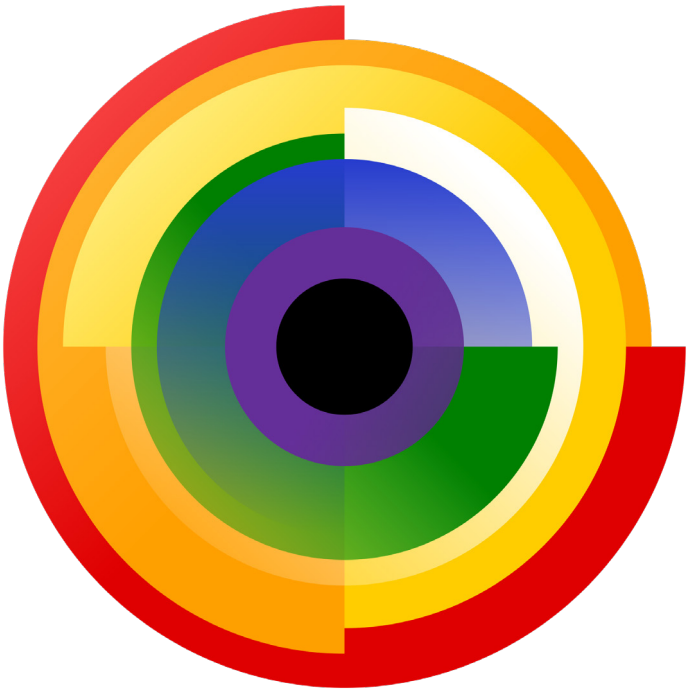
CITTADINANZA DIGITALE E TECNOCIVISMO

IN UN MONDO DIGITALE LA CITTADINANZA INIZIA DAI BIT

VOLUME PRIMO

Andrea Trentini, Giovanni Biscuolo, Andrea Rossi



Ledizioni

Edito da Ledizioni (*http://ledizioni.it*)
Collana Copyleft-Italia.it (*http://copyleft-italia.it*)

ISBN:
9788855261609 (versione cartacea)
9788855263481 (versione digitale)

Indice

Prefazioni

Matteo Ruffoni

Illuminista
Presidente Wikimedia Italia

Leggere questo libro è stato come sbirciare, saltellando, in una stanza dalla finestra al piano terra che da sulla strada. Non so se le mie competenze sono adeguate a scrivere una prefazione, moltissime sono le citazioni e tante le conoscenze e competenze richieste per una lettura efficace. Quello che so mi permette di "guardare dentro" solo per brevi istanti al culmine dei miei salti.

I miei amici informatici usano gli acronimi con una tale frequenza che mi sono sempre chiesto se per caso non usino il codice fiscale come nomignolo nei momenti di intimità.

Ho letto e riletto il libro e devo ammettere che inquadra in modo estremamente particolareggiato lo stato dell'arte della situazione della struttura della rete, della sua accessibilità, della sua neutralità, della ricchezza… e chiarisce piuttosto bene quali sono i pericoli che la piena partecipazione alla vita democratica, comprensiva della totale fruizione dei propri diritti, sta correndo a causa delle storture alle quali sono sottoposte la distribuzione e la configurazione della stessa Internet, nonché la presenza di contenuti poco attendibili.

Mi è sembrato di essere in una fiera: tutte le bancarelle, i paragrafi, esponevano merce, che però andava

poi acquistata, approfondita, leggendo anche attentamente le numerose note a piè pagina, fortunatamente spesso corrispondenti a pagine di Wikipedia, e quindi facilmente reperibili.

Ho un po' faticato a comprendere la metafora *protocollo* $\leftrightarrow$ *arcobaleno*, ho sempre pensato ad un protocollo, come il TCP/IP, come ad una cipolla, uno strato dentro l'altro piuttosto che ad un arcobaleno.

Ho maggiormente apprezzato e compreso molto meglio il metodo spettrografico, probabilmente per un malinconico ricordo del corso di Astronomia all'università, vero che di un contesto lo "spettro" proposto evidenzia molto bene punti di forza e carenze.

Mi pare molto importante inoltre il manifesto schierarsi «... dalla parte giusta della storia ...» permettendo così al lettore di comprendere le ragioni, e sono tante, degli autori. Questo schierarsi di fatto non è altro che cercare di valutare il fenomeno rete, questa fantastica interconnessione tra esseri umani, cercando di preservare alcuni valori condivisi importanti, il diritto all'informazione, alla comunicazione neutrale, che, di fatto, nella rete senza controllo si perdono, spesso senza che nemmeno ci se ne accorga.

Il primo capitolo si occupa di come *funziona* Internet, di come viaggiano le informazioni, e di come la loro mobilità può essere modificata rallentata o velocizzata, di fatto influenzata, se un sito si carica lentamente non viene letto, e, sebbene non in modo dettagliato, riesce a mettere in guardia un lettore come me sul fatto che non tutte le informazioni viaggiano in rete alla stessa velocità, cosa che potevo immaginare anche prima, ma che queste distorsioni non sono visibili chiaramente, nè tantomeno palesi rispetto all'utente. Non si può sapere a priori se per andare da Milano a Roma abbiamo scelto un autobus o una bicicletta, lo si può scoprire solo *vivendo* (navigando), ma questo ha conseguenze nefaste sulla comunicazione e l'informazione di massa, e gli autori ci forniscono il *catalogo delle guide e dei manuali* sui quali dobbiamo andare ad informarci se vogliamo veramente usare Internet in modo consapevole

sia come singoli, ma soprattutto come cittadini.

Senza che nessuno ne abbia a male, e garantendo che l'ho letto tutto il libro, mi permetto di saltare direttamente al capitolo 3 che ha per tema l'aspetto educativo (L3-education) dove dopo una sacrosanta difesa della crittografia come *naturale estensione* digitale della privacy si mettono in evidenza i rischi connessi all'utilizzo di solo codice compilato, in sostanza nascosto, cosa che ha una sua soluzione nell'utilizzo di software libero a sorgente aperto, soprattutto nei casi di programmi delicati ad esempio le *app* necessarie al tracciamento dei contatti per i casi di contagio da COVID-19 come Immuni, fortunatamente software libero.

Si sorride amaramente a leggere di quel giudice che «… non può sottolineare lo schermo del computer …», purtroppo riconoscendo in quel giudice insegnanti, dirigenti, pezzi importanti del mondo della scuola italiana, e poi il sorriso si spegne scorrendo velocemente le innumerevoli graduatorie di progresso nelle quali il nostro paese compare troppo spesso in posizioni di coda.

L'analisi del PNSD è un po' ingenerosa, ma in fondo corretta, anche se ingenuamente chiede ad un piano per la scuola di esplicitare i «… metodi per misurarne l'effettiva realizzazione …» dimenticandosi che nessuna riforma nel mondo della scuola italiana ha mai avuto modo di verificare i propri risultati, e forse nessuna riforma è nemmeno mai riuscita, e dimenticandosi anche che siamo in Italia, il paese dei principi affermati ma poi poco realizzati.

Mi ha commosso infine l'accorato appello a favore delle licenze libere, sicuramente una delle vie maestre per la difesa del sapere e del diritto di tutti ad accedervi, sono anche io da questa *parte del fronte* ed è assolutamente corretto cercare di fornire il massimo delle informazioni possibili a riguardo, ma, forse, il nostro impegno si rivela velleitario poiché il "nemico" è troppo potente e il nostro approccio troppo tecnico ed intellettuale.

Speriamo però che, almeno la scuola, si renda al più presto consapevole che vanno formati futuri cittadini di-

gitali e che riesca a trasformare il passeggero *flirting* con il *coding* con un più robusto inserimento nelle competenze scolastiche di quelle di cittadinanza digitale. Un libro come questo può, come ho scritto sopra, fare da compendio per quello che si deve sapere, o almeno sapere di non sapere del tutto, in modo da essere consapevoli e potrebbe risultare molto utile a qualche dirigente.

Buona lettura a tutti.

Giovanni Ziccardi

Professore
Università degli Studi di Milano

Cosa significa, oggi, essere un buon cittadino digitale in una società che è completamente mutata a una velocità incredibile e che continua a cambiare pelle ogni giorno?

Come noterà il lettore di questo appassionante libro, che ripercorre con cura (anche) la storia delle tecnologie che oggi permeano la nostra quotidianità, può significare tante cose. Sono tutte egualmente importanti, sia per un uso responsabile delle tecnologie che ormai ci circondano in ogni momento, sia per relazionarsi con gli altri utenti digitali in maniera corretta.

Il cittadino digitale, in estrema sintesi, è quello che vive immerso nella società digitale, ossia in una società che accanto alle relazioni "fisiche" tra le persone vede anche delle relazioni digitali, generate da impulsi, da messaggi, da giochi, da servizi, da App e da piattaforme, nonché dai quartieri e città "intelligenti" che ci accolgono.

Nella società digitale, ovviamente, bisogna comportarsi con correttezza esattamente come avviene nella società "fisica".

Un buon cittadino digitale è quindi, prima di tutto, un cittadino che rispetta la legalità, l'affettività e l'empatia nella società "tradizionale" e tiene gli stessi, identici comportamenti anche durante la sua attività online.

Stefano Rodotà è stato tra i primi studiosi in Europa a delineare questo aspetto della vita delle persone nella società digitale, sin dai primi collegamenti in rete, quanto tutto era nuovo e sembrava di essere in un Far West, in una "nuova frontiera elettronica" che consentiva per la prima volta possibilità incredibili ma che presentava, anche, grandi rischi. E queste origini, fondamentali per comprendere l'evoluzione sino a oggi, sono ben approfondite nella prima parte del libro.

