che, anche da parte sua, costituisca offesa al buon costume non può ripetere quanto ha pagato". Tale buon costume consisterebbe "in norme di carattere non giuridico che si aggiungono alle norme imperative e all'ordine pubblico. Esse rappresentano lo strumento attraverso cui l'ordinamento statuale fa propri quei fenomeni di sensibilizzazione morale che si determinano nella realtà sociale ed economica, in aggiunga ai principi morali espressi dal sistema", DIENER M.C., *Il contratto in generale*, Giuffrè, Milano, 2011, p. 351. La Cassazione ha avuto modo di affermare che "la nozione dei negozi contratti al buon costume non può essere limitata ai negozi contrari alle regole del pudore sessuale e della decenza, ma si estende fino a comprendere i negozi contrari a quei principi ed esigenze etiche della coscienza morale collettiva che costituiscono la morale sociale, in quanto ad essi uniforma il proprio comportamento la generalità delle persone corrette, di buona fede e sani principi, in un determinato momento ed in un dato ambiente" Cass, civ, S.U., n. 4414 del 1981.

[39] Il Codice Penale del 1930 dedica un titolo ai delitti contro la moralità pubblica e il buon costume. Dei delitti e degli articoli lì previsti pochi sono sopravvissuti alla riforma del 1996, ossia gli atti osceni (art. 527 c.p.) e le pubblicazioni e gli spettacoli osceni (art. 528 c.p.). Tratto comune del concetto di buon costume in ambito penale, caratterizzato per la sua natura da

Costituzionale italiana ha avuto modo di esprimersi in diverse occasioni sulla portata del concetto di buon costume sulla base di una decisione cardine, la sent. n. 9 del 1965, ove la questione ruota "sul punto se il "buon costume" che compare nell'art. 21 della Costituzione debba essere ricondotto a quello che si può costruire sulla base delle norme del diritto penale, limitatamente a quelle tra esse che tutelano il pudore, l'onore e la libertà sessuale, ovvero, più estensivamente, sulla base anche di quelle che tutelano la pubblica decenza e il comune sentimento morale, o se, invece, si debba costruire di esso una nozione costituzionale più ampia o comunque diversa da quella penalistica". La Corte sceglie di fornire una definizione in negativo secondo cui "il buon costume non può essere fatto coincidere [...] con la morale o con la coscienza etica, concetti che non tollerano determinazioni quantitative del genere di quelle espresse dal termine "morale media" di un popolo, "etica comune" di un gruppo e altre analoghe", e una prima formulazione definitoria in positivo, alla luce della quale "il buon costume risulta da un insieme di precetti che impongono un determinato comportamento nella vita sociale di relazione, l'inosservanza dei quali comporta in particolare la violazione del pudore sessuale, sia fuori sia soprattutto nell'ambito della famiglia, della dignità personale che con esso si congiunge, e del sentimento morale dei giovani, ed apre la via al contrario del buon costume, al mal costume e, come è stato anche detto, può comportare la perversione dei costumi, il prevalere, cioè, di regole e di comportamenti contrari ed opposti." [40]. In seguito a pronunce altalenanti[41] sulla compatibilità di

interpretazioni restrittive piuttosto che estensive, è la copertura del concetto di pudore sessuale.

[40] Corte Cost., sentenza n. 9, del 19 febbraio 1965, in Giur. cost. 1965, p. 61, http://www.giurcost.org/decisioni/1965/0009s-65.html;

norme giuridiche alla luce di un concetto costituzionale del buon costume, la Corte approda a due rilevanti sentenze a riguardo alla luce delle quali il buon costume "non è diretto ad esprimere semplicemente un valore di libertà individuale o, più precisamente, non è soltanto rivolto a connotare un'esigenza di mera convivenza fra le libertà di più individui, ma è, piuttosto, diretto a significare un valore riferibile alla collettività in generale, nel senso che denota le condizioni essenziali che, in relazione ai contenuti morali e alle modalità di espressione del costume sessuale in un determinato momento storico, siano indispensabili per assicurare, sotto il profilo considerato, una convivenza sociale conforme ai principi costituzionali inviolabili della tutela della dignità umana e del rispetto reciproco tra le persone"[42]. Il buon costume in senso costituzionale viene quindi ricondotto a "ciò che è comune alle diverse morali del nostro tempo"[43]. Tale incontro tra le diverse morali

[41] Se la citata sent. n. 9 del 1965 aveva infatti fatto salva la legittimità costituzionale dell'art. 553 c.p. (Incitamento alle pratiche contro la procreazione), la stessa Corte con la sentenza n. 49 del 16 marzo 1971, in Giur. cost., 1971 p. 525, e http://www.giurcost.org/decisioni/1971/0049s-71.html, la Corte dichiara l'incostituzionalità del citato articolo entrando nel merito di questa mutata coscienza comune in relazione all'incitamento pubblico alle pratiche anticoncezionali, affermando che "D'altra parte, il problema della limitazione delle nascite ha assunto, nel momento storico attuale, una importanza e un rilievo sociale tale, ed investe un raggio di interesse così ampio, da non potersi ritenere che, secondo la coscienza comune e tenuto anche conto del progressivo allargarsi della educazione sanitaria, sia oggi da ravvisare un'offesa al buon costume nella pubblica trattazione dei vari aspetti di quel problema, nella diffusione delle conoscenze relative, nella propaganda svolta a favore delle pratiche anticoncettive".

[42] Con la sentenza n. 368 del 27 luglio 1992, in Giur. cost., 1992, p. 2935, e http://www.giurcost.org/decisioni/1992/0368s-92.html

[43] Corte Cost. sentenza n. 293, del 17 luglio 2000, in Riv. pen., 2000, pag. 881, e http://www.giurcost.org/decisioni/2000/0293s-00.html.

altro non sarebbe che "il rispetto della dignità umana"[44] e, dunque, quanto protetto dall'art. 2 della Costituzione italiana.

2) *la tutela dei minori*. La libertà di manifestazione del pensiero ha visto i propri limiti determinati con maggior dettaglio anche alla luce dell'interesse supremo alla "tutela del libero sviluppo psichico e morale dei minori"[45], ritenuto dalla giurisprudenza costituzionale italiana interesse preminente della Costituzione, scaturente dal combinato disposto degli artt. 20, 30[46] e 31[47]. Dall'osservazione degli ultimi due articoli risulta un quadro articolato in due modalità di intervento

---

[44] DI LELLO C., *Internet e Costituzione: garanzia del mezzo e suoi limiti* in *Diritto dell'informazione e dell'informatica*, 2007, p. 909.

[45] Corte Cost., sentenza n. 112 del 26 marzo 1993, in Giur. cost., 1993, p. 939 e http://www.giurcost.org/decisioni/1993/0112s-93.html. In quella sede la Suprema Corte, chiamata a decidere in materia di disciplina del sistema radiotelevisivo, ebbe modo di affermare "l'imperativo costituzionale" alla luce del quale il diritto all'informazione garantito dall'art. 21 debba essere "qualificato e caratterizzato: a) dal pluralismo delle fonti cui attingere conoscenze e notizie - che comporta, fra l'altro, il vincolo al legislatore di impedire la formazione di posizioni dominanti e di favorire l'accesso nel sistema radiotelevisivo del massimo numero possibile di voci diverse - in modo tale che il cittadino possa essere messo in condizione di compiere le sue valutazioni avendo presenti punti di vista differenti e orientamenti culturali contrastanti; b) dall'obiettività e dall'imparzialità dei dati forniti; c) dalla completezza, dalla correttezza e dalla continuità dell'attività di informazione erogata; d) dal rispetto della dignità umana, dell'ordine pubblico, del buon costume e del libero sviluppo psichico e morale dei minori".

[46] L'art. 30 prevede al primo comma "è dovere e diritto dei genitori mantenere, istruire ed educare i figli, anche se nati fuori del matrimonio" e al secondo comma che "nei casi di incapacità dei genitori, la legge provvede a che siano assolti i loro compiti".

[47] Ai sensi del primo comma dell'art. 31 "la Repubblica agevola con misure economiche e altre provvidenze la formazione della famiglia e l'adempimento dei compiti relativi, con particolare riguardo alle famiglie numerose", e a sensi del secondo, "protegge la maternità, l'infanzia e la gioventù, favorendo gli istituti necessari a tale scopo".

pubblico: se infatti il primo sancisce la funzione primaria dei genitori nell'assumere il compito di "istruire ed educare" i figli, accompagnarli cioè gradatamente in quel libero sviluppo psichico e morale proprio dell'età evolutiva, il ruolo pubblico è solamente secondario ed eventuale, da attivarsi in caso di incapacità genitoriale; il secondo articolo invece afferma il ruolo primario e diretto dello Stato nel porre l'interesse dalla tutela dei minori quale valore costituzionale a cui ispirare l'opera legislativa, al punto da poter motivare interventi limitativi di altri diritti, quale la libertà di manifestazione del pensiero in particolare nella forma specifica della libertà di informazione, o valori preminenti del sistema giuridico complessivamente inteso. Quest'ultima funzione è primaria e discende dall'art. 31 e dall'art. 2 della Costituzione stessa[48].

3) *la dignità personale*. Un altro limite al diritto alla libera manifestazione del pensiero che discende direttamente dalla Costituzione è rappresentato dai diritti all'onore, alla reputazione e alla riservatezza, che si ritrovano quali beni giuridici tutelati attraverso i tipici reati di ingiuria e in particolare il reato di diffamazione. Le radici costituzionali di questi diritti, da considerarsi veri e propri limiti operanti *tout court* nei confronti della libertà di manifestazione del pensiero, tali da giustificare l'esistenza di norme penali a loro tutela, affondano nell'art. 2, ossia nel riconoscimento dei diritti inviolabili dell'uomo, e

[48] A titolo d'esempio, la Corte Costituzionale stabilisce, intervenendo sulla legittimità costituzionale delle deroghe alla pubblicità dei dibattimenti in sede penale in caso di imputati di minore età, che "la deroga alla pubblicità del dibattimento costituisce un mezzo per il conseguimento di un'alta finalità di tutela dei minori", finalità che discende dall'"art. 31, secondo comma, della Costituzione, che prevede la tutela dei minori, intesa in correlazione con il principio fondamentale dell'art. 2 della Costituzione" con la sent. n. 16 del 10 febbraio 1981, in Giur. cost., 1981 p. 83 e http://www.giurcost.org/decisioni/1981/0016s-81.html

nell'art.3, la pari dignità di ogni persona senza distinzione di condizioni personali e sociali. A riguardo di questi diritti, già nel 1974 la Corte Costituzionale stabilì che tra gli interessi la cui tutela esige un bilanciamento del diritto sancito dall'art. 21 rientra certamente il concetto di "onore (comprensivo del decoro e della reputazione)"[49], che discende dall'art. 2 della Costituzione. Osservando la giurisprudenza di merito e di legittimità italiane i casi relativi al diritto di libera manifestazione del pensiero, e in particolare nella forma del diritto di informazione e del diritto di cronaca, in rapporto con la tutela della dignità personale in questo senso intesa rappresentano la parte numericamente più consistente, sia in relazione a conflitti relativi alla parola, alla carta stampata o alla radiotelevisione, sia in relazione a conflitti relativi alla disciplina normativa o alla soluzione di casi concreti di quanto possa essere posto in essere attraverso *Internet*. Una particolarità di questo limite è quello della necessità che il diritto all'integrità dell'onore, quando confligga con il diritto di critica espressione dell'art.21 della Costituzione, impone, secondo le parole di autorevole dottrina, "una valutazione della manifestazione del pensiero in rapporto alla condotta della persona della cui onorabilità si tratta"[50], che ben può essere criterio orientativo per definire la legittimità o meno di un'espressione che, in assenza della condotta stessa o in presenza di condotta diversa, avrebbe potuto assumere rilevanza opposta. Senza entrare in un dettaglio eccessivo che non rileverebbe ai fini che qui ci si propone, resti chiaro che la tutela della dignità personale nella forma di tutela dell'onore e della reputazione può essere posto a fondamento di

---

[49] Corte Cost. sent. n. 86 del 27 marzo 1974, in Giur. cost., 1974, pag. 680 e http://www.giurcost.org/decisioni/1974/0086s-74.html

[50] FOIS, *cit.* , 1957.

limitazioni all'esercizio del diritto alla libertà di espressione.

4) *la proprietà privata e la proprietà intellettuale*. La disciplina della titolarità, dell'uso, del godimento e dei limiti della proprietà privata incide sull'esercizio del diritto alla libertà di espressione in due campi: da una parte la proprietà privata nella forma della proprietà intellettuale è uno degli interessi più fecondi, soprattutto in ambito internazionale, di limitazioni alla libertà di espressione attraverso *Internet*; dall'altra, ed è tema già anticipato nel precedente capitolo, la proprietà privata tradizionalmente intesa come diritto di disporre liberamente delle cose delle quali si è proprietario, sia esso un bene destinato al proprio esclusivo godimento oppure uno spazio di titolarità si privata ma di uso aperto al pubblico come può essere una piazza o un sito web, può comportare arbitrarie limitazioni ai diritti di libertà delle altre parti. La proprietà privata era stata già definita "diritto sacro e inviolabile" con la Dichiarazione dei diritti dell'uomo e del cittadino del 1789, così come anche poco più di cento anni dopo Papa Leone XIII, con l'enciclica *Rerum Novarum* del 1891[51], affermò che la "proprietà privata deve essere ritenuta sacra e inviolabile". Proprio tra le parole dell'allora Pontefice della Chiesa Cattolica è possibile evidenziare la contraddizione dell'inserimento del diritto alla proprietà privata nel catalogo dei diritti fondamentali spettanti a tutti gli individui, ove continua affermando che "il diritto civile, quindi, dovrebbe favorire la proprietà e nella sua politica dovrebbe indurre più persone possibile a divenire proprietari". Il riferimento a "più persone possibile" manifesta la presa d'atto dell'impossibilità materiale di caratterizzare il diritto alla

[51] Il testo complete della Lettera Enciclica è consultabile sul sito http://www.vatican.va/holy_father/leo_xiii/encyclicals/documents/hf_l-xiii_enc_15051891_rerum-novarum_it.html (verificato il 12.05.2014).

proprietà privata come diritto fondamentale umano delle persone, proprio in quanto manca del tutto, per la sua stessa natura, una possibile applicazione dell'aspirazione universalistica dei diritti umani. Il diritto alla proprietà privata è stato ed è tuttora oggetto, quanto alla sua natura, di contrastanti osservazioni politiche, economiche, sociali e giuridiche, che spaziano dalla supremazia assoluta di tale diritto[52], alla sua totale negazione, quest'ultima ormai residuo di passati regimi, la cui piena portata è assente persino dalle ultime Repubbliche Socialiste o Popolari ancora presenti.

4. Le fonti alternative dei diritti digitali

Come si è anticipato, la normazione dei rapporti sociali oggi, come nel passato, non avviene solo per mano del diritto. Se nel passato infatti vi era un forte influsso, oltre che delle norme di tipo giuridico diversamente declinate, delle norme sociali, economiche e soprattutto morali, di origine prevalentemente religiosa, oggi, ridotta l'influenza di queste ultime, rilevano soprattutto le norme di origine informatica e quelle di origine economica.

---

[52] Il legislatore italiano, nel 2005, ha persino, in questa prospettiva, introdotto una modifica al codice penale nella disciplina della legittima difesa quando ciò avvenga nel contesto della propria dimora o del proprio domicilio professionale, inserendo una presunzione di proporzionalità della reazione che cagioni la morte dell'aggressore quand'anche tale aggressione fosse diretta a beni esclusivamente patrimoniali. Tale impostazione è stata ribaltata dalla giurisprudenza di merito e legittimità, che ora richiede comunque, in ossequio ai corretti principi di bilanciamento degli interessi, un pericolo comunque anche diretto nei confronti di beni giuridici personali.

Le prime influiscono sulla nostra possibilità di compiere determinate azioni nel contesto digitale, prevedendone la pratica fattibilità o meno. Le seconde determinano i limiti delle nostre azioni sia indirettamente, ossia per il tramite del supporto del diritto e/o del supporto del codice informatico, sia direttamente, qualora una certa azione sia vincolata dalla disponibilità di risorse economiche per poterla porre in essere.

Di seguito si svolgeranno alcune riflessioni su questi due aspetti, partendo dal ruolo regolatore del codice informatico e arrivando all'accresciuta influenza dei principi economici sull'esercizio dei diritti: in particolare si trarranno ad esempi l'autonomia privata nel contesto dei *social network*, nel contesto dell'affermazione dei diritti di proprietà intellettuale e il caso, emblematico, dell'affermazione, operata dal *Conseil Constitutionnel* francese e risalente al 2009, del diritto all'accesso a *Internet* quale diritto fondamentale riconducibile al diritto alla libertà di espressione e dunque non suscettibile di compressione per via amministrativa di fronte alle violazioni della normativa in materia di diritto d'autore.

4.1. Il codice informatico

Il tema in questa sede non è dunque quello della considerazione degli strumenti di comunicazione telematica quali agevolatori dell'implementazione delle norme giuridiche, bensì, per utilizzare le parole di Lessig "il problema qui è come l'architettura della rete – o il suo codice – diventi essa stessa regolatrice". In questa prospettiva la norma non trova la propria forza cogente, o comunque la forza

dissuasiva verso il proprio rispetto, nella minaccia sanzionatoria prevista dalla legge, bensì dalle leggi della fisica: "Una porta chiusa non è un comando "non entrare" sostenuto dalla minaccia di una punizione da parte dello Stato. Una porta chiusa è un costrizione fisica sulla libertà di qualcuno di accedere ad un certo spazio" [53].

Questo aspetto si nota nelle limitazioni applicabili a livello di *Internet service providers*, siano essi *access service providers*[54], fornitori di servizi di *social networking*[55], o di *massively multiple online games* (MMOG), dei quali oltre il 97% è rappresentato dai *massively multiple online role playing games* (MMORPG)[56] .

In tutti questi contesti – ciberspazi – alcune norme sono poste da regole di tipo sociale, quale la *nettiquette*, e da scelte della stessa comunità, collettivamente o individualmente, e rileva in questo senso in particolare la scelta di conservare o meno un certo grado di anonimato, altre invece sono costruite nella struttura informatica stessa. Queste

---

[53] LESSIG L., cit., 2006, p. 81, "*The issue here is how the architecture of the Net—or its "code"—itself becomes a regulator", "A locked door is not a command "do not enter" backed up with the threat of punishment by the state. A locked door is a physical constraint on the liberty of someone to enter some space*".

[54] Quali i ventisette operatori italiani in grado di bloccare fisicamente la risoluzione del DNS nei confronti di una certa lista di siti.

[55] Tra questi spicca senz'ombra di dubbio, per diffusione ed estensività dell'utilizzo, *Facebook* che abilita o disabilita determinate funzioni, ricerca in automatico e sopprime certi contenuti o specifiche parole.

[56] All'interno degli MMOG e in particolare degli MMORPG l'infrastruttura informatica è persino rappresentata con una ricostruzione ad alta definizione grafica di un mondo virtuale dotato di proprie leggi della fisica, benché adattate all'ambientazione proposta – reale, futuristica, medievale, *fantasy* – caratterizzata da cura ed elevatissimo realismo.

ultime, e la tematica è dunque strettamente correlata al punto successivo, ossia al ruolo dell'autonomia privata, sono determinate, nello strato più profondo, dai protocolli di comunicazione della rete *Internet*, attraverso i quali circolano e vivono queste comunità, e, nello strato dell'applicazione utilizzata, da proprietari sovrani di quello spazio[57].

Il *software* e l'*hardware* determinano l'essenza del ciberspazio, determinando come un certo soggetto possa agire: dal momento della connessione alla rete *Internet*, che già avviene solo e attraverso un *access service provider*, sia esso privato, pubblico, fisso o mobile, aziendale, tramite *cyber café*, e la comunicazione di una password; i servizi di ricerca tramite *web* ricorrono a format predeterminati che prevedono necessariamente *cookies* per la funzionalità del servizio, e con frequenza ulteriori relativi alla profilazione delle preferenze; l'accesso a servizi di *chat*, *forum*, *social network* o commercio elettronico richiedono, frequentemente, fasi di registrazione e autenticazione, e lo stesso accade per i servizi di *email*. In conclusione, il ciberspazio "limita alcuni comportamenti, rendendo possibile o impossibile l'alternativa. un altro comportamento o impossibile. Il codice incorpora determinati valori o li rende impossibili. In questo senso, esso stesso è regolamentazione, così come l'architettura dei codici dello spazio reale sono regole"[58].

---

[57] LESSIG L., cit., 2006, p. 114, "*In cyberspace in particular, but across the Internet in general, code embeds values. It enables, or not, certain control .And as has been the focus of this part, it is also a tool of control—not of government control, at least in the casesI've surveyed— but instead control to the end of whatever sovereign does the coding*".

[58] LESSIG L., *ibidem*, p. 125, "*constrain some behavior by making other behavior possible or impossibile. The code embeds certain vbalues or makes*

Il ciberspazio così influenzabile dalle scelte di natura tecnica operate dai soggetti privati diventa dunque terreno di conflitto tra competenze tecnologiche: come si vedrà meglio successivamente[59], il codice delle applicazioni di *Internet* e la sottostante architettura sono il luogo e il mezzo di rivendicazione di competenze di sorveglianza e controllo, di natura securitaria da parte di Stati e istituzioni e di natura economica e attitudinale da parte di imprese commerciali, e di spazi di autonomia attraverso la programmazione e l'utilizzo di *software* e tecniche avanzate per aggirare il codice e l'architettura stessa, così facendo aggirando filtri, controlli e sorveglianza.

4.2. L'autonomia pivata

Le problematiche sollevate dalla tutela della proprietà privata intesa come fonte di regolamentazioni dell'attività connessa all'utilizzo dello strumento di *Internet* occupano un ampio spazio riguardo al diritto alla libera manifestazione del pensiero ed i suoi limiti. Se da un lato infatti la disciplina della proprietà privata e degli spazi di libertà di iniziativa economica privata può incidere sull'esercizio del diritto sancito dall'art. 21 della Costituzione, in particolare avuto riguardo ai nuovi strumenti di comunicazione di massa, *blog* e *social network*[60] in

---

certain values impossible. In this sense, it too is regulation, just as the architecture of real-space codes are regulation".

[59] V. CAP III, *Sorveglianza globale e resistenza digitale*.

[60] Una rete sociale (*social network* in inglese) consiste in un gruppo di persone connesse tra loro da diversi legami sociali. Su *Internet* il fenomeno delle reti sociali ha assunto dal 2003 in avanti una diffusione tale da divenire vero e

testa, con la reviviscenza delle *chat* anche grazie all'*Internet* mobile, e questa incidenza rappresenta il punto più rilevante sotto il punto di vista della presente trattazione, dall'altro lato la disciplina della proprietà privata è stata causa dei primi interventi legislativi e dei più ampi, quantitativamente parlando, interventi giurisprudenziali ai fini di regolamentazione dello spazio della rete, a tutela in particolare della proprietà intellettuale di opere culturali, siano esse letterarie, musicali o cinematografiche.

I due aspetti, meritevoli per la loro portata di essere trattati distintamente, affondano però le proprie radici comuni all'interno di un lontano dibattito che ha investito il mondo del diritto ben prima dello sviluppo tecnologico ed è sostanzialmente riconducibile alla "posizione" che la proprietà privata occupa al momento di effettuare un bilanciamento tra diritti, libertà e interessi in conflitto tra loro. Dibattito che, secondo l'ideologia politica o economica dominante in un determinato contesto storico e regionale, ha sospinto il diritto verso una tutela assoluta della proprietà privata a discapito di qualsiasi interesse ulteriore piuttosto che verso la considerazione che il diritto di proprietà nulla è di più di una posizione di diritto soggettivo ben lontana dal qualificarsi come diritto fondamentale dell'individuo, in condizioni quindi di soccombere al conflitto di fronte ad altri diritti invece rientranti nel novero – certo anche questo di chiara impronta ideologica – dei diritti fondamentali e inviolabili della persona umana.

Questo lungo dibattito può essere esemplificato da un caso che segnò un punto di rottura per la dottrina giuridica che vedeva la proprietà

---

proprio fenomeno sociale in grado di incidere sulle scelte politiche ed economiche di governi ed imprese, nazionali e transnazionali. In particolare, oggi Facebook e Twitter rappresentano i *social network services* più rilevanti per numero di iscritti e di accessi giornalieri.

come diritto assoluto, per quella filosofia culturale molto in auge anche ai giorni nostri del "è mio e ne faccio ciò che voglio" insuscettibile di subire compressioni dovute all'interesse pubblico: il caso dei coniugi Causby. I coniugi in questione, come ci racconta LESSIG nell'introduzione a Cultura Libera[61], presentarono nel 1945 denuncia per violazione della loro proprietà contro il Governo degli Stati Uniti, i cui aerei militari, volando a bassa quota, causavano la perdita di numerosi polli i quali, sembra per paura del rumore, si schiantavano contro le pareti del granaio, morendo. La denuncia si fondava sulla base della preesistente dottrina secondo cui i diritti di proprietà si estendono dal suolo verso l'alto, all'infinito. La Corte Suprema esaminò il caso e cancellò con poche parole questa dottrina. "Esiste un'antica dottrina" afferma il giudice Douglas, "secondo cui nel *common law* la proprietà si estende dal suolo fino alla periferia dell'universo – *cujus est solum ejus est usque and coelum*. Ma quella dottrina non ha spazio nel mondo moderno. L'aria è un'autostrada pubblica […]. Il senso comune si ribellerebbe all'idea" [62].

La nostra Costituzione raccoglie in sé il risultato della mediazione tra le estreme posizioni ideologiche che si combattevano a conclusione dell'ultimo conflitto mondiale, essendo in tutta la sua struttura punto di incontro tra le ideologie liberali, cattoliche e social-comuniste rappresentate nell'Assemblea Costituente. In particolare è proprio

---

[61] LESSIG L., *Free Culture*, ed. Penguin Press, New York, 2004, http://www.free-culture.cc/freeculture.pdf (verificato il 12.05.2014), in italiano *Cultura Libera*, Apogeo, Milano, 2005, http://www.copyleft-italia.it/pubblicazioni/Lessig-CulturaLibera.pdf (verificato il 12.05.2014).

[62] U.S. Supreme Court, *United States v. Causby*, 328 U.S. 256 (1946) No. 630, Argued May 1, 1946, Decided May 27, 1946, http://supreme.justia.com/us/328/256/case.html (verificato il 12.05.2014).

l'articolo sul riconoscimento della proprietà privata a rappresentare la mediazione al tempo ideologica e giuridica di queste ideologie: l'art. 42 della Costituzione, riconosciuto al primo comma che "la proprietà è pubblica o privata" e che "i beni economici appartengono allo Stato, ad enti o a privati", al secondo comma ne delimita i confini, demandando alla legge – al potere pubblico quindi – il compito di determinarne "i modi di acquisto, di godimento e i limiti allo scopo di assicurarne la *funzione sociale* e di renderla accessibile a tutti"[63].

In questo senso, fu chiara sin dai primi anni della sua attività la Corte Costituzionale, che nel 1968 affermò che "secondo i concetti, sempre più progredienti, di solidarietà sociale, resta escluso che il diritto di proprietà possa venire inteso come dominio assoluto ed illimitato sui beni propri, dovendosi invece ritenerlo caratterizzato dall'attitudine di essere sottoposto nel suo contenuto, ad un regime che la Costituzione lascia al legislatore di determinare. Nel determinare tale regime, il legislatore può persino escludere la proprietà privata di certe categorie di beni, come pure può imporre, sempre per categorie di beni, talune limitazioni in via generale, ovvero autorizzare imposizioni a titolo particolare, con diversa gradazione e più o meno accentuata restrizione

[63] Senza dimenticare l'art. 41 che, nel riconoscere la libertà di iniziativa economica privata, ne vieta lo svolgimento se "in contrasto con l'utilità sociale o in modo da arrecare danno alla sicurezza, alla libertà e alla dignità umana", arrivando persino a demandare alla legge il compito, più che mai disatteso dal legislatore, di determinare "i programmi e i controlli opportuni perché l'attività economica pubblica e privata possa essere indirizzata e coordinata a fini sociali"

delle facoltà di godimento e di disposizione."[64]

Queste ripercorse problematiche si possono ritrovare in un dibattito ormai impellente, in sede europea: il rapporto tra supremazia dell'interesse pubblico o dell'interesse privato, con rilievo e rilevanza anche sul piano della cogenza delle relative norme, investe il dibattito sull'adozione del Transatlantic Trade and Investment Partnership[65]. Questo trattato, definito "un attacco frontale alla democrazia"[66], prevede una riaffermazione, attraverso diversi strumenti giuridici reintegrativi, compensativi e punitivi, della supremazia dei diritti privati dinnanzi ai diritti collettivi, oltre ai principi stessi della sovranità statale. In particolare, i punti rilevanti del Trattato contestato, ancora in fase di dibattito, sarebbero in particolare:

- una maggior deregolamentazione dei procedimenti produttivi, commerciali, di confezionamento e composizione dei prodotti;
- l'istituzione di un modello di giustizia arbitrale internazionale, indicato come investor-state dispute

---

[64] Corte Cost., sentenza n. 55 del 29 maggio 1968, in *Giur. cost.*, 1968, p. 838, e http://www.giurcost.org/decisioni/1968/0055s-68.html (verificato il 12.05.2014).

[65] La pagina dedicata dalla Commissione Europea sul tema, http://ec.europa.eu/trade/policy/in-focus/ttip/index_it.htm (verificato il 12.05.2014), una breve introduzione sulla pagina dedicata al trattato disponibile sul sito di Wikipedia, http://it.wikipedia.org/wiki/Trattato_transatlantico_sul_commercio_e_gli_investimenti (verificato il 12.05.2014).

[66] Tratto dall'articolo di Ken Clarke, pubblicato sul quotidiano *The Guardian*, l'11 novembre 2013, http://www.theguardian.com/commentisfree/2013/nov/04/us-trade-deal-full-frontal-assault-on-democracy (verificato il 12.05.2014).

settlement, a cui delegare, al di fuori della sovranità nazionale o comunitaria, le decisioni in merito a conflitti;

- la garanzia della tutela, in quella sede, del ritorno economico degli investimenti privati e della protezione dalle perdite sofferte dalle imprese dovute a riforme legislative – a titolo d'esempio, in materia di sicurezza del lavoro – che diminuiscano la redditività degli stessi.