Rodotà individuò, innanzitutto, tre aspetti centrali di

questo "nuovo" mondo: i) un nuovo ambiente dove esercitare i propri diritti quando si è online e connessi, ii) l'idea di un corpo elettronico che ha ciascuno di noi (una specie di profilo che ci rappresenta nell'ambiente digitale) e iii) un diritto sui dati che immettiamo in rete affinché non siano controllati da altri soggetti contro la nostra volontà.

Quali sono, allora, gli aspetti più interessanti della società tecnologica dove noi operiamo come nuovi cittadini, come utenti che anche per otto/dieci ore al giorno vivono in rete, creano relazioni, comprano prodotti, usano servizi o guardano film e video?

Il primo aspetto è sicuramente il diritto alla privacy, ossia a che i nostri dati siano in qualche modo protetti e che non siano sfruttati contro la nostra volontà.

Uno dei primi diritti del cittadino digitale è anche in Italia, quindi, quello di veder rispettata la propria privacy, un diritto di essere lasciati soli che fin dalla fine degli anni Novanta del secolo scorso è riconosciuto in Europa.

Questo primo diritto è un vero e proprio diritto a "governare le proprie informazioni" in un ambiente tecnologico e sociale che prende i nostri dati e li tratta spesso a nostra insaputa.

Si pensi alla profilazione che subiamo quando vogliamo comprare un bene su una piattaforma, o quando guardiamo un film in streaming, o quando navighiamo e il sistema tiene traccia delle nostre preferenze, di ciò che abbiamo guardato e spesso è anche in grado di prevedere che cosa guarderemo di lì a poco.

Il diritto alla privacy, primo e imprescindibile, si accompagna ad altri diritti di libertà che costituiscono una vera e propria cittadinanza elettronica, dove i valori della nostra Costituzione - libertà, eguaglianza tra le persone, dignità e democrazia - prendono vita e trovano una nuova espressione nel mondo online.

In questa società digitale, per prima cosa dovrebbero essere tutelati i principi di eguaglianza, che si ottengono proteggendo i cittadini dalla discriminazione causata da un trattamento non corretto dei nostri dati.

I cittadini devono essere tutelati nelle loro informazioni, devono essere rispettate le loro opinioni, il loro credo religioso, le condizioni di salute, perché senza una protezione di questi dati, tali informazioni possono essere utilizzate per fare del male alle persone e per escluderle dalla vita in società e, soprattutto, per non farle partecipare alla vita di tutti i giorni.

In questo caso, diventa importante l'idea di "corpo elettronico", ossia come noi ci presentiamo online, con che profilo, modo di parlare, modo di interagire con gli altri utenti. Secondo Rodotà, ad esempio, il corpo elettronico deve avere la stessa protezione del corpo fisico.

In questo quadro, a nostro modesto ma fermo avviso, la sorveglianza è, oggi, la minaccia più grande.

Mentre noi agiamo online, il sistema, le piattaforme, le app, i Governi e le multinazionali tengono sotto controllo tutto ciò che noi facciamo e possono usare queste informazioni per danneggiarci. Società anche a noi sconosciute possono raccogliere informazioni su di noi e classificarci, inserirci in determinare categorie che possono condizionare la nostra vita quotidiana.

Purtroppo, però, sono spesso gli utenti a esibire i loro dati, a comunicare informazioni su loro stessi, ad essere spregiudicati e diffondere informazioni, fotografie o video che, poi, possono essere raccolte e usate contro di loro.

Siamo in una *società dell'esibizione*, dove il dato è comunicato direttamente dall'utente senza prevederne, però l'utilizzo successivo. Tanto che molti studiosi parlano di una "morte della privacy" causata dall'utente stesso che non vuole tenere segreti i propri dati ma li diffonde senza problemi.

In realtà, dice Rodotà, proprio l'esibizione continua dei nostri dati ci porta a riflettere sulla necessità di una loro protezione, ossia la volontà di chiudersi e di considerare continuamente quali e quanti dati che ci riguardano siano trattati in ogni momento.

Il potere di controllo sui nostri dati, nel sistema di tecno-civismo delineato puntualmente nel libro, è a nostro

avviso centrale.

Purtroppo questa attività di controllo sui propri dati non è affatto semplice, in quanto non sempre si conosce quali siano i dati raccolti e chi li raccolga, sia in ambito privato, sia in ambito pubblico. E tutto sta accadendo in un momento in cui è in corso una rivoluzione digitale che non ha precedenti.

Ecco allora che si viene a delineare in maniera chiara questa figura di "cittadino digitale" che pian piano costruisce la sua persona online, sui siti web, sulle piattaforme e nelle App utilizzate quotidianamente.

Il cittadino digitale deve quindi operare in un ambiente dove i suoi diritti possono essere messi in pericolo.

Sono diritti fragili, che possono essere attaccati soprattutto "etichettando" le persone in base ai loro dati anche quando le tecnologie sembrano positive, sembrano degli "Angeli Custodi" che però, allo stesso tempo, ci stanno osservando e catalogando insieme ai nostri dati.

Come è noto, il buon cittadino digitale non ha una "Costituzione" da seguire, ma molti Stati hanno elaborato dei principi specifici per la vita online che sono molto interessanti.

L'Italia è stata uno dei primi Paesi al mondo ad elaborare una Carta dei Diritti di Internet, sempre grazie al lavoro prezioso di Stefano Rodotà. La Carta dei Diritti contiene dieci regole importanti, e anch'esse possono contribuire al buon cittadino digitale e ai suoi comportamenti. Di alcune di queste regole e principi si parla diffusamente, come il lettore noterà, in questo libro.

Si pensi, innanzitutto, al *diritto di accesso*. Tutti dovrebbero poter accedere, oggi, a Internet. Soprattutto le persone più povere, gli emarginati, gli abitanti di Paesi che non sono ricchi come gli Stati occidentali. Collegarsi alla rete è fondamentale per la cultura, per i contatti, per allargare gli orizzonti e conoscere nozioni e abitudini che, grazie alla contaminazione, ci aiutano a crescere e a migliorare. Collegandosi a Internet, ogni persona riesce a garantirsi un pieno sviluppo individuale e sociale.

Vi è, poi, l'aspetto di un *diritto alla conoscenza* e all'educazione in rete. Oltre all'accesso, tutti dovrebbero conoscere a fondo come funziona la società digitale, soprattutto per esercitare i suoi diritti. E tale educazione al digitale dovrebbe arrivare soprattutto dalla scuola e dalle istituzioni.

Nelle pagine che seguono si tratta, poi, del fondamentale aspetto della neutralità della rete. I contenuti che circolano in rete, le informazioni, i dati, non devono essere discriminati o bloccati, ma la persona deve essere in grado di ricevere qualsiasi tipo di informazione per avere un'idea corretta di ciò che accade.

Un diritto fondamentale, si è già visto, è anche la protezione dei propri dati personali, in un'ottica di tutela della dignità, identità e riservatezza, soprattutto sulle piattaforme o con smartphone e dispositivi che generano facilmente informazioni.

Anche il diritto alla inviolabilità dei sistemi, dei dispositivi e dei "domicili informatici" rende chiara l'importanza del principio della protezione dei propri dati, dei propri sistemi e del cosiddetto domicilio informatico. I nostri dati informatici è come se fossero dentro al nostro "domicilio", e nessuno dovrebbe poter entrare per leggerli, modificarli o rubarli.

Circa il diritto all'identità, centrale diventa l'identità con la quale ci presentiamo in rete, che deve essere aggiornata e rappresentare correttamente la nostra personalità, soprattutto in un'epoca storica dove gli algoritmi ci profilano con sempre maggior cura e sono in grado di rappresentare diverse identità.

Importante è, anche, la possibilità dell'*oblio*, ossia di rimuovere a un certo punto i propri dati, affinché non rimangano in eterno. Centrale, sul punto, è la procedura di de-indicizzazione, ossia il far sì che alcuni dati non siano più indicizzati dai motori di ricerca e non appaiano, quindi, all'atto di effettuare una ricerca in Google o in altri servizi simili.

Un tema "caldissimo", correlato ai diritti del cittadino

digitale, riguarda le garanzie delle persone sulle piattaforme. L'attività quotidiana è, oggi, su grandi piattaforme e con app che permettono nuovi mezzi di comunicazione. Anche in questo caso, sono molti i diritti che vanno rispettati.

Le infrastrutture utilizzate dovrebbero, poi, essere *protette* per garantire la sicurezza degli utenti, ed è un interesse pubblico che le reti e le piattaforme siano sicure e non possano essere attaccate, ad esempio, da criminali informatici. Allo stesso tempo, bisogna proteggere le piattaforme dalla diffusione di odio e discriminazione.

Infine, sul punto della *governance*, Internet dovrebbe rimanere aperta e democratica, per consentire l'esercizio di tutti i diritti, e tutti gli enti mondiali dovrebbero contribuire per una regolazione che sia benefica per tutti gli utenti e rispettosa dei diritti fondamentali.

Nella pagine che seguono, tutti questi argomenti (e altri) sono affrontati con un corretto approccio interdisciplinare e valutando sempre con grande cura gli aspetti tecnici, essenziali per comprendere al meglio anche i risvolti sociali, giuridici e politici.

Introduzione

```
Questo è il nostro contributo
all'abbattimento della
tyranny of not understanding
technology.
```

La definizione di tyranny... in inglese è di Edward Snowden.

Questo testo è dedicato al tema della *Cittadinanza Digitale*, cioè alla declinazione digitale dell'essere *Cittadini* di un mondo sempre più digitalizzato, informatizzato, *computerizzato* dove anche i rapporti tra cittadino e stato, tra clienti e fornitori, tra dipendenti e datori di lavoro cambiano per merito o a causa della tecnologia. In questo contesto è fondamentale per ognuno di noi possedere un modello, delle linee guida, delle conoscenze e degli strumenti per non rimanere spettatori del cambiamento epocale che sta avvenendo.

Le origini

I termini *Cittadinanza Digitale* e *Tecnocivismo* sono, in prima battuta, quelli con cui *abbiamo*[1] battezzato il **corso** di CDT (Cittadinanza Digitale e Tecnocivismo) della Magistrale in Informatica presso l'Università degli Studi di Milano. Nel 2010 maturammo l'idea della necessità per i nostri studenti di acquisire non solo le conoscenze prettamente tecnologiche, ma anche la capacità di fare collegamenti con le influenze delle tecnologie sulla vita di tutti i giorni, in particolare sugli aspetti *civici*, sia nel senso della convivenza sia, soprattutto, in quello più proprio dell'essere cittadini, partecipi di un *sistema*: Comune, territorio, Paese/Nazione o Federazione. Tale consapevolezza è indispensabile sia per cogliere le *opportunità* offerte dalla tecnologia e concretizzarle in conquiste sociali (partecipa-

[1] In questo caso i soggetti sono Fiorella De Cindio e Andrea Trentini, i due docenti (del Dipartimento di Informatica dell'Università degli Studi di Milano) che hanno istituito il corso in oggetto.

zione civica, trasparenza ecc.), sia per mitigare i *rischi* a cui il cattivo uso della tecnologia ci espone (monitoraggio e controllo pervasivi, perdita di privacy ecc.).

Viviamo, infatti, in una società plasmata dalle tecnologie dell'informazione e della comunicazione. Una continua interazione tra gli eventi del mondo fisico e quelli nel mondo digitale chiede all'*homo digitalis* di riconsiderare e rimodellare la sua cittadinanza per far fronte a questo contesto *accresciuto*, in cui i diritti e gli obblighi devono essere adeguatamente declinati per soddisfare sia le opportunità che i rischi derivanti dalle tecnologie digitali. Queste opportunità e questi rischi mettono in discussione l'idea stessa di cittadinanza e l'esercizio dei diritti che ne derivano.

Partiamo dalla *definizione* istituzionale di cittadinanza mutuata dal Ministero dell'Interno[2]:

> *Il termine cittadinanza indica il rapporto tra un individuo e lo Stato, ed è in particolare uno status, denominato civitatis, al quale l'ordinamento giuridico ricollega la pienezza dei diritti civili e politici.*

Una definizione asettica, ma che esplicita subito i *diritti civili e politici* (parola, movimento, voto, petizione ecc.): un cittadino deve godere *pienamente* di tali diritti per potersi definire tale, di conseguenza uno Stato deve garantire la *pienezza di tali diritti* per potersi definire democratico e civile.

Nel mondo moderno molti di questi diritti sono *influenzati*[3] dalla tecnologia. Da quando è stato riconosciuto [Cas96] il ruolo fondamentale delle ICT (*Information and Communication Technologies*) nel modellare la società in tutti i suoi aspetti, dall'economia alla cultura, è emersa anche la loro influenza nel rimodellare la sfera pubblica

[2] *http://interno.gov.it/it/temi/cittadinanza-e-altri-diritti-civili/cittadinanza*

[3] Anche pesantemente, fino all'estremo di casi in cui per poter esercitare un diritto si deve ricorrere a qualche tecnologia digitale, senza alternativa *analogica*.

e i pilastri fondamentali della democrazia [De 00; Sun01; CB09]. Reti sociali che permettono la diffusione delle informazioni (vere e false) in tempo reale, sistemi di partecipazione digitale (dal *crowdsourcing* 🕮 fino al voto online), conoscenza disponibile online in forma libera: sono tutte tecnologie abilitanti, ma siamo capaci di usarle appieno? Quelle tecnologie sono realmente al servizio dei diritti di cittadinanza?

"I cittadini sono più capaci di quanto non fossero in tempi pre-digitali, di mettere in discussione, commentare, sfidare e influenzare coloro che li governano?"[4] [CB09]

Stefano Rodotà, primo presidente dell'Autorità italiana per la protezione dei dati personali e presidente dal 1998 al 2002 del gruppo di coordinamento dei fiduciari per il diritto alla privacy dell'Unione europea, in [Rod15] sottolinea che "Nello spazio globale [digitale], i diritti si espandono e scompaiono (p. 3) [e] la cittadinanza cambia natura (p. 4)", "I diritti… ci parlano di un impegno. Chi li detiene, deve anche essere consapevole del dovere di farli rispettare".

Coleman e Blumler scrivono: "… preferiamo pensare a Internet come uno spazio vuoto di potere che è sia vulnerabile alle strategie centrate sullo stato (e aziendali) sia aperto all'occupazione da parte dei cittadini che hanno pochi altri spazi disponibili per loro di esprimersi in modi democratici costruttivi" [CB09].

Questi autori, esperti nel campo della democrazia digitale e cittadinanza, sono sostanzialmente d'accordo, con parole diverse, nell'assegnare un ruolo fondamentale all'impegno delle persone a lottare per **abbattere i rischi** e **mettere a frutto le opportunità** derivanti dalle tecnologie applicate alla vita civica.

[4] Notare il punto di domanda.

Serve un modello di riferimento

Abbiamo citato diritti e doveri, rischi e opportunità... ma esiste un *modello* onnicomprensivo per inquadrare l'ambito *cittadinanza digitale e tecnocivismo* e descriverlo nei suoi aspetti strutturali? Un'architettura, una chiave di lettura per incasellare concetti, tecnologie, notizie di cronaca? Una sistema di classificazione che permetta una corretta analisi dell'argomento? Uno strumento di ragionamento?

Gli autori di questo testo, in mancanza di un modello soddisfacente in letteratura, ne hanno sviluppato uno definendo il *framework* **Arcobaleno della Cittadinanza Digitale** [DT14; DST12; TD13] proprio per suddividere gli aspetti della cittadinanza digitale in livelli concettuali. Il framework è costituito da strati che vanno dall'accesso alle infrastrutture (reti e servizi) fino al *diritto al coinvolgimento attivo nel processo decisionale*.

Il presente volume è organizzato seguendo il framework livello per livello, richiamando informazioni sulle tecnologie, facendo collegamenti coi fatti della vita quotidiana e descrivendo molti esempi pratici (fatti realmente accaduti e situazioni ipotetiche) di commistione fra tecnologie e cittadinanza *digitale*.

Il modello fornisce un quadro di facile comprensione per discutere della Cittadinanza Digitale, per combinare la visione di coloro che vivono in questo mondo digitale, che devono essere consapevoli dei rischi e delle opportunità, e di quelli che sono *professionisti*, sviluppatori di soluzioni (software o politiche) che - nel bene o nel male - modellano la stessa società: non è un caso che la nostra sia definita *Società dell'Informazione*.

Gli sviluppatori in particolare hanno una grande responsabilità: "La progettazione del software è come l'architettura [...] Il software non è solo un dispositivo con cui l'utente interagisce; è anche il generatore di uno spazio in cui l'utente vive." [Win96]

Le scelte fatte durante la costruzione di soluzioni digitali modellano il *mondo aumentato* [AD08] in cui le persone

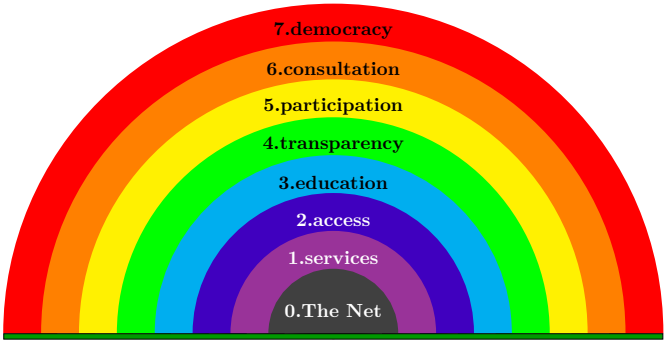


Figura 1: Arcobaleno della Cittadinanza Digitale e Tecnocivismo

vivono e quindi potenziano o limitano le possibilità a coloro che le utilizzano[5], incidendo sui diritti di cittadinanza digitale delle persone. Ad esempio, quando un sindaco o un consigliere comunale intende *comunicare* con i cittadini tramite Facebook[6] chi, se non un vero *cittadino digitale*, può evidenziare i difetti di questa pratica?

L'Arcobaleno della Cittadinanza Digitale

Storicamente, in "*A ladder of citizen participation*" [Arn69], venne suggerita la metafora della scala, mostrata in figura 2, per mettere ordine nel percorso che porta a una compiuta cittadinanza, anche non digitale. La scala evoca un percorso *in salita* che implica un impegno progressivo da parte di coloro che lo intraprendono, ma anche una realizzazione sempre più completa dei diritti di cittadinanza man mano che si sale. Modella abbastanza correttamente

[5] Spesso a vantaggio di coloro che queste soluzioni digitali le *posseggono*.

[6] Una pratica purtroppo frequente, cfr. la sezione "Social media e partecipazione digitale" in [WTM13].

l'esperienza di molte persone che scoprono di doversi impegnare per diventare cittadini nella società dell'informazione. Tuttavia, ai fini dell'efficacia della comunicazione e per fornire una visione più analitica, preferiamo adottare e soprattutto **adattare** il modello *ad arcobaleno* proposto in "*The access rainbow: Conceptualizing universal access to the information/communications infrastructure*" [CS00] perfezionandone i livelli a partire da Livello 0 [*The Net*], dedicato alla *Rete* (i.e., Internet), che indica l'importanza di una Rete libera, aperta e neutrale che costituisce l'infrastruttura indispensabile[7]. In figura 1 viene mostrata la nostra versione attuale che sarà oggetto del presente testo.