4.2.1. La proprietà privata e i *social network*

La problematica del valore della proprietà privata in relazione ai *social network* risiede nel bilanciamento, in questo caso attuato da parte dei privati stessi, tra i propri diritti, quelli rappresentati dal famoso logo © "*all rights reserved*", e i diritti costituzionali propri di ogni cittadino. Semplicemente, la domanda che si è venuta a porre è se il proprietario di un bene o nel nostro caso di un servizio che viene messo a disposizione della generalità degli utenti della rete possa esercitare liberamente un potere censorio sulla forma ed in particolare sui contenuti dei messaggi veicolati attraverso quello stesso servizio, in virtù appunto di un regolamento d'uso che il proprietario sottopone, secondo *policies* contrattuali a mo' di condizioni generali di contratto, all'atto dell'iscrizione da parte degli utenti.

La tematica, sviluppatasi in particolare attorno all'utilizzo dei *forum*, si è originariamente risolta nel rinvio a quei medesimi regolamenti accettati dall'utente all'atto dell'iscrizione. La diffusione poi dei *blog* ha stemperato, apparentemente, la questione secondo il ragionamento per cui ciascuno ha la possibilità effettiva di crearsi un

proprio spazio in cui essere libero di esercitare il proprio diritto alla libera manifestazione del pensiero senza aver bisogno di sottoporsi a regole che altri, all'interno dei propri spazi, possono darsi in piena autonomia.

Questa apparente soluzione non tiene però in considerazione la realtà strutturale di *Internet*, composta, come si diceva all'inizio di questa trattazione, da componenti meramente materiali, quali cavi, elaboratori elettronici, *server* in particolare: queste componenti non possono che sfuggire al dominio proprietario della cittadinanza, e, pur rientrando nella tipica definizione di bene pubblico, spesso non solo sono dati in concessione a privati, ma hanno attraversato direttamente i processi di privatizzazione degli anni '80 e '90. A questa considerazione sulla struttura, si possono affiancare le problematiche sollevate dalle posizioni proprietarie nei confronti dei *software* utilizzati al fine di svolgere le proprie comunicazioni, le cui condizioni d'utilizzo possono ben superare i vincoli giuridici concessi da quel "bilanciamento degli interessi" cui facevamo prima riferimento[67].

A queste considerazioni si aggiunge infine la semplice considerazione giuridica effettuata in precedenza sull'inviolabilità della proprietà privata: questa inviolabilità, nel sistema giuridico ad oggi vigente, non esiste, e i diritti proprietari del singolo non potranno mai fare a meno di affrontare quel bilanciamento con gli altri diritti fondamentali dell'individuo. Infatti, così come nessuno metterebbe in

[67] Questo aspetto è affrontato maggiormente nel dettaglio nel prossimo paragrafo, dove il concetto di proprietà intellettuale e di riserva dei diritti si scontra non solo con gli altri interessi costituzionalmente riconosciuti, quali appunto la libera circolazione delle idee e della cultura, ma con le stesse modalità di acquisizione e godimento della proprietà autonomamente intesa.

dubbio la prevalenza della dignità della persona piuttosto che il valore della vita umana di fronte alla garanzia del diritto di proprietà[68], così come nessun sistema giuridico riconoscerebbe all'autonomia privata una legittimazione tale da sottrarsi alle regole vigenti nella società[69], così bisogna ribadire con forza che l'esercizio della propria iniziativa economica privata "non può svolgersi in contrasto con l'utilità sociale o in modo da arrecare danno alla sicurezza, alla libertà e alla dignità umana", così come la proprietà privata deve sottostare alla disciplina che la legge le impone circa "i modi di acquisto, di godimento e i limiti allo scopo di assicurarne la *funzione sociale* e di renderla accessibile a tutti".

Nella prospettiva che qui ci interessa, un servizio quale un *social network*, in particolare si parla di quei *social network* ad ampia diffusione quali *Facebook*, *Twitter* ma anche di quei portali quali *Blogger* e altri che permettono ai singoli utenti di pubblicare il proprio *blog*, o addirittura strumenti di pubblicazione o ricerca dei contenuti quali *Vimeo* e *YouTube*, che ricoprono *indubbiamente* una funzione sociale e culturale, oltre a muoversi su uno spazio strutturalmente suscettibile di direzionarsi verso situazioni di concentrazionismo ostili alle libertà individuali, devono subordinare il proprio interesse privato ai limiti imposti dalla garanzia dei diritti costituzionalmente proclamati e garantiti dalla Costituzione.

---

[68] Anche se una certa "cultura" giuridica preponderante cerca di insegnarci il prevalente valore dei beni di nostra proprietà rispetto alla vita di coloro che questi beni minacciano.

[69] Si pensi alla costituzione di un'associazione ai sensi dell'art. 18 della Costituzione italiana: pur essendo questo diritto di libertà un diritto sancito in maniera ben più solenne e con minori vincoli espliciti, nessuno potrebbe vedersi legittimato dar valore ad un statuto che preveda, in estremo, l'omicidio di colui che decida di abbandonare l'associazione stessa dopo essersi iscritto.

Possiamo immaginarci un futuro in cui il potere giudiziario intervenga a garanzia del diritto alla libera manifestazione del pensiero di fronte agli abusi delle modalità di godimento della proprietà privata, nei casi in cui queste modalità ne facciano dimenticare la funzione sociale a cui deve essere orientata?

4.2.2. La proprietà intellettuale e la diffusione della cultura

Altro problema che tocca tangenzialmente l'oggetto in questione, ma su cui non si può sorvolare trattando di bilanciamento tra il diritto alla proprietà privata e gli altri diritti costituzionali nel caso dello sviluppo delle nuove tecnologie, è quello delle modalità di tutela, legislative e tecnologiche, della proprietà intellettuale su *Internet*, strumento che si è rivelato fonte di facili aggiramenti della normativa vigente in tema[70], origine quindi di una rinnovata offensiva dei sostenitori dell'assolutezza della proprietà privata[71] e di un contro movimento culturale e giuridico incentrato al contrario sulla concessione alla generalità degli utenti di parte dei diritti proprietari, riservandosene

---

[70] È sufficiente richiamare sommariamente la diffusione delle tecnologie *peer-to-peer*, quelle tecnologie in grado di favorire scambi diretti e rapidissimi di contenuti digitali tra i più distanti utenti sulla terra, che hanno generato e stimolato un'amplissima circolazione di questi contenuti a prescindere dall'adempimento degli oneri legali concernenti i diritti di proprietà intellettuale eventualmente connessi a quei medesimi contenuti.

[71] Sulla disciplina del *copyright* assoluto secondo la legislazione statunitense ampiamente ispirata dalle *lobbies* delle case discografiche, così come sulle tutele tecnologiche dei medesimi diritti attraverso strumenti tali da colpire persino i diritti propri dell'utente in questione e le connesse problematiche, vedi LESSIG L., cit., 2004, nota 55.

solo alcuni secondo la formula *some rights reserved*.

Sotto il punto di vista che ci interessa sottolineare in questa sede, la questione della tutela dei diritti di proprietà intellettuale in particolare su *Internet* investe proprio quel bilanciamento di cui si è parlato sinora, e la proposizione di un modello che prevede la riserva di alcuni diritti in capo al titolare della proprietà intellettuale di un determinato *software* o contenuto risponde proprio ad un'esigenza di autotutela[72] dai rischi fortemente connessi all'abuso della tutela assoluta dei diritti di proprietà intellettuale. Questa tutela assoluta si è infatti dimostrata capace – forse – di comportare vantaggi immediati e più consistenti – soprattutto sotto il profilo economico – ma le nefaste conseguenze sotto il profilo della diffusione della cultura e, a lungo termine, anche della profittabilità del medesimo mercato sono state svelate e spiegate da tempo e solo gli attori meno accorti hanno preferito continuare sulla linea intrapresa alla fine degli anni '90[73].

Sotto un profilo strettamente giuridico, il termine di paragone a cui il legislatore deve fare riferimento all'atto di elaborare una disciplina

---

[72] Il movimento *Creative Commons*, e prima ancora il movimenti della *Free Software Foundation* promosso da Richard Stallman, nacquero e si svilupparono sulla scia di questo dibattito, ciascuno nella propria forma e con i propri scopi specifici, come forma di autonormazione da parte degli utenti, dei tecnici e della dottrina culturalmente legata al fenomeno di *Internet* e in parte in contrapposizione all'inidoneità del modello proprietario promosso dalle citate lobbies direttamente interessate alla stretta disciplina del fenomeno e fatto proprio da un legislatore inaccorto.

[73] In senso contrario e quindi favorevole ad uno sviluppo più armonioso del rapporto tra esigenze di tutela dei diritti di proprietà intellettuale sui contenuti diffusi via *Internet* e gli innegabili vantaggi in termini di diffusione di cultura e conoscenza, non poche di queste lobbies prima accanite battagliere contro il *download* illegale hanno cambiato strategia e si muovono verso una legalizzazione di fatto del fenomeno attraverso il ricorso a diversi strumenti non coercitivi, per esempio il ricorso alla pubblicità.

della tutela della proprietà intellettuale su *Internet*, e l'interprete all'atto di applicarla ad un caso concreto, non può e non deve essere il solo criterio della tutela incondizionata della proprietà privata, ma, attraverso il rinvio da parte della medesima Costituzione alla "funzione sociale" della proprietà non può che essere, nel nostro caso, l'art. 9 della Costituzione, secondo il quale "La Repubblica promuove lo sviluppo della cultura e la ricerca scientifica e tecnica". Avendo presente i termini della questione, è più facile per l'interprete districarsi attraverso quella giungla di possibili casi concreti che vi si possono presentare: dal download per solo utilizzo personale, a quello per scopi commerciali, dall'ulteriore diffusione a titolo gratuito, a titolo d'insegnamento o di ricerca, dalla violazione volontaria di copyright a quella colposa o addirittura a quella che assume caratteri di ineluttabilità, nel caso di materiali ancora tutelati dalle legislazioni in materia ma ormai fuori da ogni catalogo commerciale, e così via.

Per ultimo, la disciplina delle eventuali conseguenze nel caso di violazione sanzionabile della disciplina della tutela dei diritti di proprietà intellettuale non può informarsi ai suddetti criteri di univoca tutela della posizione proprietaria, ma deve tener conto degli interessi che possono esserne toccati: l'esempio tangibile è il caso francese della "*loi favorisant la diffusion et la protection de la création sur Internet*" nella sua forma originaria che prevedeva, alla terza accertata violazione di copyright attraverso l'utilizzo di *Internet*, il distacco forzato, da parte di un'autorità amministrativa, della connessione del "criminale" in questione. Il progetto di legge è stato fortunatamente – e ovviamente – dichiarato incostituzionale dal *Conseil Constitutionnel* francese, in primo luogo a causa dell'affidamento ad un'autorità amministrativa di una decisione, quella del distacco da una connessione *Internet*, che per la portata in grado di incidere sui diritti costituzionali propri di ciascun

individuo non può che essere demandata ad un organo giurisdizionale, unico in grado di garantire la necessaria imparzialità. In secondo luogo, riguardo la caratterizzazione del diritto all'accesso a *Internet* come diritto inalienabile dei cittadini.

Il problema rientra a questo punto proprio sul terreno che ci interessa, quello della tutela del diritto alla libertà di espressione, come garantita dall'art. 21 della Costituzione italianao "attraverso ogni altro mezzo di diffusione", dall'art. 10 della Convenzione Europea per la salvaguardia dei Diritti dell'Uomo del 1950, dall'art. 11 della Carta di Nizza del 2004, e, nell'ambito della comunità internazionale, dall'art. 19 della Dichiarazione universale dei Diritti dell'Uomo del 1948, dei suoi limiti, tanto quelli espliciti quanto quelli impliciti elaborati attraverso il bilanciamento con gli altri diritti costituzionali e, si può aggiungere, della ragionevolezza degli interventi legislativi in sede di bilanciamento di questi interessi. In quest'ottica sorge spontaneo il dubbio: è ragionevole prevedere, nel caso di violazione, finanche reiterata, dei diritti di proprietà intellettuale, la sanzione della limitazione d'imperio del diritto alla libera manifestazione del pensiero attraverso la rete?

4.2.3. (*segue*): il ruolo del giudice nel caso Hadopi

Una palese critica alla legge appena analizzata, in particolare in materia di "tutela delle libertà individuali", si può muovere verso l'attribuzione di ampie competenze alle autorità amministrative, in particolare al Governo e alle forze di Polizia, così come alle associazioni o imprese private quali SIAE o *service provider*, secondo un modello che vede la "privatizzazione delle responsabilità" come strada maestra da perseguire al fine di raggiungere, finalmente, gli agognati obiettivi.

Il problema non è nuovol potere esecutivo viene ritenuto, generalmente, più efficace per raggiungere gli obiettivi prefissati in materia di tutela dei diritti patrimoniali propri dei detentori dei *copyright*. Poco importa se le decisioni in materia di *Internet*, così come le libertà coinvolte in caso di attività di controllo, toccano sensibili problematiche costituzionali nei confronti dei quali il potere esecutivo non è in alcun modo in grado di garantire la necessaria imparzialità. Su questa materia ha deciso il *Conseil Constitutionnel*, chiamato a giudicare sulla legge cd. "Hadopi I"[74] in materia di tutela dei diritti d'autore con una sentenza che merita un richiamo particolare.

L'art. 5 della legge istituisce un capitolo primo nel titolo III del libro III della parte prima del codice della proprietà intellettuale che sarà composta da 34 articoli (dal 331-12 al 331-45), dedicati alla disciplina di un'autorità pubblica indipendente, la "*Haute autoritè pour la diffusion des œuvres et la protection des droits sur Internet*" da cui il nome Hadopi, le cui finalità sono quelle di favorire la tutela del diritto d'autore. L'art. 11, attraverso l'aggiunta degli art. 336-3 e 336-4, stabiliva a carico di qualsiasi persona titolare di un accesso a servizi di comunicazione pubblica in linea un obbligo di sorveglianza affinché questo accesso non venga utilizzato ai fini di "riprodurre, rappresentare, mettere a disposizione o di comunicare al pubblico opere o materiali protetti dal diritto d'autore".

La legge, cosiddetta "dei tre schiaffi", prevedeva infatti che l'Alta autorità, ai sensi dell'art. 333-27, riconosciuta una prima violazione delle norme in materia di diritto d'autore inviasse un messaggio elettronico a

[74] La legge è consultabile in lingua francese sul sito del Senato all'indirizzo http://www.senat.fr/leg/pjl07-405.html (verificato il 12.05.2014).

scopo di avvertimento all'utente. Nel caso di ulteriore violazione, era previsto l'invio di una raccomandata con ricevuta di ritorno. Infine, nel caso di una terza violazione, l'Alta autorità poteva pronunciare, aperta una procedura in contraddittorio e in funzione della gravità delle violazioni, una delle seguenti sanzioni: la sospensione dell'accesso a *Internet* per un periodo da due mesi a un anno e il divieto di stabilire altra connessione attraverso un altro operatore (comma 1); un'ingiunzione di prendere misure destinate a prevenire il ripetersi delle violazioni (comma 2). Ai sensi dell'art. 331-28, era possibile stabilire, attraverso una transazione, la sanzione della sospensione della connessione per un periodo da uno a tre mesi. Il *Conseil Constitutionnel* è stato chiamato a decidere sulla costituzionalità di numerosi aspetti della legge, in particolare, ed è quello che più ci interessa in questa sede, la prevista possibilità di sospendere la connessione ad *Internet*, con tutte le ricadute sotto il profilo dei diritti costituzionalmente riconosciuti, in virtù di violazione del diritto d'autore, vale a dire del diritto alla proprietà intellettuale[75].

Innanzitutto il *Conseil Consitutionnel* richiamò i principi vigenti in materia. L'art. 11 della Dichiarazione dei diritti dell'uomo e del cittadino del 1789 stabilisce che "la libera comunicazione dei pensieri e delle opinioni è uno dei diritti più preziosi dell'uomo: ogni cittadino può dunque parlare, scrivere e pubblicare liberamente, salvo rispondere dell'abuso di questa libertà nei casi determinati dalla legge", da cui

[75] È da tenere a mente che, in ogni caso, la tutela costituzionale destinata alla proprietà privata nell'ambito dei testi e della tradizione costituzionale francese è più profonda di quella italiana. L'art. 2 della Dichiarazione universale dei diritti dell'uomo e del cittadino del 1789 stabilisce infatti come diritti naturali e inalienabili dell'uomo "la libertà, la proprietà, la sicurezza e la resistenza all'oppressione".

deriva, secondo il *Conseil*, vista "l'importanza ai fini della partecipazione alla vita democratica e di espressione delle idee e delle opinioni", il diritto ad accedere ai nuovi mezzi di comunicazione pubblica online. Gli art. 2 e 17 della Dichiarazione tutelano la proprietà privata, ed in questo senso "la lotta contro le pratiche di contraffazione che si sviluppano su *Internet* risponde agli obiettivi di salvaguardia della proprietà intellettuale". Il principio della separazione dei poteri permette si ad un'autorità amministrativa di emettere sanzioni nell'esercizio delle proprie funzioni, fintanto che siano rispettati il principio di legalità dei diritti e delle pene e i diritti della difesa. Ai sensi dell'art. 34 della Costituzione, che stabilisce la riserva di legge in materia di esercizio dei diritti civili e delle garanzie fondamentali da accordare ai cittadini in materia di libertà pubbliche, il legislatore può approvare leggi per conciliare (rectius, bilanciare) il diritto alla proprietà privata e il diritto alla libera comunicazione ma, ricordò il *Conseil*, "la libertà di espressione e di comunicazione è così preziosa che il suo esercizio è una condizione della democrazia e una delle garanzie del rispetto degli altri diritti e libertà" e, di conseguenza, "i limiti all'esecizio di questa libertà devono essere necessari, ragionevoli e proporzionali all'obiettivo ricercato".

Con riferimento alle discipline previste dalla legge della cui costituzionalità si discute il *Conseil Consitutionnel* ricordò che l'Alta autorità, "che non è un organo giurisdizionale", poteva restringere l'accesso a *Internet*. Di conseguenza "i suoi poteri possono condurre alla restrizione dell'esecizio, di chiunque, del proprio diritto di esprimere e comunicare liberamente, in particolare dal proprio domicilio". Di conseguenza, "in virtù della natura della libertà stabilita dall'art.11 della Dichiarazione del 1789, il legislatore non poteva, quali che fossere le garanzie inscritte nella pronuncia delle sanzioni, affidare tali poteri ad

un'autorità amministrativa al fine di proteggere i diritti dei titolari di diritto d'autore".

Considerato infine che, ai sensi dell'art. 9 della Dichiarazione del 1789, "ogni uomo si presume innocente fino al momento in cui è dichiarato colpevole" il legislatore "non può istituire la presunzione di colpevolezza in materia repressiva" benché, "in casi eccezionali, tali presunzioni possano essere stabilite, in materia di contravvenzioni" a condizione che non siano "irreparabili", che sia "garantito il rispetto dei diritti della difesa" e che "i fatti inducano ragionevolmente alla verosimiglianza dell'imputabilità". E, con riferimento alla disciplina della legge in questione che stabilisce che solo il titolare del contratto d'abbonamento a *Internet* può essere destinatario delle sanzioni stabilite, salvo prova contraria, il *Conseil* dichiara che l'inversione dell'onere della prova in questo ambito consiste in una presunzione di colpevolezza contraria al citato art. 9 della Dichiarazione.

In virtù delle considerazioni qui riportate, che potremmo riassumere nel valore dei principi quali quello di legalità, della separazione dei poteri, della riserva giurisdizionale dei diritti e della presunzione d'innocenza, il *Conseil Constitutionnel* dichiarò l'incostituzionalità di tutte le norme concernenti il procedimento sanzionatorio che comporta la sospensione della connessione ad *Internet*, strumento in grado di permettere "la partecipazione alla vita democratica di espressione delle idee e opinioni", e l'incostituzionalità delle norme che stabiliscono l'obbligo di controllo dell'accesso a carico del titolare di un contratto di connessione ad *Internet*.

Questa decisione stabilì un precedente importante da tenere a mente nell'ambito del costituzionalismo europeo: *Internet* èvenne considerato, a tutti gli effetti, strumento in grado di garantire la partecipazione democratica e il diritto di manifestazione del pensiero, e

il suo utilizzo non può essere limitato se non nel rispetto dei principi costituzionali in ambito sanzionatorio, così come del "principio della separazione dei poteri".

5. "*Collateral murders*": il bilanciamento improprio dei diritti e degli interessi

La tematica dei limiti concernenti il diritto alla libera manifestazione del pensiero, così come all'esercizio di altri diritti riconosciuti tanto a livello costituzionale quanto a livello di legislazione ordinaria, in *Internet* non può evitare di considerare una caratteristica propria della rete che ne rende tecnicamente e giuridicamente difficile la disciplina e spesso annulla i risultati che legislatori e Governi vorrebbero raggiungere: il carattere transnazionale della rete.

Internet è appunto una rete internazionale che attraversa i confini di ogni paese e stabilisce contatti e relazioni interpersonali tra soggetti in realtà separati da oceani e catene montuose, ed allo stesso modo si vede la possibilità di rapporti giuridici, patrimoniali o meno, tra queste persone. Entra in questo modo in crisi non solo la teoria della sovranità statale, ma persino il diritto internazionale, che su questa teoria si basa, e i legislatori si trovano a far fronte a complicati intrecci di discipline elaborate in seno a differenti ordinamenti e sistemi giuridici, ciascuno con un background di esperienze proprie che lo distingue l'uno dall'altro[76]. I legislatori dei singoli paesi non hanno quindi gioco facile

[76] Anche la giurisprudenza ha già affrontato le questioni della giurisdizione sotto cui ricade una determinata fattispecie. Ad esempio, con la sent. n. 4741 del 17 novembre 2000, la Corte di Cassazione stabilisce la giurisdizione del

nel perseguire condotte illecite che, nei loro vari elementi costitutivi, attraversano i confini di più legislazioni. Lampante il caso della legislazione in materia di *Internet* del Myanmar che, nello stabilire il proprio ambito di applicazione lo determina per qualsiasi reato commesso "all'interno del paese, dall'interno del paese all'esterno del paese, dall'esterno del paese all'interno del paese".

Secondo aspetto critico delle legislazioni in materia di *Internet*, in particolare di quelle che comportano o richiedono un sequestro di contenuti, per esempio nel classico caso di diffamazione, la realtà della rete comporta il raggiungimento di risultati ben differenti da quelli ricercati: numerosi sono i casi in cui il sequestro ottiene il solo risultato di vedere il materiale sequestrato moltiplicarsi in una pluralità di spazi della rete, in particolare in quel network di spazi personali che è la blogosfera. A riguardo, pur in un caso differente, si può considerare il risultato raggiunto (o mancato) nel caso del sequestro di The Pirate Bay, noto sito di diffusione di materiale digitale anche protetto da copyright, raggiungibile dopo poche ore. Lo stesso, attualmente, accade con il sito di diffusione di torrent Isohunt.com, bloccato dal Governo statunitense e raggiungibile, stessa forma e stessi contenuti, all'indirizzo Isohunt.to.

Il primo problema riguarda l'efficacia dell'intervento delle autorità per limitare la circolazione di quei materiali che ciascun ordinamento, sia costituzionale o autoritario, riconduce ad un'alea di illegalità. In questa prospettiva rileva la specifica attitudine alla prevenzione della circolazione di materiali illegali o del compimento di atti contrari alle norme giuridiche di un certo ordinamento. Sotto questa lente, l'attività di

giudice italiano nel caso di diffamazione attraverso scritti pubblicati su un *server* localizzato all'estero, richiamando appunto le regole sulla consumazione del reato nel luogo di percezione da parte di soggetti non destinataria dell'offesa.

sorveglianza, intercettazione, blocco e censura è da ritenersi inefficace e, talvolta, controproducente. Le potenzialità della rete, e qui risulta uno dei ruoli più incisivi svolti da questo strumento, e le conoscenze tecnologiche delle realtà eversive, superano di gran lunga l'efficacia delle attuali contromisure per una pluralità di ragioni già anticipate e più avanti meglio dettagliate: l'intercettazione può essere aggirata attraverso l'utilizzo combinato di differenti tecnologie di anonimizzazione; in quei casi ove la comunicazione sia individuata, la transnazionalità della rete e le procedure di anonimizzazione rendono difficoltosa, se non impossibile, l'individuazione dei soggetti responsabili; quando, infine, sia possibile localizzare la fonte di determinate comunicazioni, informazioni e materiali sono già arrivati alla destinazione specifica e difficilmente il destinatario lo avrà recuperato dal proprio domicilio o registrando la propria identità. In questa situazione, l'attività di blocco o di chiusura di siti si rivela in grado di travolgere facilmente l'ambito di legittimo esercizio dei diritti alla libertà di espressione, anche in quei casi più estremi al limite della legalità, senza necessariamente prevenire o perseguire attività illegali, minacce alla pubblica sicurezza, atti di eversione o terrorismo. In questo senso varrebbe la pena di chiedersi se il vantaggio conseguito da una presunta minor circolazione pubblica di comunicazioni illegali possa compensare, sul piano dell'efficacia dell'attività di prevenzione, la perdita di quei segnali di reale minaccia, destinati a cercare strade alternative e meno conosciute.

Non è quindi con leggi confuse e generalizzanti che saranno frenati le attività illegali poste in essere attraverso la rete. Così come non servono i sequestri indiscriminati a difendere i beni giuridici che un ordinamento ritenga meritevoli di tutela. Altrettanto la previsione di normative o strumenti di controllo rischia al contrario di portare alla promozione e alla diffusione di strumenti elusivi "*Internet*: né censura

né anarchia selvaggia", titolava un rilevante saggio di RODOTÁ[77] in materia. Il confine tra le due situazioni è labile e di difficile identificazione, e gli interessi in gioco, appunto, valori costituzionalmente protetti al rango di diritti fondamentali. Il lavoro del giurista, con la diffusione della rete, si complica notevolmente.

[77] RODOTÁ S., *Internet: né censura né anarchia selvaggia*, Telèma, 1996, http://www.geocities.com/centrotobagi/news2.htm (verificato il 12.05.2014).

CAP III – SORVEGLIANZA GLOBALE E RESISTENZA DIGITALE

SOMMARIO: 1. Libertà d'espressione, limiti, censura e sorveglianza. – 2. *Internet* e le ICTs come strumenti di sorveglianza globale. – 3. Stato e sorveglianza globale oggi: il dogma securitario – 3.1. La rete ECHELON e il rapporto Europeo del 2000. – 3.2. Il cd. *Datagate* e il Progetto PRISM. – 3.3. Le basi legali di PRISM. – 3.4. La FISA, PRISM e il ruolo dei *service providers*. – 4. L'approccio europeo al bilanciamento tra sicurezza e diritti. – 4.1. La Direttiva 2006/24/EC sulla *Data Retention* – 4.2. La reazione alle rivelazioni sul Progetto PRISM. 5. – La resistenza digitale. – 5.1. *Hacker* e attivismo sociale e politico. – 5.2. *Hacktivists* e *Liberation Technologies*. – 5.3. La cifratura dei dati. – 5.4. L'anonimato delle comunicazioni. – 5.5. La cancellazione sicura dei dati. – 5.6. Altre tecniche per proteggere e nascondere. – 5.7. La valutazione del rischio. – 6. La formazione dei giuristi al bilanciamento tra sorveglianza e resistenza.

1. Libertà d'espressione, limiti, censura e sorveglianza

Nei due capitoli precedenti si è dato rilievo alle dinamiche sociali che influiscono sulla posizione delle norme di fonte giuridica all'interno della disciplina dell'esercizio dei diritti su *Internet* e agli aspetti più rilevanti della disciplina, giuridica e non, del diritto alla libertà di espressione, tanto con attenzione alla tutela del suo esercizio in origine riservato ai mezzi di comunicazione tradizionali, quanto agli sforzi interpretativi e di riforma finalizzati a ricondurvi l'espressione tramite mezzi di telecomunicazione.

Il panorama che ne risulta, destinato a un costante rinnovamento

alla luce della rapidità di evoluzione dei fattori economici e tecnologici che vi influiscono, ha ora comunque contorni abbastanza delineati nei suoi caratteri generali, un po' meno invece su talune specifiche ipotesi di frontiera. Tra i caratteri generali acquisiti, la riconducibilità delle attività di comunicazione, divulgazione e informazione su *Internet* all'alveo del diritto alla libertà di espressione e quindi alla tutela garantita da eventuali testi costituzionali o di natura costituzionale che ne rivendicano la tutela: in Italia l'art. 21 della Costituzione del 1948, in Francia l'art. 11 della Dichiarazione universale dei diritti dell'Uomo del 1789, negli Stati Uniti il Primo Emendamento, in seno al Consiglio d'Europa l'art. 10 della Convenzione Europea per la salvaguardia dei Diritti dell'Uomo del 1950, nell'Unione Europea l'art. 11 della Carta di Nizza del 2004, nell'ambito della comunità internazionale l'art. 19 della Dichiarazione universale dei Diritti dell'Uomo del 1948 e l'art. 20 della Convenzione internazionale sui diritti civili e politici del 1966. Se ciò può al giorno d'oggi apparire palese, posta la natura di *Internet* quale rete globale di reti locali di comunicazione, la strada ha necessitato di sforzi interpretativi notevoli. Altra acquisizione non contestabile è l'esistenza di ragioni comuni suscettibili di essere poste a fondamento di interventi finalizzati alla limitazione e alla compressione della stessa libertà di espressione in ragione di un'operazione di bilanciamento tra i diversi interessi, operata in via tanto costituzionale e legislativa, per la definizione dei margini di manovra degli interpreti, quanto in ultima istanza in via interpretativa, da parte delle autorità chiamate a decidere sui conflitti legati a casi concreti.

Sulla base del quadro fin qui delineato, si ritiene di interesse addentrarsi nel dettaglio della vita quotidiana del diritto alla libertà di espressione su *Internet*, e dei diritti in qualche modo comunque coinvolti in particolare quello del rispetto della vita privata, del suo esercizio,

della sua protezione e della sua limitazione, in relazione alle attività di sorveglianza globale poste in essere da autorità pubbliche e operatori privati nel perseguimento dei propri interessi. La libertà di espressione su *Internet* è infatti un terreno dove quotidianamente si svolgono conflitti anche aspri tra diversi diritti e interessi ma anche e soprattutto tra idee della società, del ruolo dello Stato e degli attori privati, della stessa idea di cittadinanza globale apertamente in contrapposizione tra loro e, in taluni casi, del tutto incompatibili.