Suddividiamo il nostro arcobaleno in due gruppi logico-strutturali: i livelli *tecnico-infrastrutturali* L0-network, L1-services, L2-access e L3-education, che raggruppiamo sotto il nome di *Tecnocivismo*, e quelli *sociali-partecipativi* L4-transparency[8], L5-participation, L6-consultation, L7-democracy raggruppati nella *Cittadinanza Digitale*.

Il **Tecnocivismo**, ponendo l'accento su tecnologia, consapevolezza, Rete, standard, formati, software, servizi... serve come fondamento per la vera e propria **Cittadinanza Digitale** dove si parla di piattaforme partecipative, di consultazione e partecipazione dei cittadini, di trasparenza e di sistemi di voto.

Il nostro arcobaleno è quindi così composto:

- Livelli *tecnico-infrastrutturali*: ***Tecnocivismo***

  Livello 0 [*The Net*] =
  l'infrastruttura della Rete
  Livello 1 [*services*] =
  servizi online, pubblici e privati
  Livello 2 [*access*] =
  accesso ai servizi di cittadinanza
  Livello 3 [*education*] =
  istruzione e consapevolezza

[7] Ma non sufficiente, come vedremo nel seguito.

[8] Anche se L4-transparency è una sorta di livello *pivot* tra i due gruppi e può essere considerato parte di entrambi.

- Livelli *social-partecipativi*: ***Cittadinanza Digitale***

  Livello 4 [***transparency***] =
  la trasparenza
  Livello 5 [***participation***] =
  informarsi reciprocamente e collaborativamente
  Livello 6 [***consultation***] =
  essere ascoltati e consultati
  Livello 7 [***democracy***] =
  coinvolgimento attivo nelle scelte pubbliche e nell'elaborazione delle politiche

L'idea sottostante e il numero dei livelli ricorda il modello OSI (*Open Systems Interconnection*) per le architetture delle reti. Ci confrontiamo con il modello OSI[9] perché se uno qualunque dei livelli è carente le conseguenze negative si ripercuotono su tutti i livelli sovrastanti[10]. Esempio quasi ovvio: se la rete non funziona *correttamente*[11] potrei avere problemi nell'utilizzo di servizi **online**.

Il metodo spettrografico

Nel corso degli anni, la semantica iniziale del concetto di *dipendenza stretta tra livelli* è andata sfumando per convergere verso la metafora della **spettrografia/spettroscopia**[12] in cui ogni banda colorata rappresenta un aspetto importante della Cittadinanza Digitale.

L'ispirazione proviene dalla *spettroscopia* fisica, una tecnica per analizzare la composizione di un oggetto, magari praticamente irraggiungibile come una stella, esaminandone la luce emessa[13]. Gli elementi chimici e le molecole, se opportunamente *stimolati* (ad esempio mediante

[9] Modello architetturale a strati di servizio in cui gli strati bassi fungono da piattaforma per implementare quelli più alti. (cfr. *http://en.wikipedia.org/wiki/OSI_model*)

[10] E, contrariamente a ciò che succede nel modello OSI, possono esserci *retro-propagazioni* anche nei livelli sottostanti.

[11] Capiremo cosa si intenda con il termine nei capitoli 0, 1 e 2

[12] *http://it.wikipedia.org/wiki/Spettroscopia*

[13] *http://it.wikipedia.org/wiki/Spettro_di_emissione*

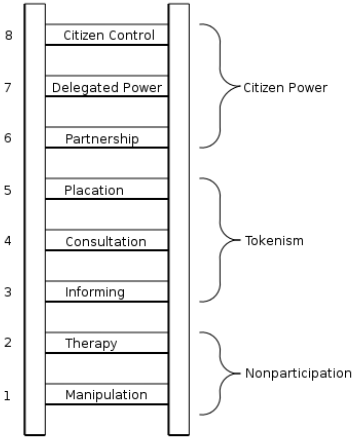


Figura 2: La scala di Arnstein (Wikipedia)

riscaldamento) emettono radiazioni a lunghezze d'onda legate alla loro composizione chimica, "spezzando"[14] la luce emessa nelle sue componenti è possibile proiettare uno *spettro* (figura 3) che "racconta" la composizione chimica dell'oggetto sotto esame.

Attraverso la nostra *spettroscopia Cittadinanza Digitale e Tecnocivismo* il contesto o la situazione oggetto dell'analisi vengono valutati in base alla *luminosità*[15] attribuita ad ogni livello in quel particolare contesto, e lo spettro che ne risulta ci fornisce *a colpo d'occhio* una panoramica dell'oggetto valutato.

Alcuni esempi ipotetici:

- un paesino di montagna dove arrivassero solo le linee telefoniche tradizionali e non ci fosse molto campo

[14] Anticamente mediante un prisma ottico, oggi con tecniche digitali.

[15] Percepita soggettivamente, salvo per alcuni aspetti dove esistono metodi di misura o classificazioni standardizzate (ad esempio la *classificazione di Davies* - `http://www.opendataimpacts.net/engagement` - per gli *opendata* 🕮), le valutazioni vengono effettuate in base al giudizio dell'osservatore.

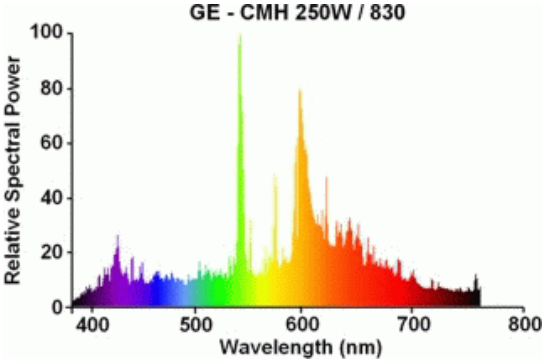


Figura 3: Spettrogramma di emissione (Wikipedia)

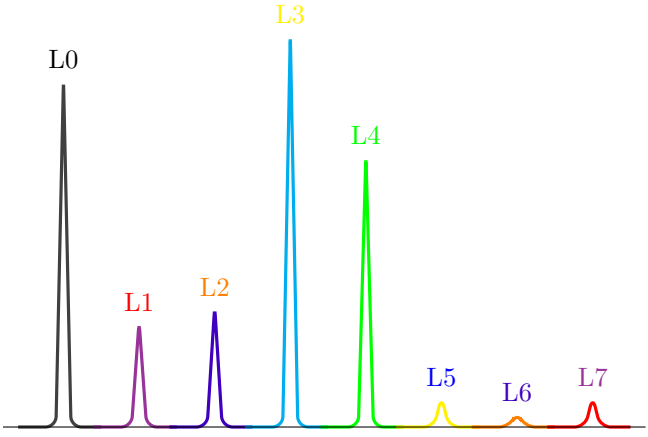


Figura 4: Spettrogramma de "*I Principi di Internet*"

della rete cellulare avrebbe L0-network molto fioco;
- una scuola dove mancasse la rete e i pochi personal computer disponibili fossero dotati solo del sistema operativo di Microsoft avrebbe le bande da L0-network a L3-education molto fioche;
- una nazione perfettamente cablata con fibra ottica ma con un governo autoritario avrebbe le bande da L0-network a L3-education molto luminose, ma quelle da L4-transparency in su molto fioche;
- una nazione perfettamente cablata con fibra ottica e con un governo molto democratico e trasparente, ma con i programmi scolastici lacunosi sulle tecnologie, avrebbe le bande da L0-network a L2-access e da L4-transparency in su molto luminose, ma il problema sulla banda della conoscenza L3-education potrebbe inficiare i bellissimi sistemi partecipativi a disposizione dei cittadini.

Un esempio reale di spettrografia CDT lo si vede in figura 4. Rappresenta l'analisi[16] della distribuzione sui vari livelli dei commenti raccolti durante la consultazione pubblica sui "*Principi di Internet*" attivata nel 2012 dal MIUR. Tale spettro rappresenta l'attenzione, sbilanciata sui livelli infrastrutturali, del campione di popolazione che partecipò alla consultazione.

La CDT intorno a noi

Lontano

Naturalmente nel corso del testo il lettore potrà apprezzare appieno la semantica e l'uso dell'arcobaleno, ma per cominciare con un piccolo assaggio citiamo un bell'esempio di cos'è lontano dalla Cittadinanza Digitale.

Scoprimmo per caso, quando pensammo di acquistare un dominio Internet legato al tema in oggetto, che *citta-*

[16] Pubblicata in [DT14].

Figura 5: Cosa **non** è *Cittadinanza digitale*

dinanzadigitale.it[17] era già stato registrato dal Comune di Venezia per… la gestione degli account del WiFi pubblico. Il Comune di Venezia, infatti, chiama *cittadinanza digitale* (figura 5) la pura e semplice fornitura di connessione Wi-Fi gratuita ai residenti, come se l'accesso WiFi gratuito fosse l'unico aspetto importante per la piena Cittadinanza Digitale! L'analisi dell'arcobaleno applicata a questo caso *accende* qualcosa (invero poco) di L0-network, qualcosa di L1-services e un lumicino di L2-access, ma brancoliamo ancora abbondantemente nel buio su tutti gli altri livelli.

Questo aneddoto dovrebbe indurre nel lettore l'effetto dello stridore del gesso sulla lavagna, se non subito sicuramente a valle della lettura di questo testo.

[17] Nota umoristico-tragicomica: il dominio è registrato, ma è configurato male. Per chi è già avvezzo, i due nomi simbolici risolvono indirizzi IP diversi (agosto 2019):

- cittadinanzadigitale.it → 195.110.124.188
- www.cittadinanzadigitale.it → 94.247.8.24

Infatti cliccando su `http://cittadinanzadigitale.it` non si ottiene nulla, bisogna proprio digitare `http://www.cittadinanzadigitale.it` per intero.

Vicino

Per fortuna esistono anche esempi positivi o perlomeno promettenti.

Politiche

Il tema **Agenda Digitale Nazionale** copre molti aspetti dell'arcobaleno, anche se con alcune lacune sui livelli partecipativi. La Regione Emilia-Romagna, per citarne un *top player*, nelle sue linee guida[18] elenca esplicitamente i seguenti *diritti* (tra parentesi indichiamo i livelli dell'arcobaleno che abbiamo evidenziato):

- diritto di accesso alle reti tecnologiche (L0-network)
- diritto all'informazione e alla conoscenza (L3-education)
- diritto ai servizi alla persona e alle imprese (L1-services, L2-access)
- diritto di accesso ai dati (L4-transparency)

Come si può notare mancano però i livelli partecipativi: l'agenda infatti non prende in considerazione la partecipazione del cittadino digitale alla vita politica. E anche sui livelli coperti si possono purtroppo evidenziare lacune, ad esempio la pagina relativa alle infrastrutture[19] non cita la *net neutrality* (che tratteremo) né gli aspetti di monitoraggio e controllo, si parla solo, grossolanamente, di *banda passante* 🕮.

Stesso discorso per l'**Agenda Digitale Europea**[20], che elenca i suoi *pilastri* (*pillars*):

- un mercato digitale unico e dinamico (L1-services, L3-education)
- interoperabilità e standard (L1-services)

[18] *http://digitale.regione.emilia-romagna.it/cos-e-agenda-digitale*

[19] *http://digitale.regione.emilia-romagna.it/cos-e-agenda-digitale/assi/infrastrutture*

[20] *http://formazione.formez.it/sites/all/files/agenda_digitale_europea.pdf*

- fiducia e sicurezza informatica (L0-network, L1-services)
- accesso ad Internet veloce e super-veloce (L0-network, L1-services)
- ricerca e innovazione (L3-education)
- miglioramento dell'alfabetizzazione, delle competenze e dell'inclusione nel mondo digitale (L3-education)
- servizi digitali (L1-services)
- internazionalizzazione (L3-education)

Anche qui i livelli partecipativi sono grandi assenti.

La **Strategia Nazionale per la Crescita Digitale** [Pre15] adotta un *framework* difficilmente correlabile ai livelli dell'arcobaleno. Comunque, scorrendo il testo, si riescono a ritrovare collegamenti verso i livelli infrastrutturali e anche in questo caso non vengono mai menzionati sistemi partecipativi… nonostante il documento stesso sia frutto di un processo partecipativo! Come orgogliosamente dichiarato in premessa:

> *La presente strategia è stata redatta a valle di un processo di consultazione partecipato sia online sia offline, svoltosi dal 20 novembre 2014 al 20 dicembre 2014 e che ha coinvolto tutti gli stakeholders pubblici e privati, nonché numerosi cittadini e associazioni civiche*[21].

In alcuni punti del documento viene identificato un *KPI* 🕮 definito "Grado di partecipazione dei cittadini attraverso il web a attività politiche e sociali" che sembra promettente, purtroppo leggendo i fattori di misura a cui è collegato (ad esempio l'uso dei servizi anagrafici digitali) si può capire come sia anch'esso legato ai livelli infrastrutturali: promessa sui livelli partecipativi purtroppo disattesa.

[21] Prego notare le date (durata complessiva: un mese!) e il fatto che si afferma che sono stati coinvolti *tutti* gli *stakeholders*, sia online che offline… lo riteniamo molto difficile dato che soprattutto per la parte offline (convocazioni via posta e riunioni *de visu*) un mese è un attimo. Per confronto con processi un po' più seri si vedano le tempistiche di approvazione degli standard IETF specificate su [Bra96]: mesi/anni per **ogni fase** di un processo a molti passi.

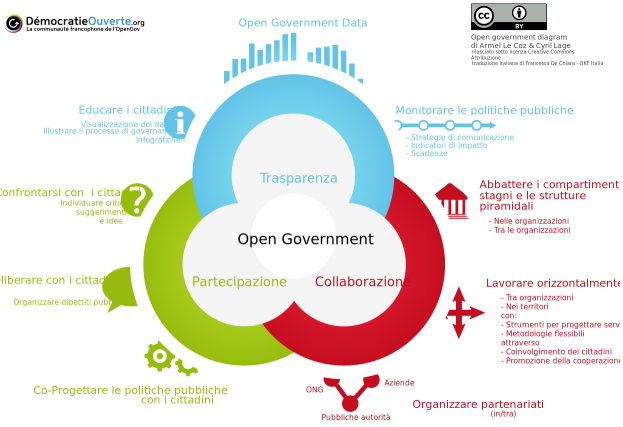


Figura 6: Schema dell'Open Government (Démocratie Ouverte)

Molto interessante e positivo invece il concetto di *open government*[22] definito dall'OECD (*Organisation for Economic Co-operation and Development*). Ne vediamo una schematizzazione in figura 6, come si può notare vengono finalmente dichiarati anche i livelli partecipativi, pur con una diversa classificazione, più grossolana rispetto alla nostra, vediamo una mappatura con l'Arcobaleno:

- Lobo *Trasparenza*:
  conoscenza (L3-education) oltre che, ovviamente, trasparenza (L4-transparency)
- Lobo *Partecipazione*:
  partecipazione (L5-participation), ma anche consultazione (L6-consultation) e (L7-democracy)
- Lobo *Collaborazione*:
  servizi (L1-services), accesso (L2-access) e ancora partecipazione/collaborazione (L5-participation)

In apparenza manca *solo* il livello più infrastrutturale, quello della Rete. Nella sostanza, esaminando il contenuto del piano d'azione [Ita19] e riportando su uno *spettro*

[22] *http://oecd.org/gov/open-government.htm*

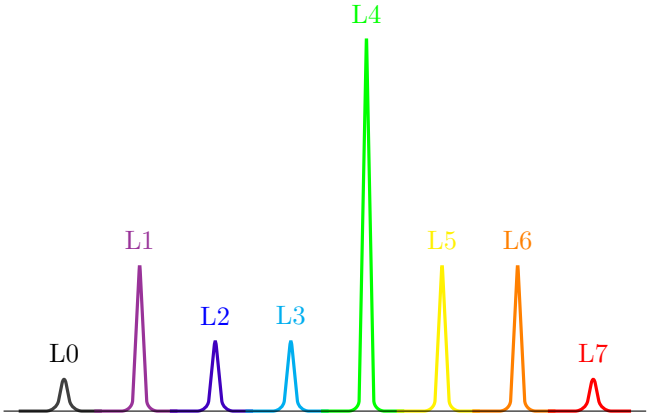


Figura 7: Spettrogramma del piano d'azione Open Government (Luca Messina)

CDT le singole sub-azioni possiamo vedere (figura 7) che purtroppo resta molto sbilanciato: di fatto concentrandosi su L4-transparency, L3-education, L1-services.

Libri

Un testo che ci aveva attratto per il titolo molto promettente è "*Cittadini ai tempi di Internet*" [Fug18]: sebbene si tratti di una trattazione molto interessante è essenzialmente incentrata su L3-education del nostro arcobaleno.

Una piacevole nota positiva la troviamo invece in "*Critica della democrazia digitale: la politica 2.0 alla prova dei fatti*" [Chi14] che finalmente cita i sistemi di voto (pur con i loro problemi) e in generale il problema della partecipazione digitale (e non solo). In tale testo possiamo riconoscere riferimenti a L5-participation, L6-consultation, L7-democracy, L3-education dell'arcobaleno.

Segnaliamo anche il piacevole libro di Rocca "*Chiudete Internet: Una modesta proposta*" [Roc19] che è un buon complemento della nostra trattazione, è quasi per nulla tecnico (contrariamente al nostro testo) e ragiona molto sugli aspetti sociali, politici e culturali, quindi di fatto sui livelli

partecipativi del nostro arcobaleno anche se si appoggia abbastanza sull'*infrastrutturale* (accennando principalmente a L1-services e L3-education) per cercare le cause dei problemi che descrive, quali:

- ignoranza al potere (ignoranza nell'elettorato passivo)[23]
- responsabilità civica abnegata (ignoranza nell'elettorato attivo)
- Internet come veicolo di ignoranza più che di cultura perché incontrollata o controllata dalle industrie delle …
- … *fake news*
- creazione di problemi supportati da *fatti* (*fake news and data*) per effettuare la …
- … manipolazione del consenso attraverso …
- … bolle informative (*filter bubble*)

Temi, quelli citati da Rocca, che è interessantissimo (dal punto di vista meramente *archeologico*) *non* trovare in un libro dal titolo molto evocativo come "*Digital citizenship*" [Wri08]. Il libro è uscito infatti nel 2008, ampiamente prima della nascita del problema delle *fake news*. Definisce *broadband access* (accesso a banda larga, ad alta velocità) quali DSL (*Digital Subscriber Line*) intorno ai 200kbit/s mentre oggi abbiamo VDSL (*Very-high-bit-rate Digital Subscriber Line*) a 100Mbit/s e reti cellulari 3/4/5G a velocità anche più elevate. Si tratta di un imponente studio basato principalmente sui dati dei censimenti statunitensi, quindi molto quantitativi e poco analitici: nei questionari venivano chieste informazioni generali come ad esempio la *frequenza uso Internet* (in ore/gg). Il testo di Mossberger è intriso di positivismo, l'ipotesi che porta avanti è che *Internet* porta ai cittadini[24] maggiore conoscenza (L3-education) e voglia di conoscere il funzionamento del sistema politico (L4-transparency) per poi indurre maggiore partecipazione, sia dal basso (L5-participation) che

[23] Una citazione *socratica*, riferendosi ad un gruppo politico attualmente (2019) al governo: "… sono quel genere di ignoranti così ignoranti da ignorare soprattutto le cose che ignorano."