A tal fine, è intenzione in questo capitolo di raccogliere alcuni esempi rilevanti di utilizzo di *Internet* e delle tecnologie della telecomunicazione ai fini dello svolgimento di attività di sorveglianza, prevenzione e repressione di attività considerate in contrasto con gli interessi statali o economici. Nella direzione opposta, la seconda parte di questo capitolo sarà dedicata alla resistenza digitale, alle pratiche, agli strumenti, alle modalità, alle giustificazioni, alle finalità e alle implicazioni derivanti dall'utilizzo delle tecnologie di comunicazione quali *Liberation Technologies*, ossia per "la difesa dei diritti umani, il miglioramento della *governance*, l'emancipazione dei poveri e la promozione dello sviluppo economico".

Tra le attività promosse dagli Stati per il tramite delle autorità di sicurezza pubblica, dei servizi segreti, delle agenzie di spionaggio o controspionaggio, delle pubbliche magistrature, i più rilevanti casi riguardano le attività formalmente indirizzate alla prevenzione o al contrasto dell'estremismo, dell'eversione o del terrorismo. Tra questi risalta in modo lampante il percorso delle agenzie governative che nell'arco degli ultimi due decenni ha portato al passaggio dal Progetto Echelon al Progetto PRISM, nella stampa internazionale ribattezzato

DataGate[1].

Un secondo gruppo di esperienze di grande interesse riguarda invece le attività di censura posta in essere dagli Stati per la tutela del diritto di proprietà intellettuale, di marchi e brevetti, dell'integrità dei minori, della dignità personale e dell'onore promosse attraverso la previsione di sanzioni penali, civili e amministrative e la predisposizione di sistemi differenziati di intervento sulle reti di telecomunicazione. La tematica più rilevante in questo ambito è l'adozione di sistemi o di modalità di censura preventiva dei contenuti su *Internet* attraverso la predisposizione di filtri o la modifica del regolare funzionamento del DNS o ancora l'adozione di ingiunzioni di collaborazione agli intermediari che ospitino o favoriscano il transito o il raggiungimento dei materiali suppostamente illeciti. Tra queste ipotesi, rilevano maggiormente le pratiche di collaborazione tra autorità giudiziari e di pubblica sicurezza e intermediari fornitori di servizi della società di comunicazione in relazione a oggetti quali il blocco di siti *Internet* di diffusione di *torrent*, abilitanti lo scambio di materiale attraverso lo strumento del *peer-to-peer*, quali i casi *The Pirate Bay* e, più recentemente, *Isohunt*, il sistema di ricerca e censura dei siti a contenuto pedopornografico e infine le ipotesi di ingiunzioni a destinazione di motori di ricerca e fornitori di servizi di *hosting* per specifiche ipotesi di illecito.

Ultimo fenomeno di interesse è ovviamente l'attività di

---

[1] Ricordando che, di sicuro interesse, vi sono anche le esperienze del *Golden Shield Project* cinese, del suo fratello minore vietnamita, e dei sistemi di censura posti in essere in Siria, Arabia Saudita, Iran e nei paesi del Mediterraneo, Egitto *in primis*, durante i movimenti di rivolta che hanno attraversato i rispettivi paesi.

sorveglianza globale e profilazione posta in essere direttamente dagli intermediari privati, quali Google, Apple, Microsoft tra le più rilevanti, svolte attraverso la raccolta massiccia e, spesso, indiscriminata di dati a carattere personale dei propri utenti e in generale degli utilizzatori tutti di *Internet* e rivolte alle finalità di profilazione personale, elaborazione di pubblicità mirata e alterazione delle regole di libero mercato per la formazione di cristallizzate situazioni di oligopolio. Tangenzialmente, la ricaduta di queste attività motivate perlopiù da interessi di natura economico-commerciale, hanno infatti in primo luogo l'effetto di comportare gravissime lesioni al diritto alla riservatezza e al diritto al controllo dei propri dati personali, dalle quali discende infine una marcata incidenza sull'esercizio della libertà di espressione, incanalata e indirizzata in binari precostituiti nella più totale negazione dell'aspirazione aperta e libera della rete delle reti. Occasionalmente, sarà di interesse tenere a mente tutto ciò in relazione alle concrete ipotesi di messa a disposizione dell'immensa mole di informazioni così raccolte, conservate ed elaborate, a favore delle autorità pubbliche interessate a conoscere gli indirizzi politici, sociali, culturali, gli interessi e soprattutto le intenzioni dei propri cittadini e dei cittadini degli altri paesi.

2. *Internet* e le ICTs come strumento di sorveglianza globale

Censura e sorveglianza fanno riferimento a due fenomeni distinti. La prima consiste nel prevenire la diffusione di contenuti, specifici o sufficientemente determinabili, ove un interesse di tutela individuale e collettivo è ritenuto prevalente rispetto alla rispettiva libertà di espressione, sia essa artistica, politica, culturale, sociale, religiosa, o

anche meramente personale. La sorveglianza invece è un'attività posta in essere in via preventiva, generalizzata o rivolta a soggetti o luoghi specifici, allo scopo di individuare condotte o contenuti illeciti o inopportuni, soggetti pericolosi o estremisti. La finalità può essere quella di provvedere successivamente a prevenire la diffusione di un determinato contenuto tramite attività, a quel punto, di censura. Oppure ancora di intervenire per impedire la commissione o il proseguimento di attività delittuose, e in questo senso vengono giustificate le odierne attività di sorveglianza globale finalizzate al compimento di attività di *counter-terrorism*.

La censura è attività che risale quantomeno fino all'Atene antica, a quel 399A.C, anno in cui Socrate venne condannato a morte. L'accusa era quella "di non riconoscere come Dei quelli tradizionali della città, ma di introdurre Divinità nuove; ed è anche colpevole di corrompere i giovani"[2], sostanzialmente un'accusa di ribellione alle istituzioni civili, allora una cosa sola con il fenomeno religioso. L'allievo di Socrate, Platone, scrisse ne La Repubblica a favore della censura nell'arte, quale imitazione di quanto noi chiameremmo realtà, a sua volta una mera imitazione. Gli esempi potrebbero continuare, con l'illuminante periodo dell'inquisizione religiosa nel Medioevo: è del 1559 l'*Index Librorum Prohibitorum*, indice dei libri il cui possesso e la cui lettura era dalla Chiesa Cattolica proibita ai cattolici tutti, abolito solamente nel 1966, neppure cinquant'anni fa. E di tale attività il XX secolo, caratterizzato da un ritorno e un'affermazione della prevalenza degli Stati, totali, sugli individuio, è stato estremamente fecondo. Così la diffusione delle

[2] DIOGENE LAERZIO, *Vite e dottrine dei più celebri filosofi*, Milano, Bompiani, 2005, II, 5, 40

tecnologie dell'informazione e della comunicazione, ampliando a dismisura le potenzialità di circolazione di informazioni, ha determinato un'impennata di attività censorie su larga scala e su ogni tipo di materiale in circolazione.

La necessità di censurare è insita nella stessa funzione dell'autorità, sia essa laica o religiosa, pubblica o privata, in ragione della distinzione operata dalle norme che regolano i rapporti tra i soggetti che determinano necessariamente la presenza di un qualcosa di illecito.

L'aumento delle attività di sorveglianza è invece strettamente legato allo sviluppo tecnologico. La diffusione dei mezzi di informazione di massa verticali e centralizzati, l'incremento nella circolazione delle informazioni è compensato dall'aumento delle capacità di diffusione dell'ordine stabilito, delle minacce sanzionatorie, dello stimolo a un'autonoma conformazione al sistema dominante. Se con lo sviluppo delle tecnologie di comunicazione digitali, capaci di offrire spazi di comunicazione alla globalità di persone, queste sono trasformate da *lettori, ascoltatori* o *spettatori* in *autori*, determinando, in apparenza, la recisione dei rapporti di dipendenza da un autorità per l'esercizio di svariate libertà, le modalità di funzionamento di queste stesse tecnologie, caratterizzate dall'identificare ogni azione posta in essere nel contesto digitale con ulteriori informazioni idonee ad arricchirla di dettagli personalissimi, mentre rendono più difficile l'attività di censura specifica, si prestano invece perfettamente alle necessità di attività di sorveglianza, con un grado di diffusività e pervasività senza alcun precedente nella storia umana. Diffusività e pervasività tali da superare ampiamente le rappresentazioni letterarie distopiche elaborate nel XX secolo. Nella citata opera di Lawrence

Lessig[3] era stato ben evidenziato il ruolo di ampliamento delle capacità di sorveglianza svolto dagli strumenti di trasmissione digitale.

Sulla base delle giustificazioni giuridiche o politiche presentate al capitolo precedente, gli Stati, e frequentemente gli attori privati, fanno ricorso a una pluralità di tecniche per la sorveglianza di *Internet* e a diversi elementi identificativi per la raccolta di informazioni specifiche sulle attività svolte e sulle specifiche persone coinvolte. Invertendo l'ordine, prima di osservare le tecniche utilizzate e alcuni casi più rilevanti, appare opportuno provvedere a un'indicazione degli elementi tecnici che forniscono, nel contesto digitale, informazioni preziose per lo svolgimento di attività di sorveglianza e, eventualmente in via successiva o preventiva, anche di censura. Questi elementi possono essere suddivisi in fattori tecnologici e fattori comportamentali, ove ai primi ci si riferisce quando gli elementi in grado di permettere le attività di sorveglianza sono strettamente legati al funzionamento tecnico degli strumenti di comunicazione adottati, generalmente a prescindere dalle scelte e dalle determinazioni degli utilizzatori, mentre con i secondi si fa riferimento ai comportamenti effettivamente tenuti nel contesto digitale, di per sé in grado di fornire informazioni ulteriori rispetto a quelli meramente tecnici o, in casi invece opposti, in grado di ridurre le tracce dagli utilizzatori lasciate dietro di sé.

Tra i fattori tecnologici, rilevano l'indirizzo IP, il numero di identificazione tecnico di un dispositivo, il *browser* e il sistema operativo utilizzati con le loro impostazioni, i *cookies*, i registri di *log* dei *server* dei siti utilizzati e i registri di *log* dei *router*, i metadati, delle *email* o dei file multimediali diffusi.

---

[3] LESSIG L., cit., 2006.

a) *l'indirizzo IP* è lo strumento utilizzato dal protocollo IP[4] al fine di permettere l'elaborazione e il trasporto dei pacchetti di dati in cui sono scomposti e che identifica univocamente i dispositivi dai quali accediamo a *Internet*. È una sequenza di numeri e punti composta da quattro numeri compresi tra 0 e 256 divisi da tre punti[5]. Può identificare lo specifico dispositivo fisso, quale un laptop o un desktop, o mobile, ovvero solamente un *router* dietro al quale vi sono poi una pluralità di dispositivi, spesso ipotesi di tipo aziendale. L'indirizzo IP ci identifica nella totalità delle azioni svolte su *Internet* e viene registrato sui registri di log di ogni *server* o *router* attraversato dai pacchetti in cui sono scomposte le nostre trasmissioni. Il fornitore del servizio di connessione, sia esso un operatore di telefonia e *Internet* privato, un'istituzione universitaria o un ente privato, o anche un *Internet* cafè, è in grado di rilevare e registrare tutte le richieste di dati operate durante la nostra connessione, catalogate sotto l'indirizzo IP corrispondente. Posto che l'indirizzo IP può essere statico oppure dinamico, ossia essere stabilmente attribuito ad una specifica utenza ovvero essere attribuito di connessione in connessione, in questo secondo caso i fornitori di servizi

---

[4] Lo IETF ha elaborato un *Request for comments*, nel 1981, documento contenente le specifiche del protocollo IP, liberamente consultabile all'indirizzo http://www.ietf.org/rfc/rfc791.txt (verificato il 12.05.2014).

[5] DE NARDIS L., nel recente paper *Internet Points of Control as Global Governance*, CIGI, 2013, pag. 5, "*IP addresses are the unique binary numbers every device using the Internet possesses, either permanently or assigned temporarily for a session. The format of Internet addresses is specified by the IP standard. The long-standing version of IP, known as IP version 4 (IPv4), assigns 32 bits (32 zeros and ones) to each binary address [...] IP addresses are at the heart of how the Internet routing functions, because they are used by routers to transmit information to its destination over the most expeditious path*". http://www.cigionline.org/sites/default/files/no2_3.pdf (verificato il 12.05.2014).

di connessione, sulla base delle regole e delle disponibilità di pacchetti di indirizzi IP assegnati dall'ICANN, attribuiscono e registrano tale attribuzione in modo da poter distinguere, a titolo d'esempio, all'interno di uno specifico orario, a quale soggetto e per quale determinato lasso temporale fosse stato attribuito uno specifico indirizzo IP poi successivamente attribuito ad altri. Infine, un meccanismo simile è adottato quando un solo indirizzo IP sia attribuito a un rete, tipicamente aziendale o universitaria, composta da una pluralità di dispositivi: in tal caso, esistono suddivisioni ulteriori dell'indirizzo IP affinché il *computer* intermediario (*proxy* o *gateway*), possa presso di sé registrare le operazioni svolte dai singoli dispositivi. Sulla base di questo strumento, è possibili risalire al dispositivo autore da cui sono state poste in essere attività le più svariate sulla rete, magari nella convinzione che le stesse fossero anonime: la pubblicazione di un post o un commento anonimo su un blog, il caricamento di un file multimediale, di un video o di un audio o di un documento, su un servizio di hosting, la registrazione o l'accesso a un servizio di webmail.

b) il numero di identificazione di uno specifico dispositivo, del tipo *Open Device Identification Number*, è strumento adottato o in via di adozione da parte degli operatori che producono l'*hardware* a cui si ricorre per utilizzare servizi interconnessi, in particolare nel contesto di operatori dell'*Internet* mobile. Consiste in un testo alfanumerico in grado di identificare quale unico al mondo il dispositivo utilizzato. È un'applicazione nell'ambito del commercio di dispositivi mobili della creazione del numero unico di identificazione – o UIN, acronimo corrispondente a diverse sigle, quali *Unique Identification Number*, *User Identification Number*, *Universal Identification Number*, *Unit Identification Number* – il cui scopo è di elaborare un catalogo che, nel rispettivo ambito, sia esso commerciale, organizzativo o militare,

consenta di individuare l'unicità di un elemento parte di un gruppo più ampio. Se tale identificato è stato in precedenza relegato all'identificazione fisica dell'*hardware*, per il riconoscimento di tipo anonimo dei dispositivi che utilizzano certe applicazioni, l'utilizzo dello stesso numero può portare alla correlazione tra dispositivo e legittimo proprietario, direttamente da parte dei produttori o distributori del dispositivo a prescindere quindi dalla necessità di risalire alle informazioni fornite dall'indirizzo IP.

c) il *browser*, ossia il *software* utilizzato per consultare siti web, e il *sistema operativo* utilizzati raccolgono e lasciano tracce relative alle attività svolte su *Internet*. Dal primo punto di vista rilevano la quantità e la qualità delle informazioni che vengono conservate presso il dispositivo dell'utente, in particolare attraverso la politica di gestione dei *cookies*, delle password e dei nomi utente personalmente impostati o standard. Inoltre tali informazioni sono arricchite dalla cronologia delle pagine *web* visitate che, ovviamente, diventerebbe fonte di informazioni rilevantissime se resa accessibile, e dai file temporanei memorizzati presso il dispositivo stesso per agevolarne la consultazione in un momento successivo. Dal secondo punto di vista browser e sistema operativo possono ben fornire elementi di identificazione dell'utente oltre gli altri strumenti: così le impostazioni dell'orario e della lingua possono fornire indicazioni relative alla localizzazione statuale del dispositivo o alla nazionalità dell'utente; le impostazioni particolari o specifiche, le versioni rare o personalizzate, i *software* o gli *add-ons* installati possono creare un profilo tendenzialmente unico e di conseguenza tracciabile nelle sue attività svolte sulla rete.

d) i registri di *log* svolgono un ruolo chiave nel funzionamento del web e sono caposaldo degli strumenti in grado di fornire informazioni sulle attività svolte su *Internet* e sull'identità dei soggetti che le pongono

in essere. I registri di *log* sono *file* di testo aggiornati dinamicamente da ogni dispositivo, *server*, *router*, sito web, relativamente alle attività svolte dagli utenti, identificati sotto forma di indirizzo IP o eventualmente di nomi utente registrati presso lo stesso, all'interno o attraverso il sito, *server* o *router* stesso. Le informazioni raccolte spaziano dall'orario di connessione alla durata della visualizzazione, dalla pagina di origine alla pagina successiva, fino alla possibile registrazione dei dati identificativi appena evidenziati in materia di *software* e sistemi operativi del dispositivo che utilizza i servizi del *server*. Tra gli utilizzi più rilevanti ai fini di tracciabilità delle attività svolte su *Internet*, la consultazione dei *file* di testo contenenti i *log* può portare a ricondurre a un medesimo utente una pluralità di indirizzi IP utilizzati oppure consentendo l'identificazione dei singoli nel caso di un medesimo indirizzo IP identificativo di più soggetti. Nel primo caso infatti l'accesso a uno stesso servizio da parte di più dispositivi potrà dare indicazioni circa la proprietà di quei dispositivi, fornendo elementi utili a suggerire l'incrocio di eventuali dati raccolti in relazione ai due diversi indirizzi IP potenzialmente riferiti a una sola persona. Nel secondo caso invece l'utilità sarà opposta, suggerendo la ricerca di elementi che aiutino a scindere la titolarità delle informazioni raccolte in capo a uno o l'altro soggetto che accede al servizio o al sito per il tramite di un medesimo indirizzo IP. In quest'ultimo caso, vale la pena anticipare come di distingua l'ipotesi in cui la ricerca di informazioni sia posta in essere da autorità pubbliche, che ben potrebbero accedere ai registri di log dei *server* o dei fornitori di servizi di connessione per risalire al dispositivo, e quindi potenzialmente al soggetto, specificamente individuato, dall'ipotesi in cui tale ricerca sia svolta, a titolo d'esempio per finalità commerciali, da operatori privati non in grado di accedere direttamente a queste informazioni e quindi in ultima

istanza estremamente interessate a quanto desumibile da tale incrocio di informazioni da fonti diverse.

e) anche i *cookies* sono piccoli file di testo, salvati però nella memoria del dispositivo dell'utente e non nei *server* dei siti visitati o dei servizi utilizzati, che forniscono informazioni ai siti o ai servizi ai quali un soggetto possa accedere su *Internet*. La quantità e la qualità delle informazioni raccolte, così come la durata della loro conservazione, è stabilita da un incrocio di elementi di cui fanno parte, sostanzialmente, le impostazioni specifiche adottate dal sito che si visita, le impostazioni generali del browser e specifiche in relazione a un sito determinato e il tipo di *cookies* di cui si parla. Sostanzialmente, i *cookies* raccolgono informazioni sui nomi utente e sulle password di accesso ai servizi online di modo da non doverli reinserire a ogni accesso, sulle preferenze o le scelte nei siti di commercio elettronico, a titolo d'esempio sulla memorizzazione del "carrello della spesa", sulle impostazioni dei siti visitati, quali preferenze di sicurezza o di numero di risultati visualizzati o di tipo di filtro attivato per i motori di ricerca online, e infine possono essere utilizzati per tracciare il comportamento di un utente all'interno di un certo sito o in una pluralità di siti per monitorarne pagine visitate e preferenze. I *cookies* sono infatti testi dinamici, il cui contenuto è consultato, ed eventualmente aggiornato, a ogni nuova visita della pagina web corrispondente. Sulla base delle informazioni archiviate e conservate dal dispositivo utilizzato è quindi possibile risalire alle preferenze e inclinazione degli utenti che utilizzano il dispositivo coinvolto. La conservazione dei *cookies* è comunque legata a due ulteriori fattori, a questo punto però indipendenti dalla politica del sito destinatario, ossia la gestione generale o specifica operata a livello di browser dall'utente stesso e il tipo di *cookies* di cui si tratta. Quanto al primo profilo, diversi browser permettono diverse politiche di gestione

di *cookies*, al punto da poter rifiutare la conservazione degli stessi. Quanto al secondo profilo invece, esistono *cookies* la cui gestione, in particolare nel profilo del rifiuto o della loro cancellazione, è tecnicamente sottratta al libero arbitrio dell'utente, essendo infatti nel caso dei cd. flash*cookies* operata a livello di *software* specifico e non di browser, con conseguente aggiornamento automatico a prescindere dalle impostazioni preferite a riguardo.

f) i *metadati* sono, letteralmente, dati sui dati, e la loro esistenza precede le tecnologie digitali. Esempio classico di metadati sono le informazioni di classificazione dei testi all'interno di una biblioteca, che permettono di risalire a uno specifico testi secondo i più diversi criteri ritenuti rilevanti. In ambito telefonico i metadati, rispetto al dato centrale che sarebbe il contenuto delle telefonate, sono i numeri del chiamante e del destinatario, l'orario e la durata delle conversazioni, il luogo di chiamata o di ricezione, ove si faccia riferimento a telefonia mobile, attraverso l'identificazione della cella di riferimento, e, sempre nell'ipotesi di telefonia mobile, l'eventuale spostamento dei soggetti coinvolti, alla luce dell'agganciamento a celle distinte nel corso della telefonata. In ambito digitale i sono metadati tutti quelli che non riguardano specificamente l'informazione o il contenuto specifico della trasmissione. Sono quindi metadati tutti gli elementi fino ad adesso introdotti, l'indirizzo IP, il numero di identificazione, le informazioni raccolte tramite logs e *cookies* sulle attività svolte in relazione a luogo di origine, sistema operativo, browser o altri *software* utilizzati. Ricche di queste informazioni sono le email che indicano mittente, destinatario, timestamp, numero di contatti tra persone, una lunga serie di informazioni che permettono sostanzialmente di delineare con estremo dettaglio la sfera sociale e relazionale di ciascun individuo. Sulla rilevanza dei metadati ai fini di sorveglianza nell'ambito di navigazione

web, trasmissione di email o utilizzo di social network ci si soffermerà più ampiamente nell'illustrazione delle strategie e dei casi di sorveglianza globale. Nell'ambito digitale esistono infine altre informazioni la cui origine dipende direttamente dalla creazione del contenuto digitale e non dalla loro trasmissione, anche queste in grado di fornire informazioni rilevanti ulteriori al mero contenuto. Si tratta dei metadati relativi a file fotografici, audiovisivi e testuali, che portano all'interno della propria sequenza di numeri binari metadati relativi alla data di creazione o modifica, all'autore e a sistema operativo o al *software* utilizzati per la creazione, eventualmente del numero identificativo del dispositivo utilizzato e, in caso di materiale fotografico o audiovisivo realizzato con strumenti dotati di sistemi di geolocalizzazione, le coordinate GPS del luogo nel quale tale fotografia o tale video sono stati creati.

3. Stato e sorveglianza globale oggi: il dogma securitario

Il problema del conflitto tra sicurezza e libertà è giuridico e politico al tempo stesso: l'origine stessa dei diritti fondamentali deriva da una scelta di natura politica che caratterizza quella parte di Paesi del mon- do che l'hanno compiuta e non quelli che l'hanno rifiutata. Allo stesso modo, l'attuale preponderanza delle parole d'ordine della sicurezza nazionale sull'inviolabilità e la garanzia dei diritti umani è frutto di determinate scelte politiche assunte successivamente ai citati fatti del 2001 e degli anni seguenti. L'aspetto giuridico riguarda il vincolo che lega l'attività delle autorità degli Stati al rispetto dei testi legali in materia di diritti umani, a seconda anche della gerarchia dei

diversi principi dell'ordinamento. Carte, Convenzioni e Trattati internazionali, così come le Costituzioni scritte o consuetudinarie vanno lette con l'attenzione rivolta agli strumenti previsti affinché le dichiarazioni ivi contenute non risultino disattese. Sotto questo aspetto, le decisioni dei diversi Tribunali internazionali e costituzionali sono lo strumento fondamentale per muoversi in materia di legittimità di questa o quella specifica legislazione che intende normare la rete. Le conseguenze delle scelte compiute in materia di diritti fondamentali possono però essere disattese o aggirate giuridicamente, e le stesse scelte essere messe politicamente in discussione. Le politiche securitarie che si sono affermate dal 2001 in avanti e ad oggi sono ancora preponderanti affrontano entrambi questi percorsi. Attraverso la manipolazione dei concetti giuridici tradizionali, e il progressivo svuotamento della reale applicabilità, gli Stati eludono gli obblighi giuridici in materia di diritti umani: di questo percorso fanno parte sia l'abuso degli strumenti quali il segreto di Stato e di disposizioni vaghe e generiche, dietro le quali si celano attività di sorveglianza non trasparenti, sia le modifiche costituzionali o di oggetto costituzionale in materia di separazione e reciproco rapporto tra poteri dello Stato tese a indebolire il ruolo delle istituzioni e dei poteri indipendenti, quali la magistratura e la stampa. Attraverso la critica politica si persegue invece la promozione di un nuova cultura del rapporto tra sicurezza dello Stato e libertà degli individui: non più il primato delle libertà individuali la cui garanzia e tutela giustifica la loro limitazione nel pubblico ruolo dello Stato, ma il primato della sicurezza nazionale così da poter garantire, per quello che resta, un certo margine di libertà, vigilata.

I paesi autoritari ricorrono frequentemente a questi strumenti al fine di reprimere qualsiasi forma di dissenso: la particolare attenzione che i grandi totalitarismi di questo secolo pongono nell'attività di

sorveglianza e censura della rete è una delle conferme, per inverso, del ruolo fondamentale che la comunicazione attraverso questo strumento svolge in relazione all'ordine costituito. I paesi democratici fanno invece ricorso alle esigenze di sicurezza e di lotta contro la violazione delle normative in materia di diritto d'autore quali strumento di contenimento e repressione di idee e comportamenti che, benché al di fuori dell'ordinario o di forte critica al sistema, spesso rientrerebbero in una piena legittimità costituzionale.

In questa situazione, come abbiamo già visto, *Internet* ha permesso il dispiegarsi di nuove tendenze in una pluralità di direzioni, ponendosi al centro del dibattito sul rapporto tra libertà e repressione.

Nei paragrafi che seguono, si tracceranno le linee di sviluppo delle attività di sorveglianza, con particolare attenzione a quella posta in essere dalle autorità statunitensi tra la fine del secolo scorso e le attualissime rivelazioni sul Progetto PRISM, le reazioni politiche - e dunque con rilievo costituzionale - delle istituzioni europee, e infine le più rilevanti pratiche di resistenza digitale, idonee a mostrare un diverso approccio al rapporto tra libertà e sicurezza.

3.1. La rete ECHELON e il rapporto Europeo del 2000

Attualmente il fenomeno della sorveglianza globale è oggetto di una penetrante attenzione anche da una parte importante dei media tradizionali, soprattutto alla luce di un interessante mutuo rapporto sviluppatosi in particolare tra la tradizionale carta stampata e le fonti di informazione su *Internet*. Pur con tutte le distinzioni del caso, che partono dall'ovvia considerazione che la stampa cartacea, o comunque legata a testate giornalistiche con origini molto radicate nel tempo, pur

godendo di una disciplina costituzionale e legislativa più garantista della Rete, deve in ogni caso rispondere a dinamiche politico-economiche molto più pervasive di quest'ultima, è proprio la diminuzione del ruolo di guida dell'opinione pubblica e della propria capacità di influenzare la società che può aver spinto alcuni quotidiani a osare quanto il mass media per eccellenza della seconda metà del secolo scorso, la televisione, non aveva nemmeno preso in considerazione.

E così siamo oggi in grado di ripercorrere con un elevato grado di dettaglio l'evoluzione dei sistemi di sorveglianza globale forgiati e utilizzati dai paesi occidentali riconducibili al modello di Stato costituzionale nei confronti dei propri cittadini, delle proprie organizzazioni interne, dei cittadini e delle organizzazioni, governative e non, degli altri paesi, alleati compresi.

Prima di entrare nello specifico del programma PRISM, alla luce delle quotidiane rivelazioni che non cesseranno neppure nel momento in cui questo elaborato potrà dirsi concluso, valga la pena dedicare qualche paragrafo a ricordare il caso del programma ECHELON, padre e precursore di PRISM e dei suoi altri *grandi fratelli*.

ECHELON nasce dall'accorso UKUSA[6] di sicurezza che coinvolge, oltre agli Stati Uniti e al Regno Unito, l'Australia, il Canada e la Nuova Zelanda. Originariamente previsto negli anni '40 dello scorso secolo con il nome di BRUSA vi si è fatto riferimento con la locuzione "i cinque occhi", essendo in origine classificato con la classificazione "*AUS/CAN/NZ/UK/US EYES ONLY*". Il termine ECHELON, di più

[6] L'accordo UKUSA è stato firmato nel 1943 e i relativi documenti, prima secretati e poi declassificati sono ora disponibili sul sito della NSA statunitense, all'indirizzo http://www.nsa.gov/public_info/declass/ukusa.shtml (verificato il 12.05.2014).

recente conio, indica un sistema globale di intercettazione delle comunicazioni telefoniche e telematiche, private e pubbliche. Il programma viene a conoscenza del pubblico con la pubblicazione nel 2000 dello studio "*Prison Technologies. An appraisal of technologies of political control*"[7], pur anticipato in scritti precedenti, a seguito del quale saranno poi avviate indagini e inchieste anche istituzionali a livello europeo.

La rete ECHELON, sviluppata dai cinque stati firmatari dell'accordo UKUSA e utilizzata da operatori e soggetti ben oltre il confine della legalità per l'intercettazione di comunicazioni dal contenuto più vario e trasmesse con diversi mezzi, via radio, via satellite, via fibra ottica. La relazione pubblicata dal Parlamento Europeo nel luglio del 2011, "*Report on the existence of a global system for the interception of private and commercial communication (ECHELON interception system)*"[8], lascia pochi margini ai dubbi: il sistema denominato ECHELON esiste, si muove nell'ambito dell'attività dei servizi d'informazione, spionaggio e controspionaggio, ha capacità di intercettare comunicazioni trasmesse attraverso diversi tipi di supporti in particolare quelle trasmesse via satellite. Tale sistema non solo può esistere, come affermazione teorica, ma esiste, ed è incompatibile con le normative di riferimento a tutela dei diritti umani fondamentali dei

---

[7] Lo studio conclusivo, in lingua inglese, è disponibile sul sito del Parlamento Europero al seguente indirizzo http://www.europarl.europa.eu/RegData/etudes/etudes/join/2000/289666/DG-4-JOIN_ET(2000)289666_EN.pdf (verificato il 12.05.2014).

[8] Il report del 2001 è disponibile sul sito del Parlamento Europeo al seguente indirizzo http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN (verificato il 12.05.2014).

cittadini europei, in particolare quelli del diritto al rispetto della vita privata previsto dall'art. 8 della CEDU.

Sempre all'interno di questo *report* vengono inoltre affrontate due questioni rilevanti e per le quali si era già anticipata la problematicità nel rapporto tra sicurezza e altri diritti rilevanti: la prima consiste nella considerazione che un sistema di sorveglianza globale, quand'anche teoricamente elaborato ai fini di un suo utilizzo strettamente legato alle questioni di sicurezza nazionale, integrità della vita delle persone, *counter terrorism activities*, è suscettibile di essere impiegato per finalità di spionaggio industriale. La preoccupazione, più che fondata, delle Istituzioni europee si rivolgeva allo squilibrio che può derivare da un accentramento delle possibilità di controllo nelle mani di una rete di Stati che, pur essendo *partners* politico-economici indissolubili, restano pur sempre entità esterne con, tra i propri interessi, la tutela delle attività economiche delle proprie imprese. Così come una corporazione ha quale finalità quella di proteggere l'investimento dei propri azionisti, a discapito di qualsiasi altro interesse che possa presentarsi come degno di rilievo, così uno Stato ha come finalità la tutela degli interessi anche economici propri e dei propri cittadini. Un sistema di sorveglianza senza alcuna possibilità di controllo rappresenta un rischio per l'economia, la scienza e il funzionamento delle stesse Istituzioni nell'ambito delle comunità dell'Europa.

La seconda osservazione meritevole di rilievo è l'importanza che lo studio attribuisce alla necessità di stabilire pratiche di autotutela attraverso il ricorso ai sistemi crittografici. Il tema non è affrontato superficialmente ma al contrario sono tenuti presente e ben illustrati i pro e i contro, da una prospettiva istituzionale, della diffusione di un tale sistema. Sono considerati da un lato i problemi derivanti da una deliberata limitazione delle funzionalità della crittografia, tale da

limitarne o addirittura escluderne una reale efficacia, in presenza di *back doors* pronte ad essere aperte da una qualsiasi istituzione straniera che dispone delle chiavi di questa porta di *in*sicurezza, dall'altro la potenziale confliggenza della diffusione di sistemi di cifratura e crittografia con gli interessi complessivi dello Stato.

In esito a questo dettagliato studio, le conclusioni sono lapidarie. Quanto all'esistenza del sistema ECHELON, "non si può nutrire più alcun dubbio in merito all'esistenza di un sistema di intercettazione delle comunicazioni a livello mondiale, cui cooperano in proporzione gli Stati Uniti, il Regno Unito, il Canada, l'Australia e la Nuova Zelanda nel quadro del patto UKUSA. Che tale sistema o parti dello stesso abbiano avuto, almeno per un certo tempo, il nome in codice "ECHELON" può essere plausibile, alla luce degl'indizi a disposizione e delle numerose dichiarazioni concordanti provenienti da cerchie assai disparate, comprese fonti americane. Ciò che conta è che tale sistema serve non già all'intercettazione di comunicazioni militari, *ma all'ascolto di comunicazioni private e commerciali*".

Le conclusioni si estendono anche ad altre considerazioni, in merito alla possibile esistenza di altri sistemi di intercettazione e sorveglianza di una tale portata e alla supposizione che la Russia gestisca un sistema simile[9], sulla sostanziale incompatibilità della

---

[9] "Poiché l'intercettazione di comunicazioni costituisce un usuale strumento di spionaggio impiegato nell'ambito dei servizi d'informazione, anche altri Stati potrebbero gestire un simile sistema, nella misura in cui dispongano delle corrispondenti risorse finanziarie e dei presupposti geografici adeguati. In considerazione dei suoi territori d'oltremare, la Francia sarebbe l'unico Stato membro dell'Unione europea tecnicamente e geograficamente in grado di gestire da solo un sistema d'intercettazione globale. Inoltre, vi sono molti elementi che consentono di supporre che anche la Russia gestisce un sistema di questo genere."

partecipazione di uno Stato membro a un sistema come quello di ECHELON al di fuori di quanto strettamente riconducibile all'ambito dei servizi di informazione con il generale diritto dell'Unione Europea[10], e nello specifico con il diritto fondamentale alla vita privata dei cittadini europei[11].

Un dettaglio maggiore è dedicato alle risultanze dello studio in materia di spionaggio economico, alla luce delle quali "i servizi d'informazione degli Stati Uniti non si accontentano tuttavia di occuparsi di problemi economici generali", ma piuttosto "con la scusa di lottare contro tentativi di corruzione, essi intercettano anche le comunicazioni delle imprese, e ciò in particolare in sede di aggiudicazione di appalti", contesto all'interno del quale "sussiste tuttavia il rischio che le informazioni detenute vengano utilizzate a fini non già di lotta contro la corruzione ma di spionaggio della concorrenza". Nello specifico il sistema di sorveglianza ECHELON può operare in modo sistematico nell'attività di spionaggio industriale a danno delle imprese Europee. E questa affermazione, secondo il report, non è una supposizione, bensì il frutto dell'analisi di quegli specifici casi di spionaggio di cui si è venuti a conoscenza. Tra gli altri, oggetto di sorveglianza con finalità di spionaggio industriale sono stati Airfrance, Airbus, il Ministero dell'Economia Federale tedesco, Enercon e il Ministero dell'Economia giapponese, la TGV o ancora la Thyssen.

---

[10] "Per converso, se l'impiego del sistema è abusivo, quest'ultimo è in contrasto con l'obbligo di lealtà degli Stati membri e con il concetto di un mercato comune caratterizzato dalla libera concorrenza, e quindi uno Stato membro che vi partecipi agisce in violazione del diritto dell'Unione europea"

[11] "vi è ragione almeno di dubitare che il principio di proporzionalità venga rispettato e di sostenere che si è in presenza di una violazione dei principi di accessibilità del diritto e di prevedibilità del suo rispetto sanciti dalla CEDU"

Il *report* si conclude con una serie di raccomandazioni nei confronti delle Istituzioni europee e nazionali, del Consiglio d'Europa, dell'ONU e degli Stati Uniti. Nello specifico:

- al Consiglio d'Europa si rivolge l'invito a stabilire un adeguamento della tutela garantita dall'art. 8 della CEDU ai moderni metodi di comunicazione, altresì indicando agli Stati membri della stessa organizzazione di elaborare un protocollo addizionale di adesione alla CEDU stessa;
- all'Unione Europea si rivolge l'invito a elaborare un codice di condotta che garantisca la tutela dei diritti fondamentali dei cittadini europei, e a stipulare con gli Stati Uniti e i paesi terzi convenzioni che prevedano il rispetto delle reciproche normative in materia di tutela del diritto alla vita privata;
- all'ONU si rivolge l'invito di redigere una proposta di adeguamento dei testi internazionali relativi alla tutela della vita privata così come previsto dall'art. 17 della Patto internazionale sui diritti civili e politici;
- all'architettura istituzionale dell'Unione Europea si rivolge altresì, "insistentemente", l'invito a dotare i sistemi di intelligence e sicurezza informativa di strumenti che promuovano il controllo democratico, da demandarsi in ultima istanza al Parlamento Europeo.

Il documento prosegue infine con il dettaglio delle misure consigliate per promuovere le pratiche cui prima si sottolineava l'interesse, ossia l'autotutela, la lotta allo spionaggio industriale e l'applicazione dei principi fondamentali dello Stato di diritto.

L'esito di questo report fu però superato dalla Storia recente.

Presentato nel luglio del 2001 fu votato e approvato il 5 settembre del 2001. Sei giorni dopo vi fu l'attacco alle Torri Gemelle di New York, la stretta securitaria degli Stati Uniti con l'adozione del Patrioc Act e le guerre preventive. L'Unione Europea, e tutte le istituzioni degli Stati membri e terzi, con i dovuti distinguo, dovettero adeguarsi alle normative eccezionali dell'anti terrorismo internazionale, così che i diritti fondamentali dei cittadini rimasero in secondo piano molto a lungo.

3.2. Il cd. *Datagate* e il Progetto PRISM

Operando un'inversione dell'ordine cronologico motivata dalla maggior rilevanza che si ritiene di dover attribuire a quanto si ripercorrerà nel prosieguo, dai punti di vista della portata territoriale e delle potenzialità di dispiegamento concrete, è corrente interesse ripercorrere quanto è stato finora assunto alla pubblica conoscenza in merito al Progetto PRISM.

PRISM è un programma, già clandestino e ora pubblicamente noto, di sorveglianza elettronica globale e di massa, *data mining* e *signal intelligence*, promosso e condotto dagli Stati Uniti attraverso l'intercettazione delle comunicazioni che viaggiano su *Internet* e, in particolare, con l'accesso, la raccolta, la conservazione, l'elaborazione, il controllo e l'analisi dei dati a disposizione delle grandi compagnie americane fornitrici di servizi *Internet*, quali Google, Facebook, Microsoft, Yahoo e Apple, operanti nella quasi totalità degli Stati dell'intero pianeta, oltre altresì alle informazioni raccolte con la collaborazione degli operatori fornitori di servizi e di telefonia operanti sul territorio americano, in particolare la AT&T.

L'origine temporale di questa massiccia pratica di sorveglianza locale e globale si può ricondurre ai fatti del settembre del 2001. Se la citata Rete ECHELON aveva come ambito primario di operatività il territorio estero degli Stati Uniti, e se comunque specifici casi di abusi da parte delle autorità di intelligence statunitensi erano già stati ampiamente riportati dalla stampa, è almeno a quell'anno che risale la certezza di un programma di controllo globale, pervasivo e illegale. Nel settembre del 2012 J. Kierke Weibe, ex analista della *National Security Agency* statunitense, ebbe modo di affermare, sotto giuramento di fronte alla Corte distrettuale della California, che "tutto è cambiato alla NSA dopo gli attacchi dell'11 settembre. L'approccio era prima focalizzato sul rispetto del *Foreign Intelligence Surveillance Act* ("FISA"). L'approccio post-11 settembre è stato invece che la NSA poteva aggirare gli statuti federali e la Costituzione fintanto che ci fosse una qualche viscerale connessione con la caccia ai terroristi"[12]. Pochi giorni dopo, William E. Binney, altro ex analista dell'NSA, confermò dinnanzi alla medesima Corte che "le libertà sancite dalla Costituzione degli Stati Uniti non erano più una preoccupazione"[13].

Le dichiarazioni ufficiali idonee a suscitare più di un sospetto rispetto all'esistenza di programmi segreti di sorveglianza massiccia attraverso le potenzialità offerte dalle tecnologie di telecomunicazione e da *Internet* in particolare, condotti sotto l'egida della lotta al terrorismo e

---

[12] Il documento è disponibile integralmente sul sito della *Electronic Frontier Foundation*, https://www.eff.org/document/wiebe-declaration-support-plaintiffs-motion (verificato il 12.05.2014).

[13] Il documento è disponibile integralmente sul sito della *Electronic Frontier Foundation*, https://www.eff.org/document/binney-declaration-support-plaintiffs-motion (verificato il 12.05.2014).

attraverso il declassamento dei diritti e delle libertà individuali, si sono susseguite frequentemente negli anni successivi. In particolare le dichiarazioni maggiormente degne di nota furono due:

- le dichiarazioni del Presidente degli Stati Uniti George W. Bush che, nel 2005, alla luce dell'articolo pubblicato il 18 dicembre dello stesso anno, confermava le pratiche di spionaggio dell'NSA[14];
- nel 2012, in una lettera proveniente dal Direttore della National Intelligence e diretta a due Senatori, viene ammessa "almeno una violazione" dei diritti costituzionali consacrati nel Quarto Emendamento alla Costituzione Americana sotto la disciplina della *Foreign Intelligence Surveillance Act*[15].

Queste scarne dichiarazioni ufficiali sono state accompagnate da numerosi *leaks* da parte di funzionari o ex funzionari in particolare dell'NSA, come quelle già citate, ed egregiamente ripercorse dalla *Electronic Frontier Foundation* in una chiara timeline degli sviluppi giuridici e politici delle questioni relative allo spionaggio da parte della

[14] "La *National Security Agency* ha iniziato a condurre intercettazioni senza mandato sulle chiamate telefoniche e messaggi di posta elettronica tra gli Stati Uniti e Afghanistan mesi prima che il presidente Bush autorizzasse ufficialmente una versione più ampia di speciale programma di raccolta interno dell'agenzia […] il presidente Bush ha confermato l'esistenza del programma nazionale di intelligence dell'agenzia di sicurezza e lo ha difeso, dicendo che era stato strumentale nel distruggere le cellule terroristiche in America" http://www.pulitzer.org/archives/7038 (verificato il 12.05.2014).

[15] http://www.wired.com/2012/07/surveillance-spirit-law/ (verificato il 12.05.2014).

agenzie statunitensi[16].

In ogni caso, l'autorizzazione formale è stata attribuita con il *President's Surveillance Program*, adottato nel 2001 e rinnovato in più occasioni fino all'entrata in vigore delle normative legislative che si vedranno in seguito, e la cui esistenza è stata rivelata con un report del 2009[17].

Il 7 giugno 2013, a seguito delle rivelazioni dell'ex analista dell'NSA Edward Snowden, attualmente in asilo politico in Russia, pubblicate in primo luogo dal Washington Post, autorevole quotidiano conservatore americano, l'esistenza del Progetto PRISM è resa pubblica e nota, anche con la diffusione di *slides* in *power point*, classificate *top secret*, che ne riassumono in modo tanto sintetico quanto chiaro la portata. A questa diffusione seguiranno interventi di politici, funzionari, giornalisti, associazioni di difesa dei diritti civili e in particolare delle libertà digitali. È difficilmente contestabile che le reazioni suscitate nei paesi terzi verso gli Stati Uniti, *inter alias* l'Unione Europea, abbiano subito una rilevante influenza dalle rivelazioni di un progetto di sorveglianza tanto diffuso, penetrante, automatizzato e lesivo dei diritti fondamentali dei propri cittadini.

Seguendo un ordine di rilevanza, di seguito si accompagnano le diapositive diffuse da Edward Snowden in relazione alle attività di

---

[16] Lo strumento messo a disposizione da parte della Electronic Frontier Foundation è disponibile all'indirizzo: https://www.eff.org/nsa-spying/timeline (verificato il 12.05.2014).

[17] L'articolo che riferisce dell'autorizzazione da parte dell'amministrazione Obama è consultabile sul sito del quotidiano *The Guardian*, all'indirizzo http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama (verificato il 12.05.2014).

spionaggio dell'NSA, in particolare in relazione al ruolo o comunque alla posizione delle impresi fornitrici di servizi di *mail*, *social networking*, motori di ricerca e *hosting* utilizzate da centinaia di milioni di persone nel mondo intero:

1) la tipologia dei dati raccolti (fig. 5): attraverso la collaborazione dei *providers* di servizi della società dell'informazione stabiliti negli Stati Uniti, è possibile per i funzionari dell'NSA, avere accesso a *email*, video e *voice chat*, materiale audiovisivo, dati conservati dall'operatore, *Voice over Internet Protocol*, trasferimento di *files*, video conferenze, le più varie notifiche relative all'attività dei bersagli quali login, pagine visitate e tempo trascorso sulle stesse, contatti stabiliti, file scaricati, dettagli relativi alle attività di *social networking*, oltre a quanto riconducibile al concetto di "richieste speciali".

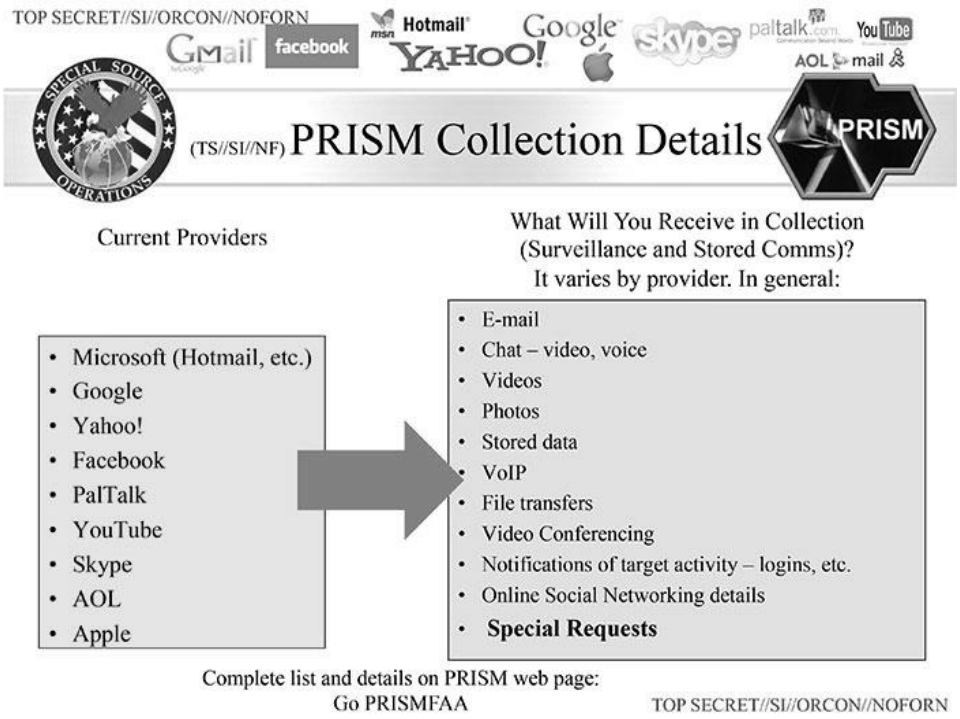

Figura 5: slide progetto PRISM: la tipologia dei dati raccolti

2) Le tempistiche di adesione dei più noti fornitori di servizi su *Internet* (fig. 6): la slide sotto indicata presenta con una schematica semplificazione la data in cui ha avuto inizio la raccolta di data sulla base di PRISM in relazione ai più noti providers di servizi di *Internet*. Microsoft sin dal 2007, Yahoo dal 2008, Google e Facebook dal 2009, Youtube dal 2010, Skype dal momento dell'acquisizione da parte di Microsoft, nel 2011, stesso anno dell'imponente AmericaOnLine, mentre Apple sarebbe diventata parte del programma "solo" nel 2012. Dalla slide in questione non risultano, però, le modalità di raccolta dei dati stessi, ossia se i dati siano consegnati dalle imprese ovvero raccolti direttamente, e se in quest'ultimo caso ciò avvenisse nella consapevolezza o meno dei *providers* stessi. Sul punto però pare dare qualche indicazione di un possibile, almeno parziale, risposta un'altra delle slides pubblicate.

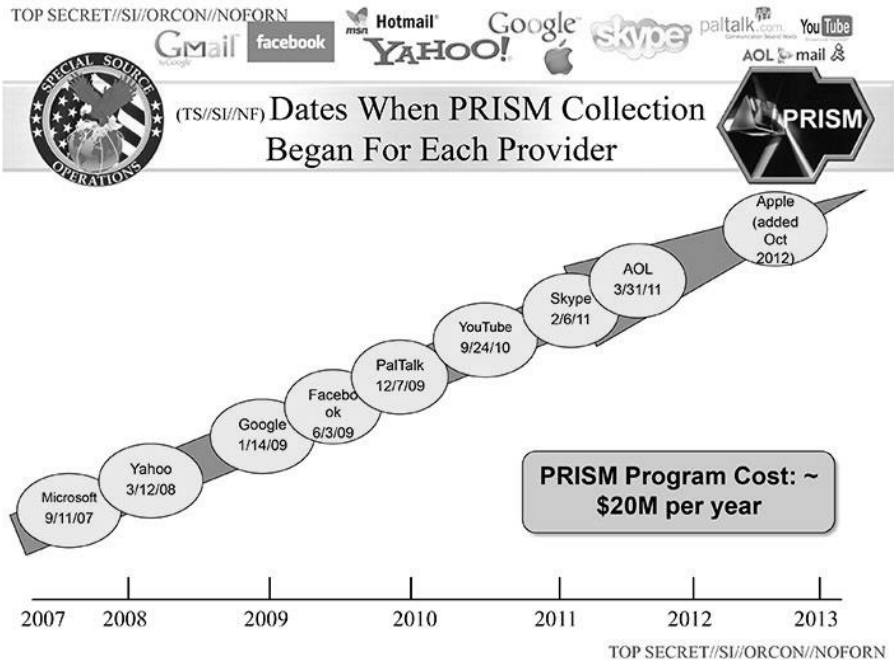

Figura 6: slide progetto PRISM: adesione dei providers a PRISM

3) Le modalità "raccomandate" per la raccolta dei dati (fig. 7): la slides sotto riprodotta indica la necessità, con la formula "you should use both", di utilizzare entrambe le tecniche di raccolta dati più efficaci e, alla luce di queste dichiarazioni, accessibili agli analista dell'NSA, ossia la raccolta diretta presso i cavi e i nodi presso i quali i dati circolano e la "raccolta diretta dai *server* dei seguenti service providers degli Stati Uniti", ove segue l'indicazione dei medesimi providers della diapositiva precedente. Quanto prospettato da questa raccomandazione suggerisce l'idea che gli agenti dell'intelligence statunitense abbiano sostanzialmente accesso a tutti i dati in transito da e per gli Stati Uniti, oltre che diretto accesso agli stessi "*server*s" dei più utilizzati e diffusi service providers del mondo.

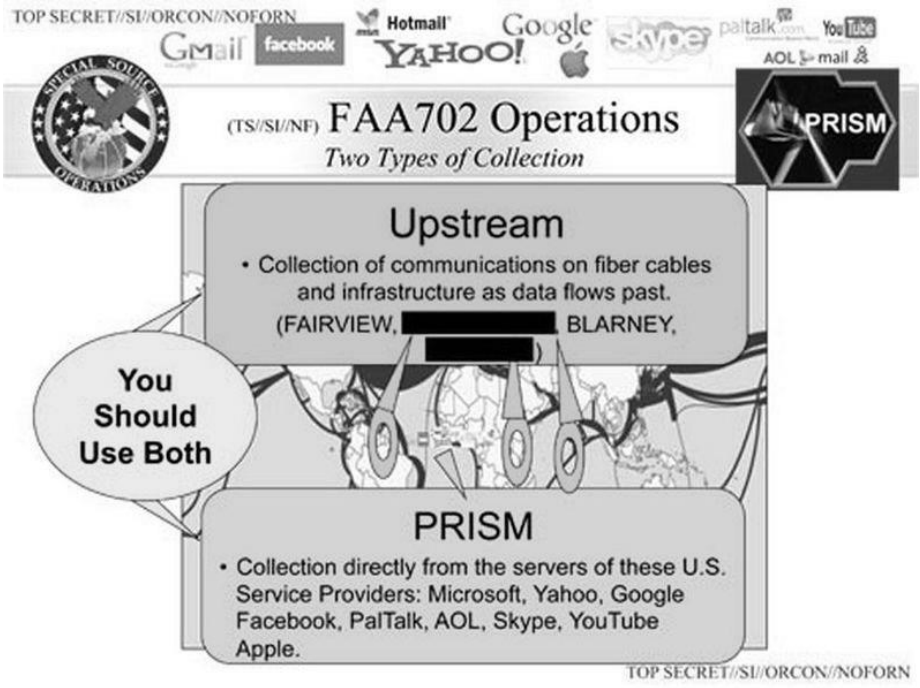

Figura 7: slide progetto PRISM: le modalità di raccolta dei dati

La classificazione dei dati raccolti (fig. 8): la slide che segue è indicativa del ruolo centrale attribuito ai service providers, come fonte immediata e fondamentale di informazioni rilevanti per attività di intelligence. Lo stesso sistema classificatorio attribuisce infatti i primi due valori, organizzati in una scala da P1 a PA, plausibilmente negli anni successivi prolungata alla luce di nuove collaborazioni a PRISM, l'identificativo della fonte, ossia del *service provider*, dal quale è stata raccolta l'informazione così classificata. Il terzo valore invece varia in funzione del tipo di contenuto raccolto. I successivi tre valori sono invece attribuiti sulla base della fonte, posto che PRISM non integra, come appena visto, il solo strumento di raccolta di informazioni di intelligence. Chiudono i dati classificativi l'anno e il numero seriale.

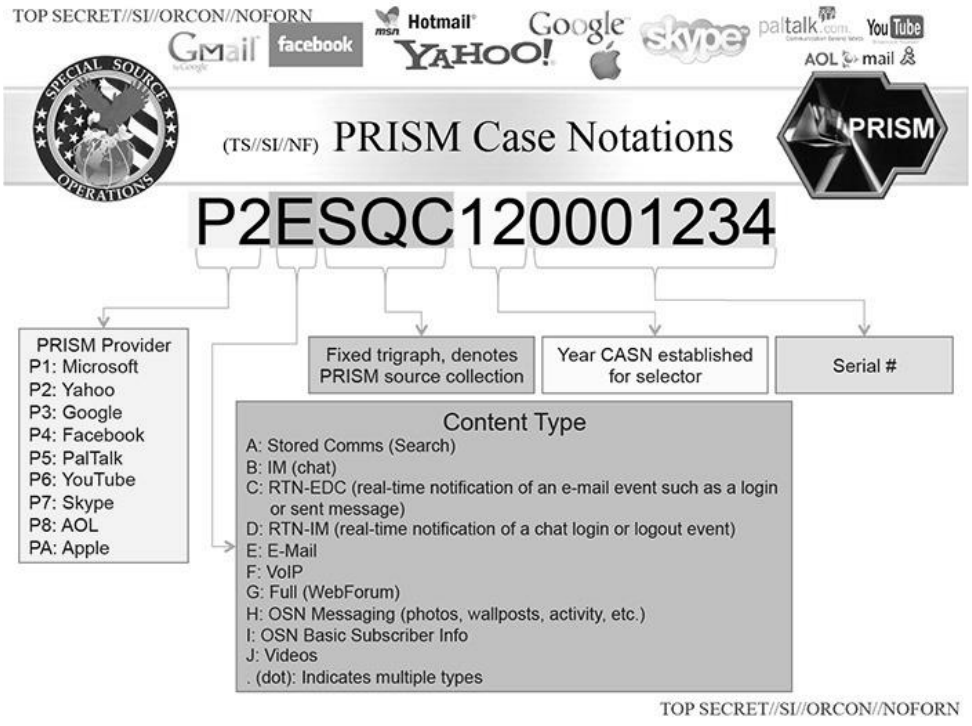

Figura 8: slide PRISM: classificazione dei casi

Altre slides e fotografie di elementi portanti di PRISM sono state rese disponibili su *Internet*, che spiegano alcuni criteri tecnici e organizzativi per il rapporto tra NSA e altre autorità nell'attribuzione delle funzioni[18], esprimono il flusso di dati così come raccolti attraverso il ricorso al sistema PRISM stesso[19] o ancora indicano i bersagli più rilevanti di uno specifico lasso temporale[20]

Tali attività, siano essere finalizzate ad operazioni di counter terrorism, di lotta alla criminalità organizzata, di prevenzione e repressione dei crimini, ovvero di profilazione dei cittadini, delle loro preferenze commerciali, sessuali, politiche, sociali e culturali, e delle loro abitudini e relazioni sociali, hanno la potenzialità di travolgere, ben più che la citata Direttiva Europea sulla Data Retention, una qualsivoglia, anche minima, concezione di *privacy* e di protezione della vita privata degli individui.

3.3. Le basi legali di PRISM

Premesso che la libertà di parola e stampa è protetta negli Stati Uniti a livello costituzionale dal Primo Emendamento e che l'*habeas*

---

[18] Slide disponibile sul sito di Wikipedia, all'indirizzo http://en.wikipedia.org/wiki/File:Prism-slide-6.jpg (verificato il 12.05.2014).

[19] Slide disponibile sul sito di Wikipedia, all'indirizzo http://en.wikipedia.org/wiki/File:Prism-slide-7.jpg (verificato il 12.05.2014).

[20] Nella slide consultabile al seguente indirizzo, risaltano Venezuela, Messico e Colombia come target privilegiati nella settimana tra il 2 e l'8 febbraio 2013: http://en.wikipedia.org/wiki/File:Prism-week-in-life-straight.png (verificato il 12.05.2014).

corpus statunitense deriva dal Quarto Emendamento, l'elaborazione del progetto PRISM, di così ampia portata, ha necessitato di un quadro normativo che anteponesse con chiarezza il principio della tutela della sicurezza nazionale ai diritti delle persone. Tale obiettivo fu, almeno parzialmente, raggiunto attraverso:

1) il *Protect America Act* del 2007[21], un emendamento al citato *Foreign Intelligence Surveillance Act* del 1978, firmato dal Presidene George W. Bush, di cui modificava sostanzialmente i seguenti elementi:

   a. sostituisce la necessità di un mandato giudiziario necessario per condurre attività di spionaggio con un sistema di controllo interno all'NSA;

   b. autorizza la sorveglianza di tutte le comunicazioni elettroniche tra cittadini americani e stranieri soggetti ad investigazioni per terrorismo, in assenza di necessità di valutazioni da parte delle corti statunitensi, fintanto che non si ritenga plausibile che il destinatario si trovi negli Stati Uniti;

   c. esclude dalla necessità di vigilanza delle Corti stabilite sotto la vigenza del FISA per la sorveglianza di qualsiasi comunicazione tra non cittadini statunitensi;

   d. esclude la necessità di essere qualificati quali agenti stranieri, prerequisito richiesto invece dal FISA, per essere sottoposti a sorveglianza;

[21] Il cui testo è disponibile in inglese al seguente indirizzo: http://www.gpo.gov/fdsys/pkg/PLAW-110publ55/html/PLAW-110publ55.htm (verificato il 12.05.2014).