[24] Che diventano appunto *digitali* con la sola aggiunta di Internet.

dall'alto (L6-consultation), cioè dal sistema politico stesso (che deve confrontarsi con cittadini più *smart*). Potremmo anche concordare con Mossberger&C. se *Internet* fosse un po' diversa da come è diventata oggi (cfr. i nostri capitoli 0, 1 e 2) cioè se fosse più controllabile dai suoi utenti invece che da pochi enti/aziende. Infatti, il problema principale di "*Digital citizenship*" è che liquida i livelli infrastrutturali del nostro arcobaleno riferendosi semplicemente a *Internet*, senza approfondimento ulteriore o quasi[25], mentre noi dedichiamo praticamente tutto il presente volume a definire bene tutti gli aspetti positivi[26] e negativi[27] della Rete e dei servizi online. Rispetto al nostro arcobaleno tocca:

- molto L2-access, inteso come *availability* (disponibilità) e *affordability* (accessibilità economica) delle reti[28] citando ad esempio il tema della disponibilità dei punti di accesso (biblioteche ecc.);
- L3-education, perché *Internet* porta conoscenza, ma senza riconoscere il problema della *relatività* (che tratteremo nei capitoli 0, 1 e 2) e senza affrontare il tema della effettiva disponibilità della conoscenza (che tratteremo nel capitolo 3);
- un po' L4-transparency, inteso però come volontà di sapere, non come *open data* e trasparenza;
- minimamente L5-participation, inteso come voglia di condividere e discutere, forum e *community*;
- un po' L6-consultation, inteso come aumento della voglia di partecipazione e interazione col mondo politico da parte dei cittadini, mentre da parte dei politici come necessità di appoggiarsi alle *community*, ma non prevede il *tipo* di partecipazione che poi si è verificata in seguito, cioè estremismi basati su *fake news* o pilotaggio di bolle cognitive (che invece il

[25] Discrimina minimamente i vari tipi di Internet a pag. 78 citando email, forum e siti di notizie.

[26] Che effettivamente migliorano la Cittadinanza Digitale.

[27] Che sono parecchi e che ostacolano/impediscono il percorso verso la Cittadinanza Digitale.

[28] Sempre senza entrare nel merito di quale tipo di rete e quali tipi di servizi.

sopracitato Rocca denuncia).
Eppure già allora, parliamo del 2008, c'erano tutti gli elementi per comprendere che non era affatto solo un problema di *broadband*, non era difficile identificare e analizzare la presenza di tutti quegli elementi che ai tempi - e da tempo - consentivano il controllo pervasivo, la perdita di privacy, le *fake news*, le *filter bubble*... tutti temi che in quel libro nemmeno appaiono.

Persone

Esistono fior di enti e *community* (alcune invero enormi) che si adoperano in L3-education e L5-participation proponendo l'importantissima *cultura libera* [Les16] e il *crowdsourcing* 🕮, ne citiamo qualcuna:

- Creative Commons[29]
- Wikimedia[30]
- Progetto Gutenberg[31]
- Openstreetmap[32]
- FSF[33]

L'ultima organizzazione citata, Free Software Foundation, si occupa principalmente di Software Libero che è un tema fondamentale per tutti i livelli dell'arcobaleno: senza Software Libero non avremmo risposte a molte delle esigenze raccontate in questo testo.

Alcune *community* più tecniche inoltre applicano i concetti della cultura libera a L4-transparency concentrandosi sulla trasparenza come Openpolis[34] e Spaghetti Open Data[35].

[29] *http://creativecommons.org*
[30] *http://wikimedia.org*
[31] *http://gutenberg.org*
[32] *http://openstreetmap.org*
[33] *http://fsf.org*
[34] *http://openpolis.it*
[35] *http://spaghettiopendata.org*

Caveat

La trattazione del *Tecnocivismo*, cioè il presente volume, è impostata come un *Cahier de doléances*[36] (quaderno delle doglianze). Attualmente i livelli bassi dell'Arcobaleno della CDT sono purtroppo costellati da ombre che vogliamo rendere evidenti a tutti i cittadini digitali. Avremo quindi un approccio militante e schierato a favore di quelli che riteniamo essere *valori*[37] importanti, ancora poco garantiti e difesi, come:

- Internet neutrale e accessibile;
- difesa della privacy digitale;
- servizi accessibili, conoscibili e interoperabili;
- software e hardware libero;
- conoscenza libera.

Ci piacerebbe dire che siamo dalla parte giusta della Storia, ma questa espressione rischia di illudere circa l'ineluttabilità del progresso e la sua direzione. Purtroppo non è così: la Storia è il risultato del conflitto tra interessi contrastanti, e in tale conflitto ognuno può giocare la sua parte, da Aaron Swartz[38] - che si impegnò fino alla morte per l'Open Access - a ciascuno di noi che può scegliere di esercitare il proprio tecnocivismo a partire da azioni quotidiane quali ad esempio:

- firmare o cifrare le mail e garantire così autenticità o riservatezza alle comunicazioni;
- salvare documenti in formato standard e aperto, rompendo il *lock-in* imposto dai formati proprietari;
- utilizzare software libero per contribuire alla diffusione e al miglioramento di un ecosistema digitale condiviso e affidabile;
- adottare licenze libere per i contenuti prodotti;
- pubblicare su piattaforme aperte e possibilmente decentralizzate, evitando *silos informativi* 🕮 e *walled garden* 🕮;

[36] *http://it.wikipedia.org/wiki/Cahiers_de_doléances*

[37] Tutti questi concetti saranno pienamente comprensibili al termine della lettura.

[38] *http://it.wikipedia.org/wiki/Aaron_Swartz*

Siamo dalla parte di chi - nelle scelte in ambito digitale e tecnologico - è consapevole delle responsabilità sociali e per questo privilegia i criteri *etici* a quelli meramente prestazionali quali la comodità o la superficiale semplicità di utilizzo.

Speriamo che questo libro spinga molti cittadini a schierarsi e a *militare* attivamente tramite le scelte, piccole o grandi, che ciascuno compie quotidianamente.

Ça va sans dire che consideriamo le tecnologie digitali un enorme vantaggio per l'umanità e che siamo quanto di più lontano dal *neo-luddismo* 🕮 si possa immaginare: noi vogliamo **più** tecnologia, non meno, ma la tecnologia che usiamo deve essere sotto il nostro controllo.

[Convenzioni di stesura]

- Ove opportuno citiamo bibliografia esterna di approfondimento in note a piè di pagina o in fondo al testo (da pag. 329).
- Sono stati inseriti alcuni *box* di *approfondimento*, generalmente a fine sezione.
- Quando citiamo pagine di Wikipedia lo facciamo consci dei suoi scopi e limiti dichiarati[39].
- Scriveremo Internet con iniziale maiuscola: per noi è un nome, è l'attuale e imperfetta incarnazione de La Rete, quella che fa tanto paura ad alcuni governi e che viene così spesso bistrattata e accusata o al contrario osannata e celebrata in funzione delle convenienze politiche degli attori in campo.
- I termini spiegati nel glossario (da pagina 310) appaiono con un'icona accanto, esempio: *blogpost* 🕮.
- La numerazione dei capitoli segue quella dei livelli del nostro arcobaleno.
- Ricordiamo che questo lavoro è suddiviso in due volumi: questo primo volume è dedicato al Tecnocivismo, il secondo alla Cittadinanza Digitale.

[39] *http://en.wikipedia.org/wiki/Wikipedia:About*

Capitolo 0

Livello 0 [*The Net*]

`Quante strade deve percorrere un *pacchetto di dati* prima di poterlo chiamare tale?`

Parafrasi da "Blowing in the wind" di Bob Dylan

Il **Livello 0** [***The Net***] del nostro Arcobaleno tratta ciò che concerne lo strato più infrastrutturale, ma non il meno importante, della *CDT (Cittadinanza Digitale e Tecnocivismo)*. Fra tutti è il più *fisico*: quello della rete (*network*, ma noi faremo quasi sempre riferimento alla Rete, cioè a Internet) che trasporta, **bene o male**[1], ogni informazione. In questo livello descriveremo e discuteremo come si comporta questa Rete, come essa può essere *piegata* ad utilizzi non sempre felici e come tentare di rilevare eventuali distorsioni, per poi attuare qualche tipo di difesa. Non sarà sempre possibile, purtroppo.