2) il *Foreign Intelligence Surveillance Act Amendments Act*[22] del 2008, che estende la durata del FISA che avrebbe dovuto perdere la propria efficacia nello stesso anno, prevedendo altresì alcune specifiche limitazioni alla raccolta di informazioni relative a cittadini non statunitensi localizzati al di fuori del territorio nazionale. Ciò che però più rileva è che il *FISA Amendments Act* del 2008 autorizza per via legislativa quanto in precedenza riconducibile all'iniziativa presidenziale del *President's Surveillance Program*, riconducendo quindi alla piena legalità, almeno formale, del progetto PRISM;

3) la rinnovata estensione del *FISA Amendments Act*, la cui scadenza era prevista nel 2012, fino al dicembre del 2017.

La vigenza di queste leggi fu contestata dall'*American Civil Liberties Union*, che denunciò il *FISA Amendments Act* del 2008 il giorno stesso dell'approvazione. Il caso, *Amnesty et al. vs McConnell*[23] fu sollevato in relazione alla considerazione che la normativa violasse sia il Primo che il Quarto Emendamento, in particolare per quanto riguarda le professioni che confidano sul segreto professionale. Decaduta per inidoneità a provare le proprie ragioni, la denuncia fu invece ripresa e accolta nel 2011. La Corte Suprema, nel caso ora denominato *Amnesty et al. vs Blair*, rigettò nel 2013 la domanda dei

---

[22] http://thomas.loc.gov/cgi-bin/bdquery/z?d110:H.R.6304: (verificato il 12.05.2014).

[23] La decisione del caso *Amnesty et al. vs McConnell* è disponibile in forma integrale, in lingua inglese, sul sito dell'*American Civil Liberties Union*, all'indirizzo https://www.aclu.org/sites/default/files/pdfs/safefree/faa_complaint_20080710.pdf (verificato il 12.05.2014).

ricorrenti, stabilendo che gli stessi non avrebbero dimostrato la certezza dell'impellenza del rischio generato dalla normativa contestata, con una opinione dissenziente limitata ad aspetti procedurali..

3.4. La FISA, PRISM e il ruolo dei *service providers*

Ripercorsa brevemente i recenti elementi politici e giuridici che hanno portato alla conoscenza del programma PRISM, quanto qui rileva di interesse è valutare la posizione dei *providers* chiamati in causa da un lato esplicitamente dalla normativa FISA e successivi emendamenti, dall'altra alla luce delle rivelazioni relative alle pratiche concrete di conduzione delle attività di sorveglianza da parte dell'NSA e delle agenzie di intelligence e sicurezza statunitensi, in particolare nei confronti dei cittadini stranieri.

Se può infatti essere d'interesse dare rilievo alle dispute strettamente giuridiche relative alla legittimità delle pratiche di sorveglianza da parte di Agenzie o Autorità statunitensi nei confronti dei propri cittadini, quanto rileva in questa sede è l'assoluta mancanza di qualsivoglia forma di garanzia per i cittadini non americani. Siano essi cittadini comuni, attivisti, giornalisti, avvocati difensori dei diritti civili, politici, amministratori, uomini d'impresa, sindacalisti, medici, accademici e ricercatori o qualsiasi categoria che svolga attività che facilmente si possono qualificare come sensibili, la diffusione e la condivisione di informazioni con il ricorso a servizi messi a disposizione da provider stabiliti negli Stati Uniti rende queste stesse informazioni prive di tutela e garanzia.

Nonostante infatti le dichiarazioni ufficiali rilasciate dai providers

coinvolti e direttamente citati nelle slides e nelle continue dichiarazioni degli operatori sotto copertura o ex analisti dell'NSA, il ruolo di collaborazione dei maggiori fornitori di servizi della società dell'informazione a livello mondiale è indubbio: tale collaborazione avviene in maniera diretta, attraverso la consegna, così come in ogni Stato ove si trovino materialmente i dati, delle informazioni alle richieste anche sulla base del mero Patrioct Act, oltre che del FISA emendato, e avviene altresì in maniera indiretta, prevedendo possibilità di accesso diretto, per il tramite di PRISM, da parte delle autorità, all'ingente mole di dati personali affidati da parte degli utenti dell'intero globo.

Nella prospettiva di accumulare la maggior quantità di dati, autonomi e soprattutto posti in stretta correlazione tra loro, al fine di elaborare profili di preferenze al cui dettaglio è collegato il valore economico degli spazi pubblicitari in vendita, i fornitori di servizi, quali in primi *Google* e *Facebook*, creano e aggiornano quotidianamente le più grandi banche dati di informazioni personalissime a diretta disposizione delle autorità di sicurezza nazionale di uno specifico paese.

4. L'approccio Europeo al bilanciamento tra sicurezza e diritti

La questione della sorveglianza globale tornò da allora confinata in ristretti circoli di matrice libertaria e frequentemente anti sistema, fatta comunque la lodevole eccezione delle diverse Autorità Garanti incaricate alla protezione della privacy e riunite nel Gruppo di Lavoro ex articolo 19. Le altre Istituzioni europee seguirono invece la svolta autoritaria avviata dagli Stati Uniti. Quanto più rileva in relazione alla libertà d'espressione su *Internet*, a parere di chi scrive indissolubilmente

legata al rispetto del diritto fondamentale alla vita privata, è stata l'adozione della Direttiva 2006/24/EC[24] sulla *Data Retention*, modificativa della Direttiva 2005/58/EC. La promozione di tale normativa fece seguito al coinvolgimento anche dei Paesi europei negli attacchi sferrati dalle organizzazioni terroristiche internazionali: in particolare, i due eventi chiave furono gli attentati dell'11 marzo 2004 a Madrid e del 7 luglio 2005 a Londra.

La direttiva introduceva, tra gli elementi più noti, l'obbligo per gli Stati nazionali di prevedere l'obblighi in capo ai fornitori dei servizi di telefonia e di connessione di conservare per un periodo compreso tra i 6 mesi e i 2 anni le seguenti informazioni (art. 5):

- i dati necessari per rintracciare e identificare la fonte di una comunicazione, quali numero telefonico e nome e indirizzo dell'abbonato per la telefonia, identificativo, numero telefonico e indirizzo IP per le comunicazioni telematiche;
- i dati necessari per rintracciare e identificare il destinatario di una comunicazione, identificato tendenzialmente simile al punto precedente;
- i dati necessari per determinare la data, l'ora e la durata di una comunicazione25;

---

[24] In italiano, il testo della Direttiva è disponibile all'indirizzo http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:IT:PDF (verificato il 12.05.2014).

[25] In particolare per "l'accesso *Internet*, la posta elettronica via *Internet* e la telefonia via *Internet*, data e ora del log-in e del log-off del servizio di accesso *Internet* sulla base di un determinato fuso orario, unitamente all'indirizzo IP, dinamico o statico, assegnato dal fornitore di accesso *Internet* a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato", e

- i dati necessari per determinare il tipo di comunicazione, ossia il servizio telefonico ovvero *Internet* utilizzato;
- i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature, ossia numeri chiamati, codice IMSI e IMEI di chiamante e chiamato, e nel caso di servizi anonimi dati concernenti l'attivazione della carta e la cellula di identificazione relativa;
- i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile, quali Cell ID.

Pur nonostante la stessa direttiva, al comma 2° del medesimo articolo, affermi che "non può essere conservato alcun dato relativo al contenuto della comunicazione", la direttiva è stata duramente criticata, per la pervasività dei controlli operabili, alla luce della semplice constatazione che il combinato dei dati sopra indicati, *ex se* apparentemente innocui e nello specifico idonei a mantenere una soglia elevata di rispetto della vita privata, riassunte nell'introduzione di una lettera rivolta al Commissario per gli Affari Interni Cecilia Malmström nel giugno 2010[26], ove si afferma che "informazioni sensibili riguardanti contatti sociali, compresi quelli economici, spostamenti e vita privata (quali contatti con medici, avvocati, sindacalisti, psicologie, linee di aiuto) di 500 milioni di Europei sono collezionate nell'assenza di

altresì "data e ora del log-in e del log-off del servizio di posta elettronica su *Internet* o del servizio di telefonia via *Internet* sulla base di un determinato fuso orario".

[26] La lettera con l'indicazione dei firmatari è disponibile al seguente indirizzo: http://www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf (verificato il 12.05.2014).

qualsiasi sospetto". Secondo gli estensori della lettera, giornalisti, difensori dei diritti civili, professionisti titolari di responsabilità relative al segreto professionale, associazioni di imprese e sindacati, questa data retention delle telecomunicazioni "minaccia il segreto professionale, creando il rischio permanente di perdita di dati e abuso degli stessi, e opera da deterrente verso i cittadini dall'effettuare comunicazioni confidenziali attraverso le reti di comunicazione elettronico". Minaccia altresì "la protezione delle fonti dei giornalisti, compromettendo dunque la libertà di stampa", e "danneggia le precondizioni della nostra società aperta e democratica".

Non solo i citati soggetti rivolsero tali critiche. Giovi infatti ricordare che, la Germania vide la normativa originata dalla trasposizione all'interno del proprio ordinamento di tale direttiva cassata dalla Corte Costituzionale Federale nel 2008.

La travagliata storia di questa direttiva ha avuto una brusca fine in tempi estremamente recenti: lo scorso 8 aprile 2014, a seguito di una procedura originata in Irlanda ancora nel lontano 2006, con la decisione C293/12[27], la Corte di Giustizia dell'Unione Europea ha espunto dall'ordinamento la Direttiva sulla Data Retention, qualificata come non "compatibile nel suo complesso con l'articolo 52, paragrafo 1, della Carta, in quanto le limitazione all'esercizio dei diritti fondamentali che essa comporta, per effetto dell'obbligo di conservazione dei dati da essa imposto, non sono accompagnate dai principi irrinunciabili destinati a disciplinare le garanzie necessarie ad inquadrare l'accesso ai suddetti

[27] La decisione può essere consultata in tutte le lingue dell'Unione Europea sul sito della Corte di Giustizia all'indirizzo http://curia.europa.eu/juris/documents.jsf?num=C-293/12 (verificato il 12.05.2014).

dati e il loro uso".

È particolarmente degno di nota il percorso argomentativo, di seguito brevemente ripercorso, dell'Avvocato Generale Pedro Cruz Villalon. Dopo anni nei quali il rapporto tra gli interessi alla sicurezza dello Stato sono stati ritenuti preminenti rispetto all'insieme dei diritti individuali e collettivi fondamentali dei cittadini europei, l'Avvocato Generae richiede alla Corte di Lussemburgo di stabilire che una normativa che non mantenga il giusto equilibro sia incompatibile con l'architettura istituzionale e costituzionale dell'Unione sia cassata:

- il legislatore europeo, nell'adottare un atto che determini ingerenze dei diritti fondamentali dei cittadini degli Stati membri, non può delegare la globalità della definizione delle rispettive garanzie agli Stati, né limitarsi a richiamare in tal senso le autorità legislative e amministrative competenti, dovenso al contrario "assumersi pienamente la propria parte di responsabilità stabilendo quantomeno i principi che devono presiedere alla definizione, alla fissazione, all'applicazione e al controllo di tali garanzie"[28];
- posto che la direttiva non disciplina l'accesso o l'impiego ai dati

[28] Il punto 120 della decisione integralmente riportato indica che "Il legislatore dell'Unione, infatti, nell'adottare un atto che impone obblighi che costituiscono gravi ingerenze nei diritti fondamentali dei cittadini degli Stati membri, non può lasciare completamente a questi ultimi il compito di definire le garanzie atte a giustificarle. Esso non può contentarsi né di rinviare alle autorità legislative e/o amministrative competenti degli Stati membri chiamate, se del caso, ad adottare misure nazionali di attuazione di un tale atto il compito di definire e prevedere tali garanzie, né confidare integralmente nelle autorità giudiziarie chiamate a controllare la sua concreta applicazione. Esso deve, a meno di non privare di significato le norme di cui all'articolo 51, paragrafo 1, della Carta, assumersi pienamente la propria parte di responsabilità stabilendo quantomeno i principi che devono presiedere alla definizione, alla fissazione, all'applicazione e al controllo del rispetto di tali garanzie.

raccolti e conservati, l'Avvocato chiede se l'Unione potesse "prevedere una misura come l'obbligo di raccolta e conservazione nel tempo dei dati di cui trattasi senza contornarla, contemporaneamente, di garanzie quanto alle condizioni cui saranno subordinati l'accesso e l'impiego di tali dati, quantomeno sotto forma di principio", e ciò alla luce del fatto che "esiste infatti uno stretto legame tra la concreta configurazione dell'obbligo di raccolta e di conservazione dei dati e le condizioni in presenza delle quali questi ultimi sono, eventualmente, messi a disposizione delle autorità competenti e da esse utilizzati" (punti 121 e 122);

- in definitiva, pure condividendo le osservazioni in merito alla difficoltà di tale determinazione al tempo[29], "nulla ostava a che il legislatore dell'Unione, nel definire l'obbligo di raccolta e di conservazione dei dati, contornasse quest'ultimo di una serie di garanzie sotto forma quanto meno di principi, da sviluppare da parte degli Stati membri", cisì che fosse definita "l'esatta portata e il profilo completo dell'ingerenza che comporta un obbligo siffatto", traducendosi quindi nell'obbligo in capo al legislatore di "stabilire i principi fondamentali che dovevano guidare la definizione delle garanzie minime" (punti 124 e 125);
- nello specifico, sarebbe stato necessario un "grado di precisione superiore rispetto all'espressione «reati gravi»" utilizzata dal legislatore per la descrizione delle attività criminali idonee a giustificare la compressione dei diritti dei cittadini (126);

[29] Benché la Corte non faccia, ovviamente, riferimento esplicito al contesto politico e sociale del tempo, si sollevano dubbi in merito al fatto che la Corte si riferisca esclusivamente ai profili tecnologici.

- sarebbe altresì stato necessario limitare l'accesso al filtro o vaglio delle autorità giurisdizionali o quantomeno ad autorità amministrative indipendenti (127);
- ci si "poteva altresì attendere" l'apertura alla possibilità per gli Stati di prevedere eccezioni insuperabili, quale a titolo d'esempio dello stesso Avvocato l'ambito del segreto medico (127), la previsione di obblighi di cancellazione dei dati e di informazione del soggetto interessato dopo l'accesso (128).

Condividendo buona parte delle osservazioni dell'Avvocato Generale, la Corte è arrivata alla decisione di operare una cesura netta dell'intera Direttiva 2006/48/EC, così da indicare alle Istituzioni europee la necessità di una valutazione da condursi *ex novo* del bilanciamento degli interessi in gioco. Il percorso argomentativo della Corte, meritevole quanto quello dell'Avvocatura di essere qui riportato, è il seguente:

- l'obiettivo della Direttiva 2006/48/EC era quello di armonizzare le disposizioni degli Stati membri relative alla conservazione ("retention"), da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, di alcuni tipi di dati che vengono generati o trattati da essi, al fine di garantire che i dati siano disponibili ai fini della prevenzione, ricerca, accertamento e perseguimento di reati gravi, quali la criminalità organizzata e il terrorismo;
- tali obbligazioni sollevano questioni relative al rispetto della vita privata e le comunicazioni ai sensi dell'articolo 7 della Carta, la protezione dei dati personali, ai sensi dell'articolo 8 della Carta e il rispetto della libertà di espressione ai sensi dell'articolo 11 della Carta;

- deve altresì osservarsi che i dati che i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione devono conservare , ai sensi degli articoli 3 e 5 della direttiva 2006/24 , comprende i dati necessari per rintracciare e identificare la fonte di una comunicazione e la sua destinazione , per determinare la data , ora, la durata e il tipo di comunicazione, per determinare le attrezzature di comunicazione degli utenti, e per determinare l'ubicazione delle apparecchiature di comunicazione mobile , i dati che consistono , tra l'altro, il nome e l' indirizzo dell'abbonato o dell'utente registrato , il numero telefonico chiamante , il numero chiamato e un indirizzo IP per i servizi *Internet* . Questi dati rendono possibile , in particolare , di conoscere l'identità della persona con la quale un abbonato o l'utente registrato ha comunicato e con quali mezzi , e di individuare il momento della comunicazione , nonché il luogo dal quale la comunicazione ha avuto luogo . Essi permettono inoltre di conoscere la frequenza delle comunicazioni di dell'abbonato o dell'utente registrato a determinate persone in un determinato periodo;
- tali dati, presi nel loro insieme, possono consentire conclusioni molto precise da trarre relativa alla vita privata delle persone i cui dati sono stati conservati, come le abitudini della vita quotidiana, luoghi permanenti o temporanei di residenza, quotidiano o altri movimenti, l'attività svolte, le relazioni sociali delle persone e degli ambienti sociali frequentati da loro;

Alla luce di queste preliminari osservazioni, la Corte sottolinea quanto più rilevante in questa sede e nella prospettiva che interessa, ossia che “non è inconcepibile che la conservazione dei dati in questione potrebbe avere un effetto sull'uso, da parte degli abbonati o degli utenti

registrati, dei mezzi di comunicazione contemplati da tale direttiva e, di conseguenza, il loro esercizio della libertà di espressione garantito dall'articolo 11 della Carta".

Il sistema di retention dei dati, in particolare i tipi di dati, le modalità di raccolta, le tempistiche e le modalità di conservazione, quand'anche infatti finalizzate a intenti meritevoli di tutela, possono gravemente incidere dunque sull'esercizio della libertà di espressione, valore e diritto fondamentale garantito dal patrimonio costituzionale comune europeo e dei singoli Stati membri.

E, continua la Corte, non solo il diritto alla libertà di espressione ne risulterebbe in questo modo leso nel suo nucleo fondamentale, ma altresì tutta la disciplina delineata è ben suscettibile di essere valutata alla luce del diritto alla protezione della vita privata sancito dall'art. 8 della Carta dei diritti dell'Unione Europea. Richiamando i criteri di valutazione fissati dall'art. 52 della Carta stessa, la Corte valuta quindi la compatibilità delle limitazioni introdotte dalla direttiva alla luce dei principi di legalità, proporzionalità e necessità a tutelare obiettivi di interesse generale o diritti e libertà di altri. A questo specifico riguardo:

- il *principio di legalità* è ritenuto pacificamente rispettato, posto il termine di riferimento da una normativa legittimamente adottata dagli organi competenti all'interno del riquadro di suddivisione delle competenze tra Istituzioni europee e nazionali;

- il *principio di necessità* e rispondenza a esigenza di tutela è altresì ritenuto rispettato, posto che l'utilizzo delle comunicazioni elettroniche è "un valido strumento nella prevenzione dei reati e la lotta contro la criminalità, in particolare la criminalità organizzata";

Restava quindi da valutare il rispetto del *principio di proporzionalità* alla luce dell'ingerenza così rilevante. È indubbiamente

il punto più rilevante, che investe tutta la tematica dell'elaborazione e dell'individuazione, al momento di operare un bilanciamento tra diritti e interessi contrapposti, quali l'interesse alla tutela della sicurezza e i diritti alla protezione della vita privata e alla libertà di espressione. Sul punto, la Corte argomenta come segue:

- posta l'assoluta rilevanza del diritto alla protezione della vita privata e dunque al controllo della circolazione dei propri dati personali, la normativa UE in questione deve fissare norme chiare e precise che disciplinano la portata e l'applicazione della misura in questione e imporre garanzie minime in modo che le persone i cui dati sono stati mantenuti avere garanzie sufficienti per proteggere efficacemente i dati personali contro il rischio di abuso e contro ogni accesso illegale e l'utilizzo di tali dati;

In questa prospettiva la Corte delinea dunque gli aspetti che travalicano i limiti imposti all'attività legislativa dell'Unione:

- la Direttiva si applicava infatti a tutte le comunicazioni svolte attraverso qualsiasi mezzo sul territorio europeo: telefonia fissa, mobile, *Internet*, email. L'interferenza nelle libertà fondamentali tocca dunque l'intera, o quasi, popolazione europea;
- la Direttiva si applicava infatti a tutte le comunicazioni a prescindere dalle persone coinvolte, dai contenuti delle comunicazioni stesse e in assenza di alcuna differenziazione, limitazione o esclusione stati fatti alla luce dell'obiettivo della lotta contro le forme gravi di criminalità, dunque si applica anche a persone per le quali non vi sono prove in grado di suggerire che il loro comportamento potrebbe avere un collegamento, anche indiretto o remoto, con la grande criminalità. Inoltre, esso non prevede alcuna eccezione, con la conseguenza che si applica anche

alle persone le cui comunicazioni sono soggetti, in base alle norme di diritto nazionale, l'obbligo del segreto professionale;

- inoltre, pur cercando di contribuire alla lotta contro le forme gravi di criminalità, la direttiva 2006/24 non richiedeva alcuna relazione tra i dati la cui conservazione è prevista e una minaccia alla sicurezza pubblica e, in particolare, non si limita a una ritenuta in relazione (i) di dati relativi ad un determinato periodo di tempo e / o una particolare zona geografica e / o ad un cerchio di particolari persone che possono essere coinvolte, in un modo o nell'altro, in un reato grave, o (ii) a persone che potrebbe, per altri motivi, contribuire, dalla conservazione dei propri dati, alla prevenzione, accertamento e perseguimento di reati gravi;
- ancora, non solo c'è una generale assenza di limiti nella direttiva 2006/24, ma la direttiva 2006/24, non fissava alcun criterio oggettivo in base al quale determinare i limiti di accesso delle autorità nazionali competenti ai dati e la loro successiva utilizzazione;
- in materia principi per l'accesso ai dati, la Direttiva non conteneva le condizioni sostanziali e procedurali in materia di accesso delle autorità nazionali competenti ai dati ed al loro successivo utilizzo, e in particolare:
    - non prevedeva alcun criterio oggettivo per cui il numero delle persone autorizzate ad accedere e poi utilizzare i dati conservati è limitata a quanto strettamente necessario alla luce dell'obiettivo perseguito;
    - l'accesso da parte delle autorità nazionali competenti ai dati conservati non veniva fatto dipendere da un esame preliminare effettuata da un tribunale o da un organo amministrativo

indipendente, la cui decisione mira a limitare l'accesso ai dati e il loro utilizzo a quanto è strettamente necessario al fine di raggiungere l'obiettivo perseguito e che interviene a seguito di una richiesta motivata di tali autorità presentate nel quadro delle procedure di prevenzione, accertamento o procedimenti penali;

- né era infine previsto un obbligo specifico per gli Stati membri volto a stabilire tali limiti;
- quanto alla durata della conservazione, la Direttiva richiedeva che tali dati fossero conservati per un periodo di almeno sei mesi, senza alcuna distinzione tra le categorie di dati di cui all'articolo 5 della stessa direttiva, sulla base della loro eventuale utilità ai fini dello scopo perseguito o secondo le persone interessate. La stessa forbice tra 6 e 24 mesi non era accompagnata da idonea previsione che la determinazione del periodo di conservazione dovesse essere basata su criteri oggettivi per garantire che fosse limitata a quanto strettamente necessario;

Tutto ciò osservato, ne deriva che la Direttiva 2006/24/EC non prevedeva regole chiare e precise per il governo dell'interferenza con i diritti fondamentali consacrati negli artt. 7 e 8 della Carta, dunque comportando un'ingerenza ampia e particolarmente grave di tali diritti fondamentali nell'ordinamento giuridico dell'Unione europea, senza che tale ingerenza fosse circoscritta proprio da disposizioni atte a garantire che essa venisse effettivamente limitata a quanto strettamente necessario.

Altrettanto non erano previste garanzie di protezione dal rischio di abusi e contro qualsiasi accesso ai dati e loro conseguente utilizzo illegale. E questo derivava tanto da un'assenza di previsioni a livello

della stessa normativa comunitaria quanto dell'assenza di specifiche obbligazioni a carico degli Stati membri per rispondere alle specificità della materia derivanti da "(i) la grande quantità di dati la cui conservazione è richiesta da tale direttiva, (ii) la natura sensibile di tali dati e (iii) il rischio di accesso non autorizzato a tali dati, le regole che servirebbero, in particolare, per disciplinare la tutela e la sicurezza dei dati in questione in modo chiaro e rigoroso, al fine di garantire la loro piena integrità e la riservatezza".

Dunque, conclude la Corte, con l'adozione della Direttiva 2006/24/EC il legislatore europeo ha ecceduto i limiti fissati dal principio di proporzionalità, alla luce dunque degli artt. 7, 8 e 52 della Carta, rendendosi altresì superflua la valutazione alla luce dell'art. 11 della Casta stessa, così che la Direttiva deve ritenersi invalida.

Sul fatto che questa decisione, indubbiamente influenzata dalle rivelazioni relative all'accesso da parte dei servizi di sicurezza statunitensi alla totalità dei dati conservati dagli operatori nel settore delle tecnologie di telecomunicazione di cui si dirà a breve, possa avere effetti nell'immediato delle pratiche diffuse da parte dei servizi di intelligence, dei servizi di polizia e in particolare dei soggetti privati interessati a una normativa quadro che gli permetta di acquisire e conservare tutta una serie di informazioni il cui valore economico è lapalissiano sostenere, possono essere nutriti alcuni dubbi. Indubbio è invece il merito di un intervento giurisprudenziale che, con nettezza e cristallinità dei principi stabiliti, potrà indubbiamente fungere da punto di riferimento per l'evoluzione del rapporto tra interessi securitari e diritti fondamentali dei cittadini nell'intera Unione Europea.

4.1. (*segue*): la reazione alle rivelazioni sul Progetto PRISM

Non vale la pena soffermarsi a questo punto su quanto disciplinato dalla Decisione della Commissione Europea 2000/520/EC[30], il cosiddetto *Safe Harbor Agreement*, ossia la decisione che delinea sette principi cardine della Direttiva Europea sulla protezione dei dati personali che permette l'adesione di Stati o imprese ai criteri europei in materia così da poter superare i vincoli posti dalla stessa direttiva al trasferimento di dati all'estero[31]. Tale modello, ispirato a principi anche corretti e idonei a rappresentare un equilibrato punto di incontro tra le esigenze primarie fissate in materia di protezione del diritto al controllo sui propri dati personali e le esigenze per lo più economiche dettate dall'evoluzione delle tecnologie di telecomunicazione, è oggi indubbiamente datato e oramai del tutto inidoneo a rispondere alle esigenze per le quali era stato elaborato. Un progetto di relazione dell'8 gennaio 2014[32], elaborato proprio a partire dalle rivelazioni sul programma di sorveglianza e controllo delle agenzie di sicurezza e intelligence statunitensi da parte della Commissione per le libertà civili,

---

[30] Il testo del cd. *Safe Harbor Agreement*, che disciplina modalità per semplificare la trasmissione dei dati riguardanti cittadini europei al di fuori dei confini dell'Unione, è disponibile sul sito dell'Unione, all'indirizzo http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML (verificato il 12.05.2014).

[31] Su tale decisione ha avuto anche modo di esprimersi il nostro Garante per la protezione dei dati personali con l'autorizzazione del 10 ottobre 2001, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/30939 (verificato il 12.05.2014).

[32] La relazione in lingua italiana è disponibile sul sito del Parlamento all'indirizzo http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/1014/1014703/1014703it.pdf (verificato il 12.05.2014).

la giustizia e gli affari interni, mostra il più recente approccio delle Istituzioni europee alla questione, attraverso la richiesta di:

- sospendere l'accordo di approdo sicuro fino a che una completa revisione non sia stata condotta e le lacune attuali siano state sanate, facendo in modo che i trasferimenti di dati personali per fini commerciali da parte dell'Unione agli Stati Uniti possano avvenire solo in conformità con gli standard più elevati dell'UE; e altresì
- sospendere l'accordo TFTP[33] fino i) alla conclusione dei negoziati per un accordo quadro; ii) alla conclusione di un'approfondita indagine sulla base di un'analisi dell'UE, e fino a che tutti i timori sollevati dal Parlamento nella sua risoluzione del 23 ottobre non siano stati adeguatamente affrontati.

Queste due proposte di azione così netta e radicale, si pensi anche al solo effetto simbolico di voler sospendere un accordo finalizzato, almeno formalmente, alla lotta contro il finanziamento del terrorismo internazionale, sono finalizzate a una più che condivisibile intenzione, che richiama il complesso di osservazioni giuridiche e politiche evidenziate nel complesso di questo elaborato:

- proteggere lo Stato di diritto e i diritti fondamentali dei cittadini dell'UE, con un'attenzione particolare alle minacce alla libertà di stampa e al segreto professionale (comprese le relazioni tra avvocato e cliente), nonché a una migliore protezione per gli informatori.

---

[33] Il *Terrorist Finance Tracking Programme*, finalizzato alla collaborazione in campo di individuazione dei canali di finanziamento suppostamente indirizzati alle operazioni di terrorismo internazionale.

È infatti lo Stato di diritto, lo Stato costituzionale di cui l'Europa e gli Stati nazionali europei hanno costantemente rivendicato la supremazia e la preminenza, che viene complessivamente messo in disparte da pratiche unilaterali di limitazione dei diritti fondamentali, in particolar modo i diritti strettamente connessi alla libertà di espressione e alla protezione dei propri dati personali.

5. La resistenza digitale

Il lato della medaglia della centralità della tecnologia nel rapporto conflittuale tra diritti individuali e sociali e interessi di Stati e corporazioni contrapposto alle pratiche e possibilità di sorveglianza globale è rappresentato invece dalla "concreta possibilità di utilizzare tutti i diversi tipi di tecnologie disponibili all'umanità per gli scopi specifici di creare reti, contribuire ai cambi sociali e politici e contrastare le dittature oppressive, e anche l'autorità in generale"[34].

Oggetto di questa ultima parte del presente elaborato sarà dunque di osservare tale aspetto, partendo dalla definizione di *hacker* e dall'incontro con l'attivismo sociale e politico, passando dunque per le finalità sociali del movimento per le *Liberation Technologies*, per

[34] ZICCARDI G., *Resistance, Liberation Technology and Human Rights in the Digital Age*, *Law, Governance and Technology Series* 7, Springer, Netherlands, 2013, p. 1, "*the concrete possibilità of using all the various types of technologies available to mankind for the specific purpose of networking, of contributing to political and social changes and of contrasting oppressive dictatorships, and even authority in general*".

arrivare infine a descrivere alcune delle più rilevanti tecniche e strategie di autotutela.