Bisogna sapere che i *bit* 🕮 viaggiano in pacchetti di *byte* 🕮 che trasportano informazioni, permettendoci di raggiungere (comunicativamente) sempre e immediatamente chiunque e qualsiasi cosa ovunque ci si trovi… Ma è davvero così? In termini semplici: in una rete TCP/IP (*Transmission Control Protocol / Internet Protocol*)[2] i pacchetti di dati hanno un mittente, un destinatario e un contenuto. Ognuno di questi tre attributi è molto importante e influenza la veridicità dell'affermazione di cui sopra, inoltre, questi attributi non sono nemmeno sempre indipendenti l'uno dall'altro e sono sotto il controllo di entità più o meno conosciute:

- provider di connettività che forniscono il servizio *ultimo miglio* 🕮
- istituzioni che impongono regole, anche molto puntuali (ad es. oscuramento di siti)

[1] E ci interesserà soprattutto il *troppo bene* (raccolta dati indiscriminata, privacy) e il *male apposta* (*net neutrality*, discriminazione *elitaria* del traffico).

[2] I cui dettagli vedremo in sezione "*Mini-esegesi di TCP/IP*" - 0.1.1.

- produttori di contenuti che possono rispondere in modo differente a richieste identiche di mittenti diversi

Attribuiremo alla Rete caratteristiche molto *relativistiche* usando come metafora proprio la relatività einsteiniana: ogni utente Internet è un *osservatore* immerso in un universo in evoluzione, ma lo **stato generale di questo universo non è identicamente conoscibile da tutti gli osservatori** poiché la propagazione delle informazioni è ben lungi dall'essere istantanea e integrale.

E vedremo anche una trasposizione digitale del *Principio di Locard* secondo cui è molto difficile, per chi interagisce con questo universo, non lasciare una traccia: **la Rete non dimentica**.

Aziende e governi tracciano ogni informazione che passa sulla Rete e la usano per ~~proteggerci dal terrorismo e dai criminali~~capire cosa facciamo, pensiamo, diciamo e… acquisteremo o voteremo. Non solo tracciano, ma spesso controllano i flussi informativi per influenzare acquisti, cognizioni, pensieri, parole, opere, … consensi e voti.

Per dirla *alla maniera della CDT*: il funzionamento della rete, le modalità di erogazione dei servizi digitali e le possibilità di accesso alle tecnologie hanno forte impatto sulla conoscenza, quest'ultima influenza la capacità di un cittadino nell'esercitare il proprio diritto alla trasparenza e infine tutti i livelli infrastrutturali influenzano quelli "partecipativi" cioè partecipazione, consultazione e democrazia.

Quindi conoscere i principi di funzionamento è fondamentale per orientarci nell'universo informativo digitale in cui siamo costantemente immersi e in cui dobbiamo navigare, possibilmente non a vista. Anche perché, purtroppo, questa Rete è stata progettata da *ingenui* (cfr. sezione "*Avete rotto Internet*" - 0.5), nel senso di gente che non si sarebbe mai immaginata un uso così distorto[3] come quello

[3] E c'è voluto il coraggio di pochissime persone che hanno rischiato (e tuttora rischiano) la propria vita per farci sapere ciò che è stato fatto (e viene fatto tuttora) alla Rete che credevamo uno strumento

che racconteremo. Ma noi cittadini tutti (non solo i tecnici) abbiamo il dovere di *conoscere per deliberare* [Ein55], non solo su argomenti *analogici* (chi mandare in parlamento o in Comune), ma anche su quelli *digitali*.

Noi tutti speravamo che Internet *ci avrebbe permesso* di:

- Rendere progressivamente più semplice e meno dispendioso consentire a qualsiasi persona con una propria attività commerciale di vendere i propri prodotti e servizi *senza intermediari*, o almeno con pochi intermediari scelti e fidati, non imposti da monopoli. (L1-services, L2-access)
- Consentire una reale *educazione all'uso degli strumenti digitali*, incentivando e diffondendo la conoscenza dei principi alla base di tali strumenti e non l'accettazione dello status-quo come fosse evoluzione naturale. (L3-education)
- *Incrementare la trasparenza* dei dati e delle informazioni, fornendo solidi *strumenti di partecipazione* che consentissero a ciascun cittadino di formare i propri giudizi basandosi su una sana dialettica anziché su logiche da tifoserie sportive. (L4-transparency, L5-participation, L6-consultation, L7-democracy)
- Facilitare la diffusione delle proprie idee *senza timore di ritorsioni* da parte di regimi autoritari o violenti fanatici, consentendo pari opportunità di *partecipazione al dibattito sociale* e alle *istanze di cambiamento* che sono alla base della civiltà moderna. (L3-education, L5-participation, L6-consultation, L7-democracy)
- *Avvicinare le istituzioni ai cittadini* consentendo loro di meglio interpretare le istanze sociali e rappresentarle nelle sedi opportune, attuando pienamente i principi fondanti delle moderne democrazie (L5-participation, L6-consultation, L7-democracy)

Effettivamente l'*e-commerce* è molto diffuso, ma dobbiamo lavorare assiduamente al contenimento dei grandi

di libertà e conoscenza.

monopoli commerciali (Amazon, Microsoft, Apple, Ebay ecc.). La conoscenza è diffusa e molto accessibile[4], ma bisogna anche limitare la propagazione delle *fake news* (bufale) e dei *complottismi*. La trasparenza delle istituzioni è un processo in corso, ma non sempre alla portata del singolo cittadino [Puu+18]. La libertà di parola è spesso, purtroppo, tacitata anche con mezzi tecnologici[5]. L'uso che si fa della Rete per conoscere le intenzioni dei cittadini è spesso *di facciata* (per guadagnare consensi vantando il proverbiale *ascolto*) o, peggio, subdolo (non esplicito) per capire le intenzioni di voto e adattare i propri programmi politici.

Noi partiremo *dal basso* fornendo concetti di base che ci serviranno per comprendere e tentare di occuparci del castello infrastrutturale che stiamo esplorando anche solo aprendo un *browser*.

Solo potendo conoscere le tecnologie, come comunità intera, potremo governarle a nostro favore invece di farci governare da chi oggi le controlla.

0.1 Internet

Internet (La Rete) è *una* (la più importante!) rete digitale di trasporto dati, serve a portare informazione in *quantità notevoli* e a *velocità molto elevate*, basti pensare che le applicazioni più recenti permettono ormai di fatto la *telepresenza*: poter (quasi) vivere dal vivo un'esperienza in un luogo che si trova molto distante.

È un sistema complesso che si basa essenzialmente sul trasmettere *pacchetti di byte* (blocchi di dati) in giro per il mondo. I pacchetti vengono ordinati in sequenze che *costruiscono* dei flussi di dati che poi l'utente fruisce ad esempio guardando un film, ascoltando musica o semplicemente consultando una pagina di un sito.

La Rete, quindi, veicola dati (in forma di pacchetti singoli o flussi) che possono essere richiesti e fruiti tramite ap-

[4]Salvo *blocchi di rete*, descritti nel presente capitolo.
[5]Ancora *blocchi*, come sopra.

plicazioni che *parlano* **protocolli di rete**. Il lettore avrà certamente sentito nominare[6] almeno HTTP e FTP, forse SMTP, IMAP, IRC, XMPP e GNUTELLA, più raramente SIP, X11 e KERBEROS. I protocolli di rete servono a codificare *opportunamente* (cioè al meglio per la particolare esigenza di scambio dati) i contenuti e le sequenze di dati in modo da ottenere la funzione richiesta.

Un esempio intuitivamente facile da comprendere è uno *stream* video: un protocollo di trasmissione dovrà occuparsi di codificare ogni *frame* nel modo più efficiente (meno byte per *frame* meglio è) possibile e poi dovrà gestire eventuali difetti di trasmissione. Se si perde un *frame* si può decidere di:

1. presentare un *buco*, un salto nelle immagini, all'utente finale;
2. chiedere alla fonte di ritrasmettere il dato mancante (operazione costosa in termini di tempo);
3. oppure si può tentare di ricostruire l'immagine mancante per differenza tra quella che precede e quella che segue (opzione non banale perché è un *calcolo* complesso e va fatto molto rapidamente).

Unità di misura sono tipicamente i multipli del *bit* 🕮 o del *byte* 🕮, soprattutto il *mega*-byte (1024∗1024 byte), il *giga*-byte (1024 megabyte) e il *tera*-byte (1024 gigabyte)[7] per quanto riguarda le *dimensioni* dei dati, mentre per i tempi tipicamente si usa il secondo, cioè per esprimere una velocità di trasmissione si parla di *(…/mega/giga/tera) bit o byte/s*.

Internet come la conosciamo oggi ha in realtà origini molto *antiche*[8], i primi studi ed esperimenti risalgono infatti agli anni '60 del novecento. Il governo USA inizialmente finanziò il progetto ARPANET allo scopo di realizzare una rete di interconnessione fra computer robusta e resistente

[6] Non li spiegheremo, ci serve solo citare qualcosa di *forse* conosciuto.

[7] Utilizzando il sistema internazionale di misura (SI) per gli ordini di grandezza dei dati, per approfondimenti si veda `http://en.wikipedia.org/wiki/Kilobyte`

[8] In ambito tecnologico anche solo cinque anni sono un'*era*.