5.1. *Hacker* e attivismo sociale e politico

Al fine di chiarire il referente delle terminologie utilizzate, si intende utilizzare il termine *Hacker* nel senso originario e non dispregiativo della parola, ossia ci si riferisce alle persone dotate di particolarmente elevate *competenze tecniche* nell'utilizzo dei *computer*, orientate al ricorso alle possibilità poste a disposizione dalle nuove tecnologie con spirito di curiosità e *creatività*. Sono dunque caratteristiche, se non del tutto pacificamente positive, come sarebbe a parere di chi scrive, almeno neutrali nei confronti delle diverse scale di valori che possano essere proposte. In ogni caso, questo chiarimento è necessario alla luce dell'abuso del termine che per almeno due decenni, nella cultura mainstream e istituzionale, è stato equiparato alla locuzione di *criminale informatico*.

La parola ha infatti origine nel contesto universitario del MIT tra gli anni '50 e '60, era associata alle suddette caratteristiche, e solo nella metà degli anni '80 divenne parte della cultura di massa l'associazione mentale ed etimologica con le intenzioni distruttive.

Dalla versione originale del Jargon file[35], un dizionario dei

[35] La versione originale di Rafael Finkel può essere consultata all'indirizzo http://www.dourish.com/goodies/jargon.html (verificato il 12.05.2014); la versione odierna è consultabile all'indirizzo http://www.catb.org/jargon/html/index.html (verificato il 12.05.2014).

significati delle parole utilizzate dalle persone operanti nel settore delle nuove tecnologie, o, come autodefinita la versione contemporanea "un compendio completo del gergo degli *hacker* che illumina molti aspetti della tradizione, del folklore e dell'umorismo *hacker*", la stessa parola *hacker* viene così definita:

[originally, someone who makes furniture with an axe] n. 1. A person who enjoys learning the details of programming systems and how to stretch their capabilities, as opposed to most users who prefer to learn only the minimum necessary. 2. One who programs enthusiastically, or who enjoys programming rather than just theorizing about programming. 3. A person capable of appreciating hack value (q.v.). 4. A person who is good at programming quickly. Not everything a hacker produces is a hack. 5. An expert at a particular program, or one who frequently does work using it or on it; example: "A SAIL hacker". (Definitions 1 to 5 are correlated, and people who fit them congregate.) 6. A malicious or inquisitive meddler who tries to discover information by poking around. Hence "password hacker", "network hacker".

Più recentemente, ed è di interesse riportare che ancora oggi sia così, sulle porte del MIT sono affisse le 11 regole dell'*etica hacker*. Ispirandosi infatti a una curiosità e creatività che, come si dirà più avanti, necessariamente traballa sul confine della legalità formale e necessariamente si pone in contrasto con le autorità costituite e il sistema di normazione positivista, non sono le leggi, le Costituzioni o le prassi istituzionali a regolare la vita degli *hacker*, bensì propositi etici caratterizzati dunque da maggior flessibilità e adattabilità:

1. *Be safe. Your safety, the safety of your fellow jackers, and the safety of anyone you hack should never be compromised.*
2. *Be subtle. Leave no evidence that you were ever there.*
3. *Leave things as you found them (or better).*
4. *If you find something broken, call F-IXIT (the local number for reporting problems wit the buildings and grounds). Hackers often go places that institute workers do not frequent regularly and may see problems before anyone else.*
5. *Leave no damage.*
6. *Do not steal anything.*
7. *Brute force is the last resort of the incompetent. ("One who breaks a thing to find out what it is has left the path of reason." - John Ronald Reuel Tolkien, "The Lord of the Rings")*
8. *Do not hack while under the influence of alcohol/drugs/etc.*
9. *Do not drop things (off a building) without ground crew.*
10. *Do not hack alone (just like swimming).*
11. *Above all, exercise common sense.*

La versione del Jargon file contemporanea è più sintetica, pur completa nei suoi punti essenziali, quanto agli aspetti etici[36]. I due riferimenti etici, a cui gli *hacker* dovrebbero, per chiamarsi tali, ispirare le proprie condotte, sono i seguenti:

[36] La pagina relativa all'etica *hacker* è disponibile all'indirizzo, in lingua inglese, http://www.catb.org/jargon/html/H/*hacker*-ethic.html

1. La convinzione che la condivisione delle informazioni è un potente bene positivo, e che è un dovere etico di *hacker* per condividere la loro esperienza scrivendo codice open-source e facilitare l'accesso alle informazioni e alle risorse di calcolo, ove possibile.
2. La convinzione che sistema di cracking per il divertimento e l'esplorazione è eticamente OK finché il *cracker* non commette furti, atti di vandalismo, o violazione della riservatezza.

L'eterogeneità del mondo *hacker* si ritrova anche nelle osservazioni a questi due riportati principi. Infatti "entrambi questi principi etici sono largamente, ma non per questo universalmente, accettati tra gli *hacker*. La maggior parte degli *hacker* sottoscrivono l'etica *hacker* nel senso 1, e molti agiscono sulla base di esso, scrivendo e distribuendo *software open-source*", mentre "alcuni vanno oltre e sostengono che tutte le informazioni dovrebbero essere liberi e di qualsiasi controllo proprietario di essa è male; questa è la filosofia alla base del progetto GNU". E così anche il secondo punto è sottoposto a diversi punti di vista[37].

È invece di recente conio, comparato all'origine del secolo scorso del termine *hacker*, il termine *hacktivist*. Se infatti l'*hacker* è spinto da curiosità e creatività e fonda la propria azione sulla convinzione dell'utilità sociale della ricerca e della condivisione delle informazioni,

[37] "alcune persone considerano l'atto di rottura si sia immorale, come effrazione. Ma la convinzione che 'etica' di *cracking* non comprende la distruzione almeno modera il comportamento delle persone che si vedono come cracker "benigni" [...]. Su questo punto di vista, potrebbe essere una delle più alte forme di cortesia *hacker*istica a (a) penetrare in un sistema, e quindi (b) spiegare al sysop, preferibilmente via e-mail da un account di superutente, esattamente cosa è stato fatto e come il buco possa essere chiuso".

della trasparenza dei sistemi informatici e può dunque perseguire, anche solo in via indiretta, obiettivi e finalità politiche e sociali, l'*hacktivist* fa di quest'ultime il baricentro della propria azione: *hacktivist* è un *hacker* che orienta le proprie competenze, i propri interessi, e declina i propri principi etici, al servizio di battaglie e campagne con risvolti fortemente politici e sociali.

Con la diffusione delle nuove tecnologie, e la stretta relazione tra le possibilità rese disponibili dalle stesse e le necessità di comunicazione delle lotte politiche e sociali contemporanee, la crasi tra la parola *hacker* e la parola attivista è rappresentazione di un rapporto ben più profondo di quanto non possa apparire.

La motivazione più rilevante che spingeva gli *hacker* ad agire in quanto tali era quella di accedere alla conoscenza e diffonderla, con curiosità, affinché la stessa, in particolare quella relativa ai sistemi informatici che, con buona dose di capacità di previsione dell'evoluzione futura, si sapeva sarebbero diventati elemento centrale nella vita quotidiana dell'umanità.

Sullo stesso binario le contemporanee lotte sociali e politiche che, pur diversificate ed eterogenee nei fini, nei mezzi, nei richiami ideologici o negli specifici ideali perseguiti, si fondano o si basano sulla necessità di cercare, ottenere e diffondere le informazioni relative alle questioni affrontate. Così le campagne ambientaliste cercano e richiedono l'accesso alle informazioni relative alle attività inquinanti, allo stato dell'aria, dell'acqua e dei suoli, e promuovono lo sviluppo di comportamenti e sensibilità sul tema attraverso la loro diffusione. Simile percorso seguono le campagne sociali, rivendicando trasparenza e responsabilità dei sistemi economici e istituzionali, raccolgono denunce, segnalazioni, studi, ne promuovono la diffusione e l'interrelazione, così da stimolare il raggiungimento degli obiettivi prefissati.

In un mondo nel quale le informazioni sono conservate in formato digitale all'interno di *server* dislocati nei diversi angoli del globo e la comunicazione tra persone, quand'anche vicine tra loro, si svolge prevalentemente attraverso le tecnologie dell'informazione e della comunicazione, l'acquisizione della consapevolezza che la promozione e la diffusione di idee innovative, rivoluzionarie e comunque alternative alle verità vigenti sarebbe dovuta passare da una piena consapevolezza dei meccanismi di funzionamento degli strumenti utilizzati ha portato all'incontro, più che proficuo, tra i principi e la tradizione *hacker* e le necessità degli attivisti dell'intero globo.

Dunque oggi si intersecano strettamente le azioni compiute dagli *hacker* per le finalità più originarie e tradizionali, quali l'apertura del codice sorgente dei sistemi operativi e dei programmi di uso comune, le prove di resistenza dei sistemi informatici relativi a servizi pubblici e privati e infrastrutture critiche, la curiosità nella scoperta dei meccanismi implementati dai responsabili di sicurezza, e le azioni di rivendicazione sociale e politica.

Sul punto, è illuminante l'idea che vi siano elementi di vicinanza tra le azioni di picchettaggio, consistenti nel blocco, totale o solo persuasivo, dell'accesso ai posti di lavoro da parte degli scioperanti al fine di impedire o anche solo di convincere colleghi e/o utenti a partecipare alla protesta, o quantomeno di accedere alle motivazioni della stessa tramite la distribuzione di volantini e opuscoli informativi, alle azioni di tipo DDoS (*Distributed Denial of Service*) nei confronti di siti istituzionali di governi, organi di polizia o giustizia, imprese private o ancora siti personali di personaggi pubblici, che esauriscono le risorse degli stessi impedendovi dunque l'accesso, e prevedendo altresì in certi casi la visione di pagine informative sulle motivazioni dell'azione posta in essere.

E ancora, non è un caso che un servizio quale quello di Wikileaks, finalizzato alla raccolta e alla diffusione di informazioni coperte da segreto di Stato o militare, abbia ricevuto e riceva tutt'ora un così ampio sostegno da parte delle organizzazioni nazionali e internazionali pacifiste, che vedono nello strumento, in poche parole un sito che fornisca la possibilità agli insiders di un certo sistema di diffondere le informazioni detenute con un elevato grado di anonimato, dunque strumento neutro quanto al contenuto, una fondamentale risorsa per la conduzione delle proprie campagne contro la risoluzione dei conflitti internazionali per il mezzo dell'uso degli strumenti militari.

Alla luce di questa prospettiva è andata dunque maturando e radicandosi una convinzione: gli strumenti giuridici più all'avanguardia messi a disposizione dagli Stati costituzionali da soli poco o nulla possono contro la segretezza con cui gli strumenti informatici possono offuscare l'informazione e la conoscenza. La necessità di affiancare alle lotte per la riaffermazione della preminenza del diritto, quale strumento di regolazione sociale rispetto all'economia, e alla forza bruta procedure di apertura dei sistemi di comunicazione ha generato l'*hacktivist* del nuovo millennio: informato, curioso, animato da spirito di partecipazione e voglia di cambiamento, disilluso dagli strumenti di mediazione politica tradizionale e consapevole della tendenza intrinseca di imprese e Stati alla menzogna, all'edulcorazione e all'occultamento.

5.2. *Hacktivist* e *Liberation Technologies*

L'*hacktivist* trova dunque nell'immateriale realtà del digitale un terreno fertile per le diverse fasi delle proprie campagne. In una stretta

relazione tra materiale e digitale, nutre la propria conoscenza e coltiva le proprie attività in un rapporto di interscambio bilaterale tra l'uno e l'altro mondo, così finalmente, dopo anni di infondate contrapposizioni, destinati a essere pienamente considerati come una realtà unitaria, ove ciò che li distingue sono le peculiari regole infrastrutturali che ne determinano il funzionamento. Così l'*hacktivist*:

1) *nasce nel mondo reale, diventa adulto con la rete*: già prima ancora di sentirsi attivista a favore di una certa rivendicazione, è attraverso *Internet* che spesso vengono scoperte ragioni, motivi o colpe di realtà che ci circondano e sono percepite come ingiuste. La povertà e l'ingiustizia sociale, l'inquinamento e le malattie, l'impunità dei potenti e dei ricchi, le guerre e la discriminazione, l'asservimento delle scienze agli interessi economici, sono tutte realtà percepite con i sensi e approfondite attraverso la ricerca dell'informazione attraverso le reti;

2) *affina, promuove, diffonde e condivide le proprie conoscenze, tra reale e digitale*: una volta fatta propria una certa idea e ritenuta la stessa meritevole di investimento della propria persona e del proprio tempo, gli strumenti di comunicazione permettono di entrare in contatto con altri soggetti interessati e così si sviluppa un circolo, possibilmente virtuoso, di scambi e condivisione di informazione, generando maggior consapevolezza e preparazione sulle campagne di proprio interesse. Se le tecnologie sono fondamentali per conoscere e raggiungere casi analoghi distanti nello spazio e nel tempo, è più unico che raro il caso in cui l'attività sia compiuta

esclusivamente nel mondo digitale: l'*hacktivist* lotta nella rete e nelle piazze;

3) *scardina i meccanismi di oscurità e segretezza delle istituzioni, tutela la riservatezza e la libertà di espressione*: con la consapevolezza del ruolo chiave che le tecnologie di comunicazione svolgono nelle dinamiche politiche e sociali, l'*hacktivist* impara e cerca di diffondere le modalità di funzionamento delle tecnologie stesse, le potenzialità e soprattutto i limiti, l'utilità e soprattutto i rischi. Come si avrà modo di affrontare in sede di conclusioni, l'*hacktivist* ha chiaro il conflitto tra riservatezza e libertà di espressione, l'esistenza di un ineludibile incoerenza di fondo che obbliga a rivendicare trasparenza e libertà promuovendo contestualmente riservatezza e anonimato.

Non è dunque con un superficiale utilizzo delle tecnologie di comunicazione che sono poste in essere campagne efficaci e idonee a raggiungere i propri obiettivi, minimizzando i rischi per le persone coinvolte e massimizzando i risultati. Il funzionamento dell'infrastruttura informatica dev'essere conosciuto così da poter utilizzare coscientemente gli strumenti che garantiscano la più elevata probabilità di sfuggire alle dinamiche di sorveglianza e controllo che sono invece strutturalmente proprie dello strumento al quale l'*hacktivist* ha deciso di fare ricorso.

È in questo contesto che nasce il termine di *Liberation Technologies*, coniato da Larry Diamond[38] e elemento centrale del

[38] DIAMOND L., *Liberation Technology*, *Journal of Democracy*, 2010, Vol. 21 no. 3, pp. 69-83, http://iis-

Programma sulle *Liberation Technologies* dell'Università di Stanford[39]. Quest'ultimo, esattamente nell'ottica dell'incontro tra cultura *hacker* e attivismo politico e sociale, condotto in un contesto universitario, "cerca di capire come la tecnologia dell'informazione può essere utilizzata per difendere i diritti umani, migliorare la governance, potenziare i poveri, promuovere lo sviluppo economico, e perseguire una varietà di altri beni sociali". Ancora, "posizionato sul punto di incontro tra scienze sociali, informatica e ingegneria, il Programma sulle *Liberation Technologies* cerca di capire come - e in che misura – le varie tecnologie dell'informazione e le loro applicazioni - tra cui telefoni cellulari, messaggi di testo (SMS), *Internet*, blog , GPS, e altre forme di tecnologia digitale - consentano ai cittadini di promuovere la libertà, lo sviluppo, la giustizia sociale e lo Stato di diritto". Puntualmente questo progetto individua la correlazione tra lo sviluppo e la diffusione alla globalità delle persone delle tecnologie dell'informazione e le possibilità di perseguimento di quella pluralità di beni politici e sociali – la difesa dei diritti umani, la trasparenza delle attività economiche e di governo, la riduzione del divario sociale e dell'ingiustizia sociale tra classi e tra Stati – che sono stati la chimera del ventesimo secolo, solo in parte raggiunti e oggi tanto messi in discussione. Le *Liberation Technologies* possono essere distinte in due ordini di tecnologie: quelle finalizzate a conoscere

db.stanford.edu/pubs/22952/JoD_July2010_Diamond.pdf (verificato il 12.05.2014) e DIAMOND L., PLATTER M., *Liberation Technology: Social Media and the Struggle for Democracy*, *The Johns Hopkins University Press*, p. 208, 2012 .

[39] E in relazione al quale non può sfuggire un richiamo alla Teologia della Liberazione, movimento della Chiesa Cattolica nato nella seconda metà del secolo scorso e sviluppatosi sotto le dittature sudamericane con la prospettiva di porre la Chiesa stessa al servizio dei poveri e dei diseredati, prendendo esplicitamente parte ai gravi conflitti sociali che attraversavano il continente.

e testimoniare, e quelle invece dirette a proteggere e nascondere.

1) *per conoscere e testimoniare*; tra le prime risaltano i progetti sociali e informatici, costruiti su scala locale, nazionale o internazionale, generalmente a partire da specifici eventi traumatici che hanno generato il senso di necessità di qualcosa di nuovo per evitarne o prevenirne il ripetersi. Rientrano in questa categoria tutti i progetti diretti a favorire la condivisione dell'esperienza diretta, il *citizen journalism*, l'accesso all'informazione, la diffusione di *leaks* riservati, la promozione dell'apertura del codice sorgente nei sistemi informatici pubblici e privati;

2) *per proteggere e nascondere*; tra queste seconde invece rientrano tutte quelle tecnologie abilitanti la protezione di identità, dati, informazioni, persone, sottoposte a limitazioni per ragioni di persecuzione o discriminazione

Per evitare dunque di cadere nella trappola di una rete ispirata alla sorveglianza e al controllo, un *hacktivist* deve ricorrere a strumenti e strategie idonee a minimizzare i rischi di interferenza esterna sulle proprie attività e a massimizzare la capacità diffusive delle proprie informazioni. In questo senso, nel prosieguo si intenderanno ripercorrere gli strumenti più diffusi in grado di rendere le attività condotte attraverso la rete più efficaci e sicure.

È dunque prioritario rispetto a qualsivoglia altra considerazione una *valutazione del rischio*. Di questo se ne dirà meglio nei paragrafi che seguono, ove si forniranno specificazioni relative al tipo di attività svolta, attivismo politico, professioni sensibili quali quelle di giornalista o avvocato. Basti dire in questa sede che le pratiche di seguito elencate richiedono tempo ed esperienza per il loro efficace utilizzo. In questo

senso è necessario condurre una valutazione preliminare del tipo di rischio dal quale ci si intende proteggere, e comportarsi di conseguenza: se l'interesse fosse quello di sottrarsi al controllo delle multinazionali del *web* quanto all'acquisizione e al traffico dei nostri dati personali per finalità pubblicitarie, le misure da porre in essere saranno di un certo tipo, e l'obiettivo potrà essere perseguito con l'ausilio di semplici e accessibili programmi scritti *ad hoc* per questo tipo di tutela; se le necessità dovessero essere quelle di conservare la riservatezza delle proprie fonti o delle informazioni sui propri assistiti contenute nei dispositivi fissi o portatili attraverso i quali viene svolta la propria attività professionale, l'attenzione dovrà essere posta sulle modalità di conservazione e protezione dei dati, sulle modalità di trasmissione e infine sulle modalità di cancellazione; se ancora invece l'attività di attivismo politico o civile, o ancora l'esercizio delle professioni legali o giornalistiche, siano condotte in ambienti ostili, quali regimi autoritari, o anche solo in momenti di particolare attenzione delle istituzioni al perseguimento delle forme di sostegno, apologia o incitazione al reato, maggiore sicurezza dovrà essere assicurata con l'ausilio di tutta una serie di accortezze ulteriori rispetto al mero dato, coinvolgendo dunque una pluralità di aspetti da tenere in considerazione.

Altrettanto preliminare, in quanto necessario a prescindere dal tipo di pratiche poste in essere e dal grado di rischio considerato sussistente, è l'acquisizione di un *comportamento umano* orientato all'attenzione, alla precisione nei dettagli, alla coerenza complessiva della condotta di protezione. Risulterà infatti del tutto inutile, anticipando alcune delle pratiche di seguito dettagliate, cifrare i propri dispositivi, se poi tale estremamente efficace protezione venisse affiancata dalla trascrizione su un "foglietto volante" della *passphrase* di accesso, o ancora se tale chiave fosse la stessa utilizzata per una pluralità di altri contesti – quali

gli account dell'*email* pubblica o di un *social network*, o ancora per l'accesso alla pagina personale del servizio di fornitura di energia elettrica – attraverso i quali la stessa possa essere facilmente reperita. Allo stesso modo, rendersi tecnicamente anonimi nella propria navigazione su *Internet*, nascondendo il proprio indirizzo IP, bloccando *cookies* e *software* invasivi, magari ricorrendo altresì a una macchina virtuale, tutto ciò diverrebbe inutile se nel corso della sessione così attentamente predisposta ci si collegasse alla propria email personale con identificativo il proprio nome o cognome, o ad un *qualsiasi altro servizio che abbia registrato un nostro precedente accesso in chiaro*.

Le pratiche la cui conoscenza e utilizzo è fondamentale in questo senso sono le tre seguenti: la cifratura dei dati, attraverso la quale si rendono inaccessibili a soggetti terzi le informazioni di cui si sia in possesso; la navigazione anonima su *Internet*, al fine di non rendere possibile risalire all'origine della trasmissione di certi dati e, con particolari accorgimenti, neppure alla destinazione; la cancellazione sicura dei dati, attraverso la quale si persegue l'obiettivo di mantenere pieno controllo sui propri dati escludendo del tutto o limitando che tracce o residui restino sui dispositivi utilizzati.

Nell'ottica del perseguimento delle stesse finalità, ci sono ulteriori attenzioni che possono o devono essere poste in essere, in relazione alla previa valutazione del rischio: il ricorso a *email* temporanee, che permettano di accedere a determinati servizi senza costruire tracce eccessivamente stabili nel tempo; applicazioni e sistemi operativi *portable*, di modo da ridurre l'ostilità dei dispositivi pubblici o comunque di terzi con i quali una persona dovesse trovarsi, in una certa contingenza, ad operare; macchine virtuali, per creare ambienti operativi puri, utili a costruire profili idonei sia a trarre in inganno i servizi utilizzati su *Internet* sia a ridurre al minimo le tracce sullo stesso

dispositivo utilizzato, certamente compreso anche il proprio; la predisposizione di firewall *hardware*, così da poter accedere in sicurezza anche a reti pubbliche o private delle quali non sia possibile stabilire il grado di affidabilità.

5.3. La cifratura dei dati

Conoscere e praticare la cifratura dei dati è il passo immediatamente successivo all'acquisizione della consapevolezza della necessità di un utilizzo cosciente delle tecnologie dell'informazione e della comunicazione. Quale che sia il grado di rischio dal quale ci si intenda difendere e l'importanza dei dati da proteggere, la cifratura è allo stato lo strumento più efficace, e di semplice utilizzo, per conseguire lo scopo di impedire l'accesso a terzi ai dati propri o in proprio possesso.

Il principio della cifratura risale quantomeno ai tempi di Atene, con l'utilizzo della scitala lacedemonica, un bastone di determinate lunghezza e larghezza attorno al quale arrotolare un telo di stoffa sul quale era scritto un messaggio, leggibile solo a condizione di avere il bastone delle giuste dimensioni.

L'idea di rendere illeggibile un testo se non attraverso il ricorso a una chiave di lettura che ne rivelasse il contenuto originario, ha attraversato secoli e millenni[40], ed è con il calcolo elettronico che ha raggiunto la forza e l'accessibilità odierna. L'attuale crittografia infatti,

---

[40] ZICCARDI G., *Crittografia e diritto*, Giappichelli ed., Torino, 2003, pp. 31-39

fondata su algoritmi la cui risoluzione, in senso inverso nella prospettiva di accedere al testo originale cifrato, abbisogna di una quantità enorme – e non disponibile – di potenza di calcolo e di tempo dedicato, è utilizzabile attraverso programmi semplici da comprendere e gratuitamente reperibili attraverso *Internet*.

La questione è la seguente: il dato informatico comune è di per sé accessibile a chiunque entri in possesso del supporto che lo contiene, ovvero di chiunque abbia accesso alla porzione di *server* ove tale dato sia conservato, qualora il luogo virtuale non sia un proprio dispositivo. Proprio come un documento cartaceo appoggiato su un tavolo ben potrebbe essere letto da chiunque ne entri in possesso e un qualsiasi documento conservato in un archivio cartaceo possa subire la medesima sorte qualora chiunque, per qualunque ragione, abbia accesso all'archivio, così potrebbe accadere anche per ciò che è conservato in formato digitale.

Non importa in questo senso che un dispositivo sia protetto da *password*. Non soltanto infatti è sufficiente, come nella parte materiale della realtà, trovare la chiave corretta o rompere la serratura e la protezione sarà caduta, ma altresì le peculiarità della tecnologia rendono possibile, attraverso l'utilizzo di versioni LIVE dei sistemi operativi, ovvero attraverso la copia *bit-to-bit* del supporto che contiene di dati, la lettura del contenuto senza neppure doversi preoccupare di superare la protezione della password. Il contenuto di un dispositivo non protetto da cifratura è accessibile da chiunque abbia possibilità di entrare in contatto con il dispositivo stesso, sia materialmente sia attraverso una connessione ad *Internet*, salvo in quest'ultimo caso l'ipotesi di idonea protezione da accessi esterni.

I dati possono essere dei tipi più svariati: dati attinenti la propria persona, i propri gusti, le proprie amicizie o la propria famiglia; foto di

vacanza o materiale audiovisivo di svago; documenti attinenti il proprio lavoro o la propria professione, i propri studi; documenti ancora medici, sanitari, assicurativi, politici; dati, documenti, fotografie o materiale audiovisivo idonei a rivelare l'orientamento politico, religioso o sessuale dei detentori; tutti i dati sopra indicati relativi però a terze persone, semplici conoscenti, amici o familiari, o ancora clienti, assistiti, fornitori, pubbliche amministrazioni, colleghi. Ancora, informazioni relative al nostro posizionamento geografico in un determinato momento, alla cronologia delle attività svolte attraverso il nostro dispositivo, delle nostre relazioni sociali e professionali.

Vista la mole di informazioni conservate nei nostri dispositivi, è altrettanto ampia ed eterogenea la platea di soggetti che potrebbero essere interessati ad accedervi: dai conoscenti intenzionati a spettegolare alla moglie che cerca conferme o smentite ai propri sospetti, dai concorrenti nella propria attività economica, alle autorità governative in cerca di tracce di reato o di dissidenza dal regime vigente. Senza arrivare alle ipotesi di *cyberwarfare* che coinvolgono le infrastrutture critiche dei servizi pubblici e di sicurezza di interi Stati.

La cifratura (o crittografia) dei supporti e dei dispositivi è l'unico e più efficace strumento di protezione, di fronte a questi esemplificati attacchi e a tutti gli altri che siano in grado di portare nella disposizione dell'attaccante il contenuto del supporto o del dispositivo. Se infatti i dati non saranno stati preventivamente cifrati, tutto sarà liberamente consultabile. Ove al contrario colui che acquisisca il supporto si trovi di fronte materiale cifrato – bene – le probabilità di riuscita di un eventuale tentativo di recupero sono estremamente basse.

Un'ipotesi degna di nota per sollevare l'utilità della cifratura riguarda infatti l'utilizzo di dispositivi mobili, *computer* portatili o chiavette USB. Se infatti un dispositivo *desktop* è dotato, quantomeno

rispetto ai curiosi, della protezione aggiuntiva delle proprie mura di casa, protezione ovviamente non efficace nei confronti di ricerche o perquisizioni delle autorità, i *computer* portatili, i cellulari smart e le chiavette USB hanno una probabilità di essere perduti estremamente elevata. Se non cifrati, eventuali informazioni presenti sui dispositivi stessi saranno di agile accesso a chiunque ne venga in possesso.

Ulteriore attenzione da porre in essere consiste nell'applicazione del medesimo principio al trasferimento dei dati: l'utilizzo di chiavi di cifratura di tipo PGP/GPG[41] per occultare il contenuto delle nostre conversazioni via *email*, così come l'utilizzo di connessioni sicure cifrate e private, quali una *Virtual Private Network*[42], permettono di conseguire lo stesso risultato ma nella dinamica dello scambio delle informazioni. È ovvia considerazione che una tale operazione non rileverebbe alcuna utilità, se lo scopo fosse quello di diffondere pubblicamente un dato materiale o una certa informazione – in quel caso, plausibilmente, il problema potrebbe essere quello di occultare l'identità del soggetto che lo diffonde, o ancora del soggetto che ha generato quello specifico contenuto[43]. Qualora invece sia necessario stabilire un rapporto sicuro e confidenziale, il ricorso a sistemi, anche a pagamento e per quanto possibile a codice sorgente aperto, di cifratura delle connessioni può rendere possibile nascondere, dagli occhi

---

[41] Sul sistema di cifratura Pretty Good Privacy (o PGP), si veda la relativa pagina di Wikipedia, http://it.wikipedia.org/wiki/Pretty_Good_Privacy (verificato il 12.05.2014).

[42] L'utilizzo di *Virtual Private Network*, promosso da ormai tre lustri dal *Virtual Private Network Consortium*, garantisce una pluralità di vantaggi, oltre a quelli appena citati della riservatezza dei contenuti trasmessi, v. http://it.wikipedia.org/wiki/Virtual_Private_Network (verificato il 12.05.2014).

[43] Per quest'ipotesi, si veda il paragrafo immediatamente successivo.

indiscreti, il contenuto delle nostre comunicazioni. Tale sistema è presente nelle connessioni di tipo *https* che caratterizzano soprattutto i siti di *home banking*, e, se usati in concorso con accortezze di *human behavior* e di anonimizzazione dei dati identificativi dei propri dispositivi, e dunque delle proprie identità, fornisce un'ottima protezione.

Per gli operatori giuridici, la cifratura delle trasmissioni permea l'intero sistema del Processo Civile Telematico, proponendosi dunque il meritevole obiettivo, oltre a quello di garantire l'autenticità, la paternità e l'integrità, di proteggere i contenuti trasmessi, rientranti nella nozione di dati giudiziari ai sensi della normativa europea e italiana sulla protezione dei dati personali, da eventuali intromissioni di soggetti terzi[44].