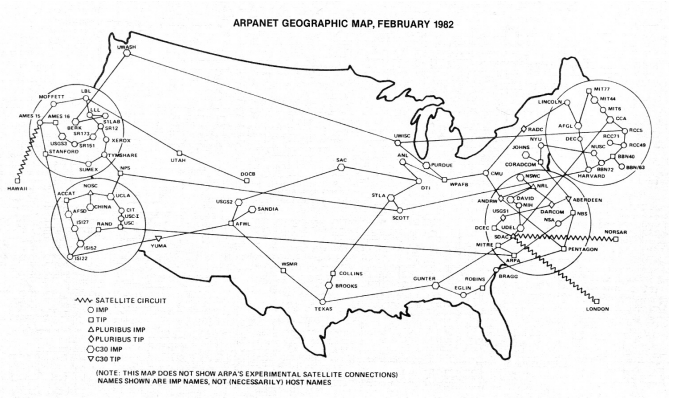


Figura 1: *Internet* (Arpanet) nel 1982 (vox.com)

ai guasti (*fault tolerant*). L'idea era tutto sommato relativamente semplice, creare una rete di connessioni *ridondata*: da un nodo preso a caso si deve poter raggiungere un altro nodo preso a caso utilizzando più di un *percorso* (insieme di *archi*: canali che connettono due nodi direttamente). Il *percorso* è composto dai nodi stessi della rete, essi cioè fungono anche da *passacarte* per il *traffico* (le comunicazioni) diretto ad altri nodi. Nella figura 1 che illustra la situazione della rete nei primi anni '80[9] si può notare che:

- c'è **un certo grado** di ridondanza, e.g., CCA è raggiungibile da MIT6, RCC5 e UDEL;
- ma **non è totalmente** ridondata, e.g., il nodo DOC8 è raggiungibile solo passando per UTAH.

Come viene realizzata questa architettura?

Semplificando molto e rimandando ad un classico testo, il "*Computer Networks*" [TW12], per eventuali approfondimenti, in questo contesto a noi basti sapere che nei primi anni '80 viene introdotta la suite di protocolli di rete chiamata **TCP/IP**[10] che si basa principalmente sul

[9]Su *http://vox.com/a/Internet-maps* si può trovare una bellissima storia di Internet attraverso *mappe*.

[10]Si veda *http://livingInternet.com* per una interessante raccolta di documenti sulla storia di Internet, oppure la sempre uti-

meccanismo qui di seguito descritto:

- ogni comunicazione (arbitrariamente lunga: dal semplice messaggio di posta elettronica fino al video da molti MB/GB) viene *spezzata* (*chunked*) in *pacchetti* (dalla lunghezza massima prestabilita) che vengono spediti lungo la rete indicando il destinatario finale;
- ogni pacchetto viaggia lungo la rete seguendo potenzialmente percorsi diversi (in funzione delle condizioni della rete stessa) arrivando a destinazione anche non rispettando la sequenza originale di partenza;
- il (computer del) ricevente ricostruisce la sequenza originale[11] opzionalmente chiedendo la ritrasmissione di pacchetti persi;
- all'utente finale viene presentato il *dato* originale ricostruito.

L'apparente complicazione ha in realtà due scopi principali:

1. quello di permettere la gestione *contemporanea* di più comunicazioni sullo stesso canale. Infatti, dato che ogni canale di trasmissione ha una sua capacità trasmissiva superiormente limitata[12], se ogni singola trasmissione impegnasse stabilmente un canale (fino a saturazione) si rischierebbe di non poter servire altre richieste per tempo molto lungo (e.g., per trasmettere un file da $10MB$ su una linea da $10kB/s$ ci si impiegano circa 1000 secondi). Invece, spezzando la singola trasmissione si realizza il cosiddetto ***multiplexing*** del canale: viene inviato un pacchetto relativo ad una trasmissione, poi un pacchetto relativo ad un'altra, poi uno di un'altra ancora e così via. In questo modo ogni richiesta di trasmissione ve-

le Wikipedia *http://en.wikipedia.org/wiki/Internet_protocol_suite*.

[11] I pacchetti contengono dei *metadati* (si veda sezione "*Mini-esegesi di TCP/IP*" - 0.1.1) che permettono la ricostruzione del flusso.

[12] Negli anni '80 sulle grandi distanze si potevano utilizzare ad esempio le linee telefoniche esistenti (per non dover stendere chilometri di cavi ad hoc), esse permettevano velocità di trasmissione dell'ordine delle decine di $kilobit/s$ nella migliore delle ipotesi.

drà un *avanzamento lavori* progressivo, senza lunghe interruzioni[13];

2. quello di rendere la rete nel suo complesso **robusta** nei confronti di eventuali problemi (momentanei o permanenti) di trasmissione lungo uno degli archi. Se ad esempio, durante una comunicazione (*flusso di pacchetti*), un canale *cade* (si interrompe per un guasto o viene considerato inutilizzabile per troppa congestione), ma esiste un percorso alternativo tra i due nodi coinvolti, allora è possibile reindirizzare il flusso attraverso il secondo percorso senza che i due estremi della trasmissione si accorgano di nulla[14].

La caratteristica della rete di scegliere percorsi arbitrari per ogni singolo pacchetto di una comunicazione permette una grande adattabilità alle variazioni di traffico. Il costo, per il ricevente, è un maggiore lavoro per la ricostruzione delle sequenze originali dato che in questo caso la probabilità di arrivi *fuori sequenza* è molto alta.

Chi (e come) valuta il **percorso *migliore*** - vedremo che il concetto di migliore/peggiore è molto aleatorio - per ogni pacchetto in transito?

Ogni nodo della rete ha una parziale conoscenza delle caratteristiche trasmissive e di utilizzo dei vari canali (archi entranti/uscenti) che lo collegano ad altri nodi per cui **può decidere dove** inviare i vari flussi secondo criteri di velocità pura, efficienza, opportunità, disponibilità, co-

[13]Nota bene: la capacità trasmissiva totale del canale ovviamente non cambia, viene semplicemente suddivisa su tutti i richiedenti che quindi sperimenteranno (subiranno!) una velocità di trasmissione *apparente* grossomodo equivalente (in realtà inferiore, di qualche punto percentuale) alla capacità totale divisa per il numero dei richiedenti contemporanei.

[14]O quasi, è probabile che si avvertano delle variazioni di velocità di trasmissione, sia a causa del tempo per accorgersi che il canale non funziona, sia per decidere il nuovo percorso e sia perché il nuovo percorso potrebbe avere caratteristiche trasmissive diverse. Inoltre aumenta la probabilità di ricevere i pacchetti fuori sequenza, specie se il *guasto* (motivo per cui si decide di cambiare canale) non è un guasto vero e proprio, ma semplicemente un momentaneo *clog* (ingorgo di traffico) che causa un *back and forth* (avanti e indietro) tra più canali alternativi.

sto ecc. Ad esempio, un nodo potrebbe scegliere per ogni pacchetto la *strada* (il canale):

- **meno trafficata**: ad ogni canale viene associata una coda di pacchetti da trasmettere, se la coda non è vuota il software di gestione del canale trasmette i vari pacchetti alla massima velocità possibile, il canale con la coda più corta è il meno trafficato;
- **meno costosa**: si pensi ad una configurazione *odierna* di un nodo con due canali, una ADSL (*Asymmetrical Digital Subscriber Line*) *flat* economica ma lenta (10Mbit/s) e un modem cellulare 4/5G (100Mbit/s) con un contratto a consumo, in questo caso, a meno di esigenze prestazionali particolari conviene indirizzare il traffico sulla linea economica per riservare la scelta costosa ai momenti di *reale bisogno*[15].

Ovviamente il criterio di scelta potrebbe essere differente tra nodo e nodo e, anche nel caso di utilizzo della stessa *policy* (e.g., canale meno costoso), non è detto, anzi è molto raro, che due nodi valutino il canale che li collega allo stesso modo. Infatti si immagini ad esempio la seguente situazione:

- un nodo N_1 collegato a N_2 dal canale $C_{1,2}$;
- N_1 è connesso ad altri 2000 nodi da altrettanti canali;
- N_2 invece è connesso solo a 4 altri nodi;
- N_1 spunta un prezzo per canale più basso dato che ottiene una *scontistica* (dal *provider* di connettività) di volume.

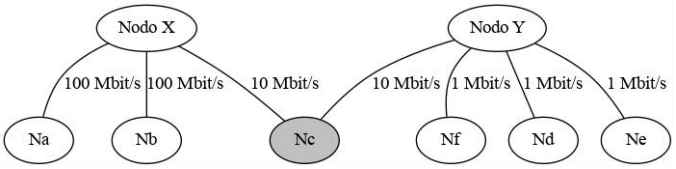
Cioè il canale $C_{1,2}$ viene **venduto a prezzi diversi** ai due estremi (clienti) della connessione.

Per applicare un ragionamento *di relatività* anche al criterio *velocità* basti pensare che in questo caso il concetto di *più veloce* è relativo al nodo che deve inviare: esso confronta la velocità di un canale con quelle degli altri canali che ha disposizione.

Vediamo un esempio *disegnabile*: se un nodo N_X ha 3 canali di cui 2 da 100Mbit/s e 1 da 10Mbit/s che lo collega a N_Y che ne possiede 4 di cui 3 (gli altri) da 1Mbit/s ecco

[15] Tipo vedere una puntata di un *talent show*.

che avremo lo stesso canale valutato come *il più veloce* da N_Y e come *il più lento* da N_X (si veda figura sottostante).



La complessità aumenta se pensiamo ad un percorso completo, cioè ad una catena di canali che collegano un generico nodo della rete ad un altro attraverso una serie di *connessioni* (*hop*, ovvero salto, è il termine tecnico): diventa infatti molto più difficile anche solo definire matematicamente una metrica. Come si può, ad esempio, definire il traffico[16] momentaneo lungo un percorso? Inoltre, anche quando riuscissimo a definire un criterio dovremmo poi implementarlo… e ci servirebbero le informazioni di stato di tutta la parte di rete interessata, insomma non certo un compito facile. A onor del vero dobbiamo aggiungere che le informazioni di stato della rete vengono divulgate… attraverso la rete stessa o su canali dedicati usando protocolli come ICMP (*Internet Control Message Protocol*) e BGP (*Border Gateway Protocol