5.4. L'anonimato delle comunicazioni

Come si ha appena avuto modo di introdurre, cifrare i dati e le comunicazioni è la tecnica migliore per salvaguardarne il contenuto da intromissioni, lecite o illecite, da parte di soggetti terzi, siano essi istituzionali o meno. Il passo successivo consiste nell'applicare lo stesso principio alla tutela dell'identità del soggetto autore e/o destinatario di una certa trasmissione. Riprendendo quanto indicato nei paragrafi

[44] Sul punto, sono di grande interesse, per il giurista, le Regole Tecnico-Operative per l'uso di strumenti informatici e telematici nel processo civile, elaborate dal Ministero della Giustizia e liberamente consultabili all'indirizzo http://www.processotelematico.giustizia.it/pdapublic/resources/D.M.%2017-7-2008%20(Regole%20tecniche%20PCT%20-%202008)%20allegato.pdf (verificato il 12.05.2014).

precedenti relativamente agli strumenti di sorveglianza, l'identità anagrafica e l'identità digitale di un soggetto possono essere rivelate, nel contesto dell'utilizzo delle infrastrutture e dei servizi della società dell'informazione, da una pluralità di tracce, usualmente raccolte nei registri di log: l'indirizzo IP, i numeri di identificazione dei dispositivi utilizzati, i sistemi operativi e i *browser*, con relative impostazioni, utilizzati, i *cookies*, i metadati, tra i quali ovviamente spicca la geolocalizzazione, ma anche e soprattutto l'approccio umano all'utilizzo dei servizi, quali l'auto identificazione o la diffusione di dati personali idonei, già di per sé o aggregati ad altri, a rivelare l'identità personale[45].

Nuovamente, le ragioni che possono motivare l'esigenza di nascondere, e dunque proteggere, la propria o l'altrui identità possono essere le più svariate: in un contesto commerciale, dissociare ogni sessione di utilizzo di determinati servizi dal profilo digitale elaborato alla luce delle sessioni precedenti può servire per bloccare le attività di profilazione, consistente nell'elaborazione di profili di preferenze, e le susseguenti attività di pubblicità mirata; un soggetto strenuo oppositore dei limiti imposti dalla normativa a tutela del diritto d'autore sui contenuti multimediali potrebbe voler proteggere la propria identità nell'utilizzo di servizi di *peer-to-peer* o *streaming*; in un contesto professionale, quale quello giornalistico, l'occultamento dell'identità propria o dei destinatari delle proprie comunicazioni, così come dell'origine, può garantire una tutela rispetto a ritorsioni sempre professionali, repressive, determinate dalle notizie diffuse; in un contesto

[45] Per una raccolta ampia e onnicomprensiva degli articoli scritti in materia di anonimato, da un punto di vista eminentemente tecnologico, si veda la raccolta contenuta su Freehaven, http://freehaven.net/anonbib/ (verificato il 12.05.2014).

di resistenza contro un regime oppressivo, diventa fondamentale, avuto riguardo alla tutela della propria integrità personale e della stessa vita umana, separare dalle informazioni comunicate o diffuse qualsivoglia elemento in grado di permettere ai soggetti, che per la conservazione del regime lavorano, intenzionati a reprimere la diffusione stessa.

I quattro esempi sopra delineati ben rappresentano la questione della valutazione del rischio, necessità preliminare, al fine di individuare di quale livello di garanzia del proprio anonimato si abbia bisogno. Nel primo caso, le esigenze di difesa da aggressioni commerciali indesiderate giustificano uno sforzo calibrato ad una minaccia che, seppur percepita come rilevante, ha una portata dannosa limitata, e in tal senso l'impiego di energie e potenza di calcolo per la tutela della propria identità sarà più limitato. Nell'ipotesi di tutela dell'identità durante attività di *download* o condivisione o fruizione di materiali coperti dal diritto d'autore, l'interesse sarà presumibilmente quello di proteggersi dalle – limitate – possibilità di tracciamento da parte di imprese o autorità, o più probabilmente da parte del proprio datore di lavoro. Diversamente, nel terzo e specialmente nell'ultimo caso, tutti gli strumenti disponibili al fine di tutelare la propria identità dovranno essere messi in campo, cumulativamente tra loro, adattandosi di volta in volta alle specifiche necessità calibrate anche sul dispositivo utilizzato.

Quanto ai livello di anonimato, ci sono diversi strumenti che permettono di conseguire risultati progressivamente sempre più efficaci: dalla disattivazione di *cookies*, dalla disabilitazione di *software* quali *Flash*, dalla pulizia delle tracce cronologiche e delle impostazioni personalizzate dei propri sistemi operativi e *browser*, passando per l'utilizzo di *proxies* per accedere ai servizi in rete e di *email* temporanee per iscriversi a tali servizi, per arrivare all'utilizzo di reti cifrate e anonime, quali tra tutte TOR (*The Onion Routing*). Ancora, questi

strumenti possono essere utilizzati non solo per specifiche comunicazioni, ma anche per la creazione di spazi di diffusione dell'informazione anonimi, come *blog* e siti *web* nascosti, in quella che viene definita *deep web*[46], Questi strumenti, utilizzati con un *human behavior* attento a non rilasciare intenzionalmente o inconsapevolmente tracce che permettano la riconducibilità al soggetto autore, possono far conseguire livelli di anonimato estremamente elevati, in grado di resistere ad attacchi provenienti anche dai più avanzati livelli di *forensics* digitale.

Nel specifico, l'utilizzo di *proxies*[47] consiste nel domandare l'accesso ad una determinata pagina o a un determinato servizio passando attraverso una pagina terza, un *proxy*, che si incarica di inviare la richiesta e di restituire il risultato filtrato attraverso il proprio servizio. La pagina di destinazione non registrerà dunque sul proprio registro di *log* l'indirizzo IP dell'autore originario della domanda bensì quello del sito che ha messo a disposizione il servizio di *proxy*. L'utilità di questo servizio, oltre a quella appena indicata, si può ritrovare anche nella possibilità di utilizzo al fine di aggirare filtri di accesso a determinati siti bloccati su base di *router* territoriali. Se infatti il sito che offre servizi di *proxy* risiede all'estero, e ovviamente non è a sua volta bloccato, sarà questo a richiedere l'accesso alla pagina richiesta, e a restituirla quale

---

[46] Il *deep web* è l'insieme delle risorse del *web* non segnalate dai motori di ricerca e non raggiungibili attraverso i browser tradizionali. TOR, *I2P anonymous network* e *Freenet* sono *software* per l'accesso e la messa a disposizione di risorse sul *deep web*.

[47] Una descrizione, sintetica ma completa, delle potenzialità dei *proxies* è consultabile alla relativa pagina sul sito di Wikipedia, http://en.wikipedia.org/wiki/Proxy_*server* (verificato il 12.05.2014), mentre per una lista aggiornata di siti che forniscono servizi di proxy, http://proxy.org (verificato il 12.05.2014).

risultato, bloccata nel paese di origine della comunicazione.

L'utilizzo di *email* temporanee[48] può essere utile al fine di preservare la propria identità digitale al momento di iscriversi a servizi che richiedano la comunicazione di un'email valida e funzionante, alla quale inviare una conferma dell'avvenuta iscrizione. Posto infatti che le *email* tradizionalmente utilizzate saranno piene di tracce che riconducano la casella stessa ad una specifica identità, quand'anche il dominio e il nome scelto appaiano anonimi, il loro utilizzo comporterebbe necessariamente una *disclosure*, magari non diretta ma mediata, dell'identità del titolare dell'*account*. Il ricorso a *email* temporanee, avendo cura di nascondere altresì il proprio indirizzo IP e gli altri dati basilari identificativi, può ovviare a queste necessità.

L'utilizzo della rete di TOR[49] è uno dei più avanzati sistemi di protezione della propria identità, oltre che di parziale cifratura delle comunicazioni, e soprattutto di aggiramento dei filtri imposti su base geografica a scala locale, regionale o nazionale. Rinviando alla pagina del progetto per le specifiche tecniche, il principio di funzionamento di

---

[48] Esempi di servizi di email temporanee sono disponibili ai seguenti indirizzi, http://it.getairmail.com/, http://10minutemail.com/10MinuteMail/index.html, https://www.guerrillamail.com/ (collegamenti verificati il 12.03.2014).

[49] Il sito del Progetto TOR è https://www.torproject.org/ (verificato il 12.05.2014), mentre per una descrizione, sintetica ma completa, si rinvia alla relativa pagina di Wikipedia, http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29 (verificato il 12.05.2014). Tra gli articoli più recenti relativi alle falle di sicurezza nel sistema di TOR, JANSEN R., TSCHORSCH F., JOHNSON A., SCHEUERMANN B., *The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network*, in *21st Annual Network & Distributed System Security Symposium*, 2014, consultabile all'indirizzo http://www.robgjansen.com/publications/sniper-ndss2014.pdf (verificato il 12.05.2014).

TOR è di una semplicità disarmante: i dati trasmessi attraverso il *browser* di TOR non arrivano direttamente alla destinazione richiesta, ma attraversano tre diversi *computer*, ciascuno dei quali opera un proprio livello di cifratura dei dati relativi all'origine. In tale modo il primo *computer* conosce l'origine, ma non la destinazione; il secondo *computer* non conosce né l'origine né la destinazione, e il terzo *computer* conosce solo la destinazione. Tutti questi passaggi sono altresì cifrati, fintanto che la comunicazione rimane all'interno della rete TOR, dunque fino al terzo *computer* o nel caso di accesso agli *hidden services*[50] interni alla stessa rete, ma non nel passaggio dal terzo *computer* alla destinazione. Se dunque TOR può ben essere utilizzato per nascondere la propria identità e il contenuto delle trasmissioni al proprio ISP o al proprio datore di lavoro, lo stesso non può dirsi di eventuali soggetti capaci di interporsi prima dell'arrivo al sito di destinazione. Per ovviare a tale problema sarà dunque necessario adoperare, di concerto con TOR, altri sistemi di cifratura, quali le connessioni di tipo *https* e le *mail* o servizi di *chat* a loro volta cifrati. Come anticipato per i *proxies*, anche TOR[51] può essere efficacemente utilizzato per aggirare i sistemi di filtro, blocco e sorveglianza su base territoriale, oltre a fornire la possibilità di impostare il nodo di uscita, così da scegliere da quale paese si intende far

[50] Per gli hidden services della rete TOR, https://www.torproject.org/docs/hidden-services.html.en (verificato il 12.05.2014).

[51] Per uno studio dettagliato sull'utilizzo dei *proxies* e di TOR per le finalità di aggirare i filtri e i blocchi geografici di *Internet*, si consiglia AA.VV., *2010 Circumvention Tool Usage Report*, a cura del *Berkman Center for Internet & Society at Harvard University* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf (verificato il 12.05.2014).

apparire proveniente la propria trasmissione[52].

5.5. La cancellazione sicura dei dati

Un ulteriore elemento fondamentale nella difesa dei propri dati, delle proprie attività e della propria identità nel contesto digitale è il ricorso a sistemi sicuri per la cancellazione dei propri dati[53]. I dispositivi perduti, venduti o dismessi, nel caso non fossero stati a loro volta cifrati, sono infatti una delle più cospicue fonti di informazioni relative al soggetto che li avesse utilizzati. Si pensi, per andare subito nel concreto, al disco rigido di un dispositivo, *desktop* o *laptop* che sia, utilizzato all'interno di una struttura ospedaliera o di uno studio legale alla fine della propria utilità: la mera cancellazione dei dati o formattazione del disco – e in certi casi persino questo passaggio rischia di essere omesso – non impedisce in nessun modo a chiunque entri in possesso del dispositivo di accedere alla quasi totalità dei dati, rispettivamente sanitari e giudiziari, ivi contenuti.

La cancellazione basilare dei dati, così come la formattazione, altro non fa che impostare i *bit* che definiscono lo stato di disponibilità di un certo spazio digitale nello stato "libero", non provvedendo in alcun modo ad alterare i *bit* relativi invece al contenuto del materiale cancellato. Tale contenuto sarà, eventualmente, sovrascritto nei

---

[52] Pratica particolarmente utile nel caso si intenda ricorrere a servizi, quali streaming o acquisti online, limitati su base territoriale nazionale o regionali.

[53] Un programma di semplice utilizzo per la cancellazione sicura dei dati è Eraser, disponibile gratuitamente all'indirizzo http://eraser.heidi.ie/ (verificato il 12.05.2014).

successivi utilizzi, continuando però a conservare a lungo tracce di quanto originariamente salvato. Le pratiche di *digital forensics* hanno per l'appunto l'obiettivo di procedere al recupero di dati suppostamente cancellati, e la facilità di utilizzi di tali strumenti è tale da permettere a chiunque di operare questo recupero, detto *data carving*. Diversamente, al fine di rendere inaccessibili tali dati originari, i supporti di memorizzazione dovranno essere cancellati attraverso il ricorso a *software* che operino successive cancellazioni e sovrascritture, di modo da eliminare la totalità dei *bit* e delle tracce lasciate dal materiale originariamente contenuto. Queste procedure richiedono tempi molto lunghi, persino di diverse ore o giornate intere, nel caso si provveda a cancellare in maniera sicura interi dischi di diverse centinaia di *gigabytes*. Nel caso la valutazione del rischio richieda prudenza ancora ulteriore, può essere raccomandato procedere con la distruzione materiale del supporto e, o in alternativa, la conservazione dello stesso, benché già cancellato in maniera sicura, in luoghi fisici sicuri di propria pertinenza.

5.6. Altre tecniche per proteggere e nascondere

Ulteriori tecniche che possono essere utilizzate per proteggere o nascondere sono l'utilizzo di distribuzioni LIVE di programmi o sistemi operativi, la creazione di chiavi USB con versioni *portable* dei propri *software* utilizzati, o ancora l'utilizzo di macchine virtuali in vece dell'ambiente virtuale predisposto nel dispositivo che si abbia a propria disposizione. Tutti e tre questi strumenti hanno lo scopo di creare ambienti autonomi rispetto al dispositivo utilizzato, svincolandone l'utilizzatore e fornendo così un certo livello di protezione della propria identità, dei propri dati, e delle attività così poste in essere. In definitiva,

sono strumenti finalizzati ad aumentare il proprio anonimato digitale.

L'utilizzo di macchine virtuali, o *virtual machines*[54], è orientato allo scopo di creare ambienti autonomi dal dispositivo che si sta utilizzando. Le utilità sono molteplici e vanno dal testing di sistemi operativi diversi da quelli usualmente utilizzati, prevenendo il rischio di danneggiare l'ambiente principale, dal testing di programmi o *software* potenzialmente malevoli, alla creazione di profili digitali diversi da quelli originari facendo in modo, per esempio, che nel corso dell'utilizzo di un servizio su *Internet* risalti la provenienza da un certo sistema operativo piuttosto che un altro. Il funzionamento è semplice, e consiste nell'utilizzo di *software* che "aprono" un ambiente virtuale e che, una volta "spenti", non lasciano, sul dispositivo originario, alcuna traccia delle attività svolte al suo interno. La cura sarà quella di doversi assicurare, attraverso il riavvio del dispositivo, siano cancellate le informazioni conservate nella memoria RAM del dispositivo.

L'utilizzo di distribuzioni LIVE dei sistemi operativi apre possibilità molto eterogenee tra loro: il principio consiste nella possibilità di avviare un dispositivo facendo ricorso non al sistema operativo ivi presente, ma al dispositivo presente in una chiavetta USB o in un supporto ottico predisposto a tal fine. L'ambiente nel quale ci si troverà ad operare potrà essere stato configurato per le più disparate finalità: potrà essere orientato al massimo anonimato, qualora fosse stato impostato per l'utilizzo di *software* quali TOR per la navigazione sul

[54] Tra i più semplici e funzionali *software* per la creazione di macchine virtuali, si veda OracleVirtual Box, https://www.virtualbox.org/ (verificato il 12.05.2014), e QEMU, http://wiki.qemu.org/Main_Page (verificato il 12.05.2014).

web, *I2P anonymous network*[55] per lo scambio dei *files* attraverso reti cifrate *peer-to-peer*, *Cryptocat*[56] per *chat* cifrate, e così discorrendo; potrà essere invece già predisposto in tal senso da altri programmatori, ed è il caso di TAILS[57], un sistema operativo basato su Debian impostato al fine di garantire riservatezza e anonimato; potrà essere finalizzato ad avere a disposizione un ambiente operativo per lo svolgimento di attività di *digital forensics*, qual è il caso di DEFT[58], distribuzione basata su Linux con la quale si hanno immediatamente a disposizione gli strumenti più utili per le indagini informatiche; oppure ancora potrà essere una versione generica di un sistema operativo, quali le versioni LIVE di Ubuntu[59], il cui scopo è, principalmente, quello di provare un diverso sistema prima di implementarlo sul proprio dispositivo.

Infine, la creazione di una chiavetta USB con le proprie applicazioni in versione *portable*[60] risponde alle medesime esigenze: attraverso questo sistema è infatti possibile utilizzare specifici *software*, installati per l'occasione sulla chiavetta, quando ci si trovasse ad utilizzare dispositivi di terzi. I *software* possono essere gli stessi anonimi

---

[55] Il sito del progetto *I2P anonymous network*, https://geti2p.net/en/ (verificato il 12.05.2014).

[56] Il sito del progetto *Cryptocat*, https://crypto.cat/ (verificato il 12.05.2014).

[57] Il sito di TAIL, https://tails.boum.org/ (verificato il 12.05.2014).

[58] Il sito di DEFT, http://www.deftlinux.net/it/ (verificato il 12.05.2014).

[59] Il sito di Ubuntu, http://www.ubuntu.com/ (verificato il 12.05.2014).

[60] Per una sintetica, ma completa, descrizione del funzionamento delle applicazioni portable, http://en.wikipedia.org/wiki/Portable_application (verificato il 12.05.2014), mentre per una lista delle più utilizzate applicazioni, http://portableapps.com/ (verificato il 12.05.2014).

citati in precedenza, oppure semplicemente *software* per la videoscrittura o l'utilizzo di servizi VoIP usualmente non disponibili sulle macchine generiche. La peculiarità dell'utilizzo di versioni *portable* riguarda la possibilità di bypassare eventuali *keylogger* al momento di inserire la propria password in relazione a servizi email, VoIP o altro. Se infatti un *keylogger* permette di registrare tutti i tasti premuti in una certa sessione di utilizzo di una tastiera, per il tramite di una versione *portable* è possibile avviare la propria autenticazione ricorrendo alle password memorizzate all'interno della chiavetta stessa, non dovendo così digitarle a propria volta. Al di là dell'ipotesi della presenza di un *keylogger*, attraverso le applicazioni *portable* è possibile utilizzare, per esempio, propri *browser* o propri *software* di accesso al servizio di email, possibilmente cifrati, di modo da non lasciare alcuna traccia sul dispositivo utilizzato.

5.7. La valutazione del rischio

Alla luce di tutte queste possibilità sopra brevemente descritte, in relazione alle quali si rinvia in ogni caso alle specifiche tecniche e alle guide disponibili sui relativi siti e sugli specifici *forum* di discussione, gli strumenti per rendere più discreto il proprio utilizzo delle reti di telecomunicazione sono diversificati e spesso tra loro complementari. Il punto più rilevante nell'individuare la soluzione adatta alle proprie necessità si ritrova in una fase che dovrebbe essere preliminare rispetto all'implementazione di queste strategie: la *valutazione del rischio*.

Questa fase è di fondamentale importanza e *consiste nella valutazione di tutte le possibili minacce in termini di probabilità di occorrenza e relativo danno potenziale*. Sulla base del risultato di tale

valutazione, l'*hacktivist* o il soggetto che utilizza gli strumenti informatici decide quali contromisure adottare. Questa fase riveste fondamentale importanza per un duplice ordine di motivi: in primo luogo, perché permette di focalizzare la propria attenzione non su astratti comportamenti in grado di garantire, suppostamente, un ideale anonimato digitale, bensì sulle specifiche esigenze in relazione ai rischi che si intendono prevenire, individuando così il combinato di pratiche più idoneo alle contingenti necessità; in secondo luogo, perché consente di limitare al massimo le controindicazioni di ciascuna di queste strategie.

Quanto all'individuazione dei rischi specifici, come si è avuto modo di anticipare in sede di descrizione di alcune delle precedenti tecniche, è naturale rilevare come la difesa nei confronti di attività pubblicitarie meriti attenzione distinta rispetto a quella nei confronti di un regime autoritario nei confronti del quale si intende condurre una lotta politica, ovvero di un'organizzazione criminale oggetto delle proprie investigazioni. Se infatti è certamente buona pratica abituarsi a lavorare in contesti cifrati, anonimi e sicuri, non sarà necessario combinare distribuzioni LIVE, TOR, *mail* temporanee e cancellazione sicura dei dati per la mera difesa dalla profilazione commerciale di Google. Diversamente, nel caso di attività condotte in contesti di alto rischio per l'incolumità propria e altrui, il ricorso al maggior numero di tecniche integrate da loro sarà un prerequisito della condotta ispirata alla sicurezza e all'anonimato.

Allo stesso modo, le pratiche di cui sopra non sono esenti da controindicazioni e da rischi. La navigazione anonima attraverso TOR, per esempio, rallenta notevolmente la velocità di connessione, e non è infrequente incontrare siti web che rifiutano l'accesso percependo che la connessione proviene da terzi intermediari, piuttosto che dall'originale

autore della trasmissione. Il ricorso a strumenti di cifrature consente sì di proteggere il contenuto dei dati cifrati, ma in caso di perdita della *password* o della *passphrase* di accesso non sarà più possibile recuperare quanto nascosto. E lo stesso rischio si corre nell'ipotesi della cancellazione sicura dei dati: in quanto sicura, per propria stessa definizione, un eventuale errore nella selezione dei contenuti da cancellare non potrà essere rimediato, così come non vi sarà margine per un ripensamento.

Come si avrà modo di chiarire in conclusione, la fase della valutazione del rischio è il momento più importante che permette di compensare costi e benefici del ricorso alle *Liberation Technologies*, tenendo presente i rischi, le esigenze, le minacce e anche le proprie competenze, e valorizza altresì il fondamentale ruolo svolto dall'approccio umano nell'utilizzo consapevole e responsabile delle nuove tecnologie. Nello specifico, i tratti del comportamento umano maggiormente suscettibili di ingenerare conseguenze dannose in punto di conservazione e protezione del proprio anonimato o della riservatezza delle proprie attività nel contesto digitale sono: la scelta degli elementi di autenticazione, quali *password* o *passphrase* semplici o banali; il rilascio volontario o inconsapevole di informazioni che riconducano alla propria vita personale; e ancora l'accesso a servizi – *webmail*, *social network* – ai quali vi sia dato accesso in precedenza “in chiaro”, quand'anche i profili creati siano di per sé anonimi. In generale, il rischio maggiore è insito nella convinzione di essere completamente anonimo e nascosto, quando invece lo strumento digitale contiene in sé tutto quanto necessario a tracciare, memorizzare e conservare le informazioni relative alle attività condotte, nonostante la quantità e la qualità delle accortezze che possano essere messe in campo.

"*La libertà, come tutti sappiamo, non fiorisce in un paese*
che sta sempre sul piede di guerra, o che si prepara a combattere.
Una crisi permanente giustifica il controllo su tutto e su tutti,
da parte del governo centrale."

Aldous Huxley, Ritorno al mondo nuovo, 1958

CONCLUSIONI

La rete di oggi nell'ottica dell'Europa di domani

Giunti alla conclusione di questo percorso, si spera di aver fornito alcuni esempi di quanto affermato in introduzione, sull'incidenza che il contesto sociale, economico e tecnologico, che caratterizza l'età contemporanea della società dell'informazione ha e avrà sull'esercizio del fondamentale diritto alla libertà d'espressione, così come sullo strettamente correlato diritto alla tutela della vita privata e con questo sul diritto al controllo dei propri dati personali da parte degli individui.

In particolare, quanto portato alla pubblica conoscenza dalle rivelazioni relative al Progetto PRISM, condotto dalle autorità di sicurezza nazionale degli Stati Uniti complice anche l'inerzia, il silenzio e in certi casi persino il sostegno delle autorità nazionali di alcuni paesi terzi, anche membri dell'Unione Europea, non rappresenta quindi altro che una certificazione di quanto noto o quantomeno deducibile dallo stato dei rapporti di forza tra gli Stati e le imprese transnazionali in ambito diplomatico, politico ed economico. L'impronta imperiale nella gestione della attuale supremazia tecnologica si è tradotta in plurime condotte, osservabili nei più svariati campi dell'azione istituzionale,

lesive dei diritti dei soggetti terzi, cittadini, organizzazioni e Stati. Il risultato, nell'ambito delle infrastrutture delle *Information and Communication Technologies*, quello che qui rileva, è un modello di *governance* fondato sì sul decentramento e sull'acefalia tecnica e, in parte, anche giuridica, ma sospinto e diretto, nelle proprie evoluzioni, verso un accentramento ed un indirizzamento del traffico di dati attentamente mirato, in modo tale da poter concentrare le attività di sorveglianza e controllo su nodi infrastrutturali sostanzialmente obbligati. E questo risultato viene raggiunto sia attraverso le implementazioni tecnologiche della rete, sia attraverso il ruolo centrale svolto da fornitori di servizi della società dell'informazione con sede, perlopiù, oltreoceano.

Vi sono dunque la diffusione di enormi *server farm*, contenenti dati personali, familiari, professionali, sanitari, giudiziari, politici, di centinaia di milioni di persone, il diretto accesso da parte delle autorità alle informazioni lì conservate, il controllo dei nodi materiali o satellitari di trasporto dei dati tra continenti, la costruzione di *data farm* dotate di una estremamente elevata potenza di calcolo in grado di analizzare, studiare ed elaborare i profili derivanti dall'ingente mole di informazioni così raccolta. Indifferentemente poi l'utilizzo dei profili umani a base digitale così elaborati potrà essere disposto per finalità di promozione commerciale, pubblicità mirata, fornitura di servizi non richiesti, o discriminazione e persecuzione politica, economica e sociale sulla base delle più svariate preferenze assunte come criterio di devianza dagli ordini costituiti. E, profilo di non scarso rilievo, tutto ciò viene condotto nella segretezza delle operazioni di difesa delle sicurezze nazionali, degli spazi di autonomia privata, nelle pieghe lacunose del diritto interstatuale e internazionale.

In questa prospettiva, i soggetti nelle rilevanti posizioni di cui

sopra hanno nelle proprie mani gli strumenti per indirizzare la circolazione delle informazioni, limitarne o estrometterne contenuti nel perseguimento delle proprie finalità, siano esse la "protezione della sicurezza nazionale" ovvero "perseguire, senza sosta o eccezione, il proprio interesse, disinteressandosi delle conseguenze frequentemente dannose che possa causare agli altri". E così l'accentuazione della rilevanza della tecnologia nella determinazione di ciò che è possibile e impossibile, accompagnato da un allentamento della presa degli ordinamenti giuridici nazionali sui comportamenti e sulle scelte attuate dai propri cittadini – siano indifferentemente persone fisiche cittadini o imprese e persone giuridiche operatrici nel concorrenziale mondo della globalizzazione economica e comunicativa – non può che comportare una riduzione delle garanzie dei diritti dell'individuo, poste precipuamente a tutela della libertà di autodeterminazione, in assenza di vincoli o influenze sui processi mentali di adozione delle proprie scelte.

Dunque diventano gli operatori privati che forniscono servizi nella società dell'informazione, spalleggiati da Stati e Agenzie più che interessate a conseguire i propri risultati attraverso la loro collaborazione, a determinare quando e in che forma comunichiamo, così influenzando indubbiamente il contenuto stesso delle nostre comunicazioni. La previsione di dettagliate normative, anche a rilievo sopra nazionale, a tutela della libertà di espressione o, aspetto ancor più calzante nel recente dibattito in particolare europeo, del diritto al controllo sul trattamento e dunque al controllo della circolazione dei dati che ci riguardano devono necessariamente rapportarsi al dato di fatto alla luce del quale i dati sono fatti circolare, anche a seguito di nostre scelte di volontà, al di fuori dei territori di operatività delle normative stesse, poste a tutela delle garanzie che ne permettono una libera determinazione.

Tutto questo rileva ai fini dell'individuazione dei punti critici irrinunciabili attorno ai quali elaborare risposte normative nazionali, regionali e internazionali efficaci a ristabilire la supremazia degli strumenti dello Stato costituzionale di diritto, esso stesso inteso quale mezzo strumentale alla libera autodeterminazione delle persone e delle comunità. Nel nostro contesto culturale e giuridico europeo, i principi irrinunciabili da perseguire dovrebbero dunque essere i seguenti:

1. *il riconoscimento della supremazia, in punto conclusivo, dei diritti fondamentali dell'individuo dinnanzi agli interessi istituzionali alla sicurezza statale e ai diritti di natura economica*, siano essi la proprietà privata, l'iniziativa economica privata, i diritti in materia di proprietà intellettuale o, alla luce dei presupposti giacenti sotto le bozze del TTIP, le aspettative di ritorno economico degli investimenti;

2. *il riconoscimento del luogo giurisdizionale integralmente pubblico quale unico e solo adibito a sciogliere le controversie in materia di conflitti tra diritti diversi e diritti e interessi confliggenti:* sia esso un tribunale nazionale o un organo di giustizia comunitario, le eventuali decisioni prese da soggetti interposti nelle more dei lunghi tempi della giustizia devono essere trasparenti, denunciabili e non definitive;

3. *la rinuncia ai privilegi offerti dalle normative in materia di segreto industriale e segreto di Stato*, prevedendo nel caso, per questo ultimo, strettissimi e ineludibili vincoli temporali, possibilmente compresi tra i cinque e i dieci anni: un'efficace tutela di quanto sopra non può che essere perseguita nella piena coscienza di quanto posto in essere dagli operatori istituzionali ed economici, nei termini di decisioni interne sulle procedure di sorveglianza e controllo, delle attività di profilazione, delle

attività di ricerca, individuazione e selezione dei contenuti da segnalare o rimuovere;

4. *il superamento delle normative che permettono di mantenere segreto il codice sorgente delle infrastrutture critiche e dei servizi informatici, disponibili al pubblico,* della società dell'informazione, prevedendo obblighi di *disclosure* regolari, costanti e completi;

5. *il coordinamento, a livello comunitario, di progetti di formazione e investimento nell'utilizzo cosciente delle nuove tecnologie dell'informazione*, capillarmente proposto attraverso i diversi sistemi di formazione pubblici e privati, sin dall'infanzia e in particolare destinati all'adolescenza, sul modello di programmi di educazione alla cittadinanza digitale.

Il paradosso delle tecnologie della liberazione

Come si è già espresso, il tema delle *Liberation Technologies* è attraversato da un paradosso di fondo ineludibile sul piano della logica stretta, che altro non è se non la riproposizione delle tematiche relative al *dual use* delle tecnologie sviluppate nei diversi campi: una tecnologia o tecnica è sostanzialmente neutra, e l'orientamento etico e morale degli effetti conseguiti dipende dalla direzione del suo utilizzo, e ancor prima dal sistema valoriale di riferimento. Dunque le progressioni scientifiche in materia di energia nucleare potrebbero essere utilizzate tanto per finalità civili e di accrescimento del benessere generale, quanto per le più distruttive finalità belliche; gli avanzamenti in materia di manipolazione genetica degli organismi potrebbero essere utilizzate tanto per il supposto rafforzamento delle specie dinnanzi a minacce

naturali o artificiali esterne, quanto per la creazione di deviazioni idonee a devastare la natura ambientale o umana, rispettivamente attraverso la creazione di specie vegetali sterili o di individui con sistemi immunitari esclusivamente artificiali inidonei a difendersi autonomamente ad un ambiente, invece, in continua evoluzione.

Allo stesso modo una tecnologia di cifratura può essere utilizzata per occultare i propri intimi pensieri e proteggere la propria riservatezza, ovvero per nascondersi e occultarsi dalla raccolta di profili individuali e collettivi, condotta attraverso pratiche di sorveglianza illegali. Ancora lo stesso strumento può essere utilizzato da parte di soggetti criminali per rendere inaccessibili i database relativi alle proprie attività, ai propri bersagli, ai propri collaboratori, ovvero diversamente da parte delle autorità dedite alla lotta contro i fenomeni di corruzione, associazionismo di stampo mafioso, tratta degli esseri umani e dei corpi su scala internazionale.

Di fronte a questo pluralismo di possibilità, non risulta agevole stabilire un confine al di qua del quale un utilizzo sarebbe lecito e al di là del quale l'utilizzo sarebbe, al contrario, da considerarsi illecito. Se è possibile fissare un punto fermo nel riconoscimento che, in linea generale, il principio del *dual use*, ovvero il più ampio concetto della neutralità tecnologica, appare sostanzialmente condivisibile, è fondamentale riconoscere che la via d'uscita da questo paradosso è rappresentata da una scelta eminentemente politica.

Così come le scelte costituzionali non furono frutto di logica giuridica stretta ma rivendicazione politica tradotta nel mondo del diritto, così le scelte in materia di promozione o dissuasione dall'utilizzo di una o dell'altra tecnologia non può che passare per una motivazione sostanzialmente politica, che effettui una rivendicazione dell'analisi costi-benefici, puntualizzando che sì la tecnologia in sé è neutra, ma

l'utilizzo che si intende farne o che sia plausibile che venga fatto è, o meno, accettabile, *di modo dunque che la neutralità dello strumento non diventi uno schermo dietro il quale nascondere una, questa non esistente, neutralità delle finalità*.

È dunque necessario, all'atto di promuovere la diffusione del ricorso alle *Liberation Technologies* tra gli individui della collettività, chiarire la natura fortemente politica di questa rivendicazione, in relazione al rapporto tra sicurezza, libertà, trasparenza e riservatezza. In questo senso, è parere di chi scrive che l'aumento della riservatezza degli individui e della trasparenza invece dei soggetti economici e istituzionali comporti un aumento delle libertà individuali e collettive e, con esse, della sicurezza sociale complessiva. Tale assunto, si ripete, eminentemente politico, comporta rischi e pericoli di lesioni, che necessariamente potranno avvenire e avverranno, di altri diritti. Così come infatti riconoscere diritti di libertà di movimento e di azione comporta un aumento del rischio di condotte antisociali, così rivendicare la supremazia della libertà di espressione comporta, dinnanzi ai diritti individuali alla dignità e tutela della riservatezza, accentuati rischi di comunicazioni diffamatorie o ingiuriose, dinnanzi ai diritti di natura patrimoniale relativi al diritto d'autore, rischi di più frequenti lesioni e, dinnanzi agli interessi securitari, ridotti margini di intervento in sede repressiva e sanzionatoria. Però è questo il nodo: giunti nella prossimità del punto di contatto da questi diversi interessi, il confine è rappresentato da una linea senza dimensioni, e dunque non esiste possibilità di equilibrio, essendo al contrario necessario operare una scelta, possibilmente riducendo al minimo la distanza dall'ideale mediano.

La convinzione di fondo è quella libertaria, secondo cui l'accrescimento degli spazi di libertà individuali, pur comportando concreti rischi di abusi, specie nel breve e nel medio periodo, ma

comunque persistenti in ogni tempo e luogo, sia comunque la strada migliore per garantire lo sviluppo e la maturazione di criteri di responsabilità idonei ad accrescere, nel complesso, la tenuta sociale, e dunque la sicurezza, dell'intero sistema di relazioni interpersonali. E in questa direzione, quella dello sviluppo di responsabilità nella libertà, si muovono le intenzioni pedagogiche, didattiche e formative nell'uso cosciente delle possibilità messe a disposizione dalle tecnologie informatiche.

Resta, prima di passare al punto conclusivo, il conflitto tra diritti entrambi individuali ed entrambi con rilievo personalissimo e fondamentale. Si parla del rapporto tra tutela del diritto alla libertà di espressione e tutela del diritto alla riservatezza. Se infatti si ritiene il diritto al controllo dei propri dati personali un diritto strumentale alla garanzia dei diritti di cui sopra, la riservatezza intesa nell'ampia concezione della tutela di un proprio intimo spazio personale è valore fondamentale imprescindibile. Sul punto l'equilibrio non è, allo stato, raggiungibile: le diverse proposte elaborate dalle legislazioni e dalle giurisprudenze comportano rischi ancora molto elevati. Non è in grado, chi scrive, di stabilire criteri sostanziali del rapporto tra questi due diritti, pur ritenendo di individuare nel concetto di *interesse pubblico alla conoscenza* il discrimine tra preminenza del diritto alla libertà di espressione rispetto al diritto alla tutela della propria riservatezza. Diversamente, si ritiene possano essere fissati alcuni elementi procedimentali, utili a raffinare il tiro nell'individuazione di una soluzione il più equilibrata possibile. E questi possono essere riassunti nella questione della competenza e della durata temporale della tutela:

1) *riconoscimento della competenza giurisdizionale nel dirimere le controversie relative alla sussistenza o meno dell'interesse pubblico alla conoscenza* di determinate informazioni, con esplicita esclusione dei

soggetti privati nell'operare tale bilanciamento. In questo senso, la decisione della Corte di Giustizia dell'Unione Europea in merito al diritto all'oblio pare aprire scenari poco rassicuranti, con rischio di ingenerare procedure del tutto interne ai fornitori dei servizi della società dell'informazione piuttosto che uno snellimento della giustizia ordinaria statale o comunicaria;

2) *preminenza, in via sostanziale, del diritto alla libertà di espressione, in questo contesto declinata nel diritto di critica, di cronaca e del diritto alla verità storica, eventualmente elaborando la tutela del diritto all'oblio quale eccezione limitata temporalmente*, invertendo dunque l'approccio prevalente che vorrebbe l'interesse all'informazione svanire con il passare del tempo: se in un primo momento rileva la libertà di espressione nella forma del diritto di cronaca e di informazione, e in un secondo momento, esaurito l'interesse immediato alla conoscenza, si possa ritenere prevalente un diritto alla tutela della propria riservatezza, e dunque allo svolgimento di una vita serena, per il tramite del riconoscimento di un diritto all'oblio, è indubbio che, trascorso un ulteriore periodo, i fatti storici debbano poter essere recuperati, narrati e riproposti senza limitazioni, in ossequio alla necessità di elaborare una ricostruzione storica il più fedele possibile agli accadimenti fattuali.

Formazione all'uso cosciente delle tecnologie.

Alla luce delle conclusioni su riportate, rivendicando chi scrive la necessità di diffondere l'utilizzo delle tecnologie di autotutela nel più ampio numero di individui, è auspicabile che i programmi didattici e

formativi delle istituzioni pubbliche e private italiane e dell'Unione Europea prevedano strumenti per la proposizione, già quantomeno dal periodo delle scuole secondarie inferiori, della tematica dell'educazione alla cittadinanza digitale e all'uso cosciente e responsabile delle tecnologie dell'informazione.

Secondo un modello, per il momento in fase di schema indicativo, suddiviso per età anagrafica e per professione o ruolo sociale, gli elementi centrali nella proposizione di tali programmi andranno individuati nelle diverse problematiche più sensibili alla luce delle esigenze giuridiche e sociali individuate. In particolare:

- *per i soggetti di minore età*, la formazione dovrà essere orientata all'insegnamento, dal punto di vista tecnologico, delle implicazioni sottostanti all'utilizzo delle ICTs e, dal punto di vista giuridico, delle problematiche nascenti dal rapporto tra diritti propri e diritti altrui, ponendo in rilievo i concetti di responsabilità, danno, scelta, volontà e riflessione. Quanto al primo aspetto, i giovanissimi nativi digitali, e presto la generazione *touch*, pur disponendo di competenze elevatissime quanto all'utilizzo delle tecnologie per i propri obiettivi, frequentemente non ne conoscono le implicazioni sottostanti, quanto a immediatezza, diffusività e permanenza del tempo dei contenuti diffusi e delle tracce relative all'atto di comunicare o diffondere: il riscontro degli stessi dinnanzi a semplici considerazioni in merito alla distinzione tra le tracce lasciate nel mondo materiale e quelle nel mondo digitale è più efficace di numerose campagne esclusivamente poste sul piano giuridico e dei rapporti sociali. Ciò detto, questo secondo aspetto dev'essere comunque portato ad oggetto di riflessione dei soggetti di minore età: scansando i rischi criminogeni insiti nell'approcciare soggetti

adolescenti o preadolescenti su tematiche relative al rapporto tra doveri, obblighi e divieti, è importante porre in rilievo il rapporto tra esercizio delle libertà e responsabilità quanto alle conseguenze di tale esercizio, ben rappresentando la differenza tra la percezione goliardica di un fatto e l'esito dannoso e pregiudizievole dello stesso nella vittima, con complessiva spinta verso un approccio caratterizzato da riflessività. Pochi secondi di dubbio e riflessione possono infatti evitare danni e responsabilità molto più gravi di quanto un soggetto di minore età possa rappresentarsi;

- *per i soggetti universitari*, la formazione può e dev'essere molto più approfondita. Pur nella consapevolezza che, allo stato, il punto precedente non è affrontato nella generalità dei sistemi scolastici e sarebbe dunque opportuno premetterlo in sede di qualsivoglia formazione all'informatica giuridica, il percorso deve portare più lontano, sia dal punto di vista tecnologico che dal punto di vista giuridico. Quanto al primo aspetto, la formazione deve comportare l'insegnamento delle pratiche di autotutela della propria identità e delle informazioni di cui si dispone attraverso le pratiche di cifratura, comunicazioni anonime, cancellazione sicura dei dati, utilizzo di supporti LIVE, conoscenza delle funzioni dei dispositivi e dei servizi chiusi e proprietari quali *geotagging*, profilazione e *cloud computing*, e nel complesso di un *human behavior* orientato in funzione di una previa valutazione del rischio. Dal punto di vista giuridico, la formazione dovrà essere calibrata in relazione al percorso sul quale si va ad incidere: se si tratta di giuristi, la formazione dovrà essere il più dettagliata e profonda possibile, con stimolo al dibattito e alla presa di posizione in un contesto caratterizzato da incertezza e

mutevolezza; se invece si tratta di universitari non giuristi, la formazione andrà focalizzata sulle esigenze del rapporto tra i diritti fondamentali individuali propri della globalità degli individui e sulle normative rilevanti nelle professioni verso le quali è diretto il percorso universitario, e si pensa in particolare alle professioni medico-sanitarie e alle professione giornalistiche;

- *per i soggetti genitori*, la formazione va elaborata con la finalità di sviluppare e valorizzare capacità didattiche e pedagogiche nei confronti dei soggetti di minore età, permettendo così di anticipare persino la soglia di età della formazione all'uso cosciente delle tecnologie, con l'approfondimento dunque delle tematiche di cui al primo dei punti di questo elenco: implicazioni tecnologiche relative alla immediatezza, alla diffusività e alla permanenza dei dati e delle trasmissioni digitali; implicazioni sociali del rapporto tra diritti e libertà individuali e responsabilità per i rischi posti in essere e i danni determinati;
- *per i soggetti lavoratori o professionisti*, infine, una formazione all'uso cosciente delle tecnologie dev'essere distinta per categorie in base alle diverse esigenze delle stesse, pur *ponendo come elemento assolutamente centrale e preminente la valutazione del rischio* - e in questo senso l'abolizione dell'obbligo del Documento Programmatico sulla Sicurezza a seguito delle riforme della normativa sulla protezione dei dati personali, benché lo strumento fosse foriero di fraintendimenti, fu una scelta adottata nella direzione sbagliata. Tale valutazione dev'essere svolta anche nel rapporto con datori di lavoro, collaboratori, associazioni di categoria, attori istituzionali e altri soggetti operanti nel medesimo settore. Si dovrebbe dunque individuare il tipo di rischio di ogni settore, che ben

comprensibilmente sarà diverso nel caso si tratti di dati fiscali per la fatturazione di opere e vendita di prodotti comuni, piuttosto che di dati relativi ad attività di giornalismo d'inchiesta o ancora dati giudiziari trattati da avvocati, magistrati e collaboratori e ausiliari dei giudici, per poi impostare i sistemi informatici e l'approccio umano al loro utilizzo di conseguenza, prevedendo il ricorso a una o più pratiche tra quelle descritte nel capitolo precedente.

Auspicando dunque che le istituzioni preposte all'elaborazione dei programmi didattici, e non solo, e le organizzazioni anche non istituzionali finalizzate alla diffusione della cultura digitale, così come gli *hacker* stessi, volgano attenzione e risorse verso la carente cittadinanza digitale, e che il dibattito sul rapporto tra libertà e sicurezza si spogli, rapidamente, della retorica securitaria che ha dominato il panorama culturale degli ultimi lustri, si ritiene di poter chiudere questo *excursus* richiamando nuovamente Norberto Bobbio il quale, nel suo saggio Politica e Cultura, ebbe modo di affermare che “il compito degli uomini di cultura è più che mai oggi quello di seminare dei dubbi, non già di raccoglier certezze”. Nel contesto della società dell’informazione, l’arte del dubbio è requisito fondamentale sia per i giuristi, dell’informatica e non solo, sia per gli *hacker* e gli *hacktivisti,* che l’hanno frequentemente tradotto, nel mondo digitale, con l’invito, forse di più difficile condivisione ma certamente adatto al proprio contesto operativo, ad un sano esercizio di paranoia.

BIBLIOGRAFIA FONDAMENTALE

AA.VV., *2010 Circumvention Tool Usage Report*, a cura del *Berkman Center for Internet & Society at Harvard University* .

AA.VV., *A Human Rights Perspective on Citizen Participation in the EU's Governance of New Technologies* in *Human Rights Law Review* 10(4): 661–688, 2010.

AA.VV., *Extreme Speech and Democracy*, in *Oxford University Press*, New York, 2009.

AA.VV., *Freedom of Connection – Freedom of Expression The Changing Legal and Regulatory Ecology Shaping the Internet*, in *UNESCO Publishing*, 2010.

AA.VV., *Internet Use and Civic Engagement: A Longitudinal Analysis*, in *The Public Opinion Quarterly* 67(3): 311–334, 2003.

AA.VV., *The blog versus big brother: new and old information technology and political repression*, 1980–2006 in *The International Journal of Human Rights* 15(8): 1315–1330, 2010.

ALU F., *Caso "The Pirate Bay": la parola della Cassazione su file sharing e peer-to-peer*, del 11.02.2010, in *Altalex.*

AMATO G., *Il potere e l'antitrust*, Il Mulino, Bologna, 1999.

ANZERA G. ,COMUNELLO F., *Mondi digitali. Riflessioni e analisi sul Digital Divide*,: Guerini Associati, Milano, 2005.

BAKAN J., *The Corporation: the pathological pursuit of profit and power*, Simon & Schuster, 2004.

BASSOLI, *La disciplina giuridica della seconda vita in Internet. L'esperienza Second Life* in *Informatica e diritto*, 2009, 1 pp. 165-189.

BAUMANN Z., *Dentro la globalizzazione. Le conseguenze sulle persone*, Laterza, Roma-Bari, 1998.

BECK U., *Che cos'è la globalizzazione. Rischi e prospettive della società planetaria*, Carocci, Roma, 1999.

BECK U., *L'era dell'e*, Asterios, Triestre, 2001.

BEDUSCHI, *Caso Google: libertà d'espressione* in *Internet* e *tutela penale dell'onore e della riservatezza* (nota a Trib. Milano 12 aprile 2010) in Il Corriere del Merito, 2010, 10, pp. 963-970

BENKLER Y., *A Free Irresponsibile Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, in *Harvard Civil Rights-Civil Liberties Law Review* 46: 311–397, 2011.

BENKLER Y., *Communications Infrastructure Regulation and the Distribution of Control Over Content*, in *Telecommunications Policy* 183, 1998.

BENKLER Y., *Law, Policy and Cooperation* in *Government and Markets: Toward a New Theory of Regulation*, E. Balleisen & D. Moss eds., Cambridge University Press, 2009.

BOBBIO N, *L'età dei diritti*, Einaudi, Torino, 1990.

BONGIOVANNI G., *Costituzionalismo e teoria del diritto*, Laterza, Roma-Bari, 2005.

BORIS MENGHI C. (a cura di), *Sovranità e diritto*, in *Teorie del diritto e della politica*, Giappichelli, Torino, 2004.

CASSESE S., *Il diritto globale. Giustizia e democrazia oltre lo stato*, Einaudi, Torino, 2009

CHELI E., *La Costituzione italiana tra storia e politica*, Il Mulino, Bologna, 2012.

CORRIAS LUCENTE G., *Internet e libertà di manifestazione del pensiero* in *Diritto dell'informazione e dell'informatica*, 2000, pp. 597-608.

CRITICAL ART ENSEMBLE, *Digital Resistance: Explorations in Tactical Media*, Autonomedia, 2001.

CRITICAL ART ENSEMBLE, *Electronic Civil Disobedience and Other Unpopular Ideas*, Autonomedia, 1996.

CUCEREANAU G., *Aspects of Regulating Freedom of Expression on the Internet*, Intersentia, 2008.

DAHLBERG L., *Pirates, Partisans, and Politico-Juridical Space* in *Law and Literature* 23(2): 262–281, 2011.

D'ALBERTI M, *Poteri pubblici, mercati e globalizzazione*, Il Mulino, Bologna, 2008.

D'ANDREA A., GUIGLIA G., ONIDA V., *L'ordinamento costituzionale italiano*, Torino, Utet, 1990.

DE AZEVEDO CUNHA M.V., MARIN L., SARTOR G., *Peer-to-Peer Privacy Violations and ISP Liability: Data Protection in the User-Generated Web* in *International Data Privacy Law*, 2012.

DE FILIPPI P., MCCARTHY S., *Cloud computing: legal issues in centralized architectures*, in *Neutralidad de la red y otros retos para el futuro de Internet*, p. 225, dagli Atti del VII Congresso Internazionale su *Internet*, Diritto e Politica, 12-13 luglio 2011, *Universitat Oberta de Catalunya.*

DE ROSA V, *La formazione di regole giuridiche per il "cyberspazio"*, in *Diritto dell'informazione e dell'informatica*, 2003, pp. 361-400.

DELITALA G., *I limiti giuridici alla libertà di stampa* , in *Iustitia*, 1959.

DE NARDIS L., nel recente paper *Internet Points of Control as Global Governance*, CIGI, 2013, http://www.cigionline.org/sites/default/files/no2_3.pdf.

DIENER M.C., *Il contratto in generale*, Giuffrè, Milano, 2011.

DI LELLO C., *Internet e Costituzione: garanzia del mezzo e suoi limiti* in *Diritto dell'informazione e dell'informatica*, 2007, pp. 895-915.

DIAMOND L., *Liberation Technology*, in *Journal of Democracy* 21:69-83, 2010.

DIAMOND L., PLATTER M., *Liberation Technology: Social Media and the Struggle for Democracy*, *The Johns Hopkins University Press*, 2012.

DOSSENA G., *Le privatizzazioni delle imprese. Modalità, problemi e prospettive*, EGEA, Milano, 1990.

DWORKIN R., *Freedom's Law. The Moral Reading of the American Constitution*, Cambridge, Harvard University Press, 1996, p. 1-38.

ESPOSITO C., *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Giuffré, Milano, 1958.

FACCI, *La responsabilità dei providers*, in ROSSELLO, FINOCCHIARO, TOSI (a cura di), *Commercio elettronico*, Giappichelli, Torino, 2007.

FALLETTI E., *I diritti fondamentali su Internet. Libertà di espressione, privacy e copyright*, Exeo, Padova, 2011.

FERRARESE M. R., *Il diritto al presente*, Il Mulino, Bologna, 2002.

FERRARESE M. R., *Le istituzioni della globalizzazione. Diritto e diritti nella società transnazionale*, Il Mulino, Bologna, 2000.

FINOCCHIARO G. (a cura di), *Diritto all'anonimato: anonimato, nome e identità personale*, Cedam, Padova, 2008.

FOIS S., *Princìpi costituzionali e libera manifestazione del pensiero*, Milano, 1957.

GALLI C., *Spazi politici. L'età moderna e l'età globale*, Il Mulino, Bologna, 2001

GIANFORMAGGIO L., *L'argomentazione della Costituzione tra applicazione di regole ed argomentazione basata su principi*, in *Filosofia del diritto e ragionamento giuridico*, G. Giappichelli, Torino, 2008

GRISOLIA G., *Libertà di manifestazione del pensiero e tutela penale dell'onore e della riservatezza*, CEDAM, Padova, 1994.

GROSSI P., *Globalizzazione e pluralismo giuridico*, in Q*uaderni fiorentini per la storia del pensiero giuridico moderno*, fasc. 29, Giuffré, Milano, 2000

HANDS J., *@ Is For Activism: Dissent, Resistance And Rebellion In A Digital Culture*, *Pluto Press*, London, 2010

HELD D., *Governare la globalizzazione. Un'alternativa democratica al mondo unipolare*, Il Mulino, Bologna, 2005.

HOPKINS J., *Excavating Toronto's Underground Streets: In Search of Equitable Rights, Rules and Revenue*, in *City Lives and City Forms*, University of Toronto Press, 1996

IASELLI M, *Caso "about Elly": non convincono le conclusioni del giudice cautelare*, in Altalex, 9.11.2011

JAEGER P.G., DENOZZA F., TOFFOLETTO A., *Appunti di di diritto commerciale*. *Impresa e società*, Giuffré, Milano, 2010, p. 52.

JANSEN R., TSCHORSCH F., JOHNSON A., SCHEUERMANN B., *The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network*, in *21st Annual Network & Distributed System Security Symposium*, 2014.

JAMES J. *Digital Divide Complacency: Misconceptions and Dangers*, in *The Information Society*, 24, 54-61, 2008, Indiana University

JURIS J. S., *The New Digital Media and Activist Networking within Anti-Corporate Globalization Movements* in *Annals of the American Academy of Political and Social Science* 597: 189–208, 2005

KELSEN H., *Lineamenti di dottrina pura del diritto*, a cura di TREVES R., Torino: Einaudi, 1952.

KELSEN H., *La dottrina pura del diritto*, Torino, Einaudi, 1966.

KLEIN N., *No Logo*, Baldini e Castoldi, Milano 2001.

LESSIG L., *Code v2.0*, Basic Books, New York, 2006.

LESSIG L., *Cultura Libera*, Apogeo, Milano, 2005.

LOPEZ-TARRUELLA (a cura di), *Google and the Law* in *Information Technology and Law Series* V. 22, 2012.

LUPARIA L.. (a cura di), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Giuffrè, 2012.

LUZZATTO G., *Lega Anseatica*, in *Enciclopedia italiana Treccani*, vol .III, pp. 426-428, 1929.

MARTUFI R., VASAPOLLO L., *Le diverse forme di privatizzazione*, http:// proteo.rdbcub.it/article.php3?id_article=18#nb2

MASSARONN ROSS M., SMITH L., PRITT R., The *Zoning Process: Private Land-Use Controls and Gated Communities: The Impact of Private Property Rights Legislation, and Other Recent Developments in the Law, Urban Lawyers*, v. 28, 1996.

MAYER-SCHONBERGER V., *Delete. Il diritto all'oblio nell'era digitale*, EGEA, Milano, 2010.

MCLUHAN M., *Gli strumenti del comunicare*, Il Saggiatore, Milano, 1966

MORTATI C., L*a costituzione in senso materiale*, Giuffré, Milano, 1942.

MOSTACCI E., *La soft law nel sistema delle fonti: uno studio comparato*, CEDAM, Padova 2008.

MUELLER M., *Ruling the root: Internet governance and the taming of cyberspace*, in MIT Press, California, 2004.

MULA D., *Responsabilità del motore di ricerca nel caso About Elly: fraintendimenti informatici a base di un'ordinanza (revocata) dal contenuto anomalo*, in *Diritto Mercato e Tecnologia*, e in *Responsabilità Civile*, in corso di pubblicazione.

NUNZIATO D., *Virtual Freedom: Net Neutrality and Free Speech in the Internet Age*, Stanford University Press, 2009.

OSTREICH G., a cura di G. Gozzi, *Storia dei diritti umani e delle libertà fondamentali*, Roma, Laterza, 2001.

PACE A., *Problematica delle libertà costituzionali*, Cedam, Padova, 2003.

PALADIN L., *Per una storia costituzionale della Repubblica Italiana*, Il Mulino, Bologna, 2004.

PARIOTTI E., *La comunità interpretativa del diritto*, Giappichelli, Torino, 2000.

PARIOTTI E., *La giustizia oltre lo stato: forme e problemi*, Giappichelli, Torino, 2004.

PASQUINO, *Servizi telematici e criteri di responsabilità*, Giuffrè, Milano, 2003.

PECES-BARBA G., *Teoria dei diritti fondamentali*, Giuffrè, Milano, 1993.

PERRI P., *Privacy, diritto e sicurezza informatica*, Giuffré, Milano, 2013.

PETERS J., *WikiLeaks, the First Amendment, and the Press* in *Harvard Law and Policy Review*, 2011.

PIZZATTI F. (a cura di), *Il caso del diritto all'oblio*, Giappichelli, Torino, 2013

RICCIO, *La responsabilità civile degli Internet providers*, Giappichelli, Torino, 2002.

RICOTTI S., *Fondamento e limiti della responsabilità penale dei Service-providers in Internet*, in *Diritto penale e processo*, 1999.

RICOTTI S., *La responsabilità penale dei Service-providers in Italia*, in *Diritto penale e processo*, 1999.

RODOTÁ S., *Internet: né censura né anarchia selvaggia*, Telèma, 1996, http://www.geocities.com/centrotobagi/news2.htm.

SARTOR G., *Providers' Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?* in *International Data Privacy Law*, 2013.

SARTOR G., *Social networks e responsabilita del provider*, in *Annali italiani del diritto d'autore, della cultura e dello spettacolo*, 2012.

SEMINARA S:, *La responsabilità penale degli operatori su Internet*, in *Diritto dell'Informazione e dell'Informatica*, 1998, pp. 441-458.

SPARROW A., *The Law of Virtual Worlds and Internet Social Networks*, Gower, 2010.

STIGLIZ J., *La globalizzazione che funziona*, Einaudi, Torino, 2006.

TEUBNER G. *Global Law without a State*, Darthmouth, 1996.

TEUBNER G. *La cultura del diritto nell'epoca della globalizzazione*, Armando, Roma, 2005.

TEUBNER G. *Law as an Autopoietic System*, Blackwell, 1993.

TEUBNER G. *Transnational Governance and Constitutionalism*, Hart, 2004.

VECCHIOLI L., *Il rischio della sovranità globale*, Giappichelli, Torino, 2004.

VOLANTE R. (a cura di), *Soft law e hard law nelle società postmoderne*, Giappichelli, Torino, 2009.

WIENER N., *Cybernetics, or Communication and Control in the Animal and the Machine*, in *MIT Press*, Cambridge, 1948.

WU T., *Network Neutrality, Broadband Discrimination*, in *Journal of Telecommunications and High Technology Law*, 2.2, 2003.

ZAGREBELSKY G., *Il diritto mite*, Einaudi, Torino, 1992.

ZAGREBELSKY G., *Manuale di diritto costituzionale, I, Le fonti del diritto*, Utet, Torino, 1988.

ZAGREBELSKY G:, MARCENO V., *Giustizia costituzionale*, Il Mulino, Bologna, 2012.

ZENO ZENCOVICH V., *Informatica ed evoluzione del diritto*, in *Diritto dell'informazione e dell'informatica*, 2003, pp. 89-93

ZENO ZENCOVICH V., *La libertà d'espressione. Media, mercato, potere nella società dell'informazione*, Il Mulino, Bologna, 2004

ZENO ZENCOVICH V., *Freedom of Expression. A Critical and Comparative Analysis*, Routhledge-Cavendish, 2008.

ZICCARDI G., *La libertà d'espressione in Internet al vaglio della Corte Suprema degli Stati Uniti*, in *Quaderni costituzionali*, 1998, pp.123-134.

ZICCARDI G., *Crittografia e diritto*, G. Giappichelli, Torino, 2003.

ZICCARDI G., *Informatica, diritti e libertà*, Mucchi, Modena, 2005.

ZICCARDI G., *Libertà del codice e della cultura*, Giuffrè, Milano, 2006.

ZICCARDI G., *Informatica Giuridica, Vol. 2: Privacy, sicurezza informatica, computer forensics e investigazioni digitali*., Giuffré, Milano, 2008.

ZICCARDI G., *Hacker. Il richiamo della libertà*, Marsilio, Venezia, 2011.

ZICCARDI G., *L' avvocato hacker. Informatica giuridica e uso consapevole (e responsabile) delle tecnologie*, Giuffré, Milano, 2012.

ZICCARDI G., *Resistance, Liberation Technology and Human Rights in the Digital Age, Law, Governance and Technology Series* 7, Springer, Netherlands, 2013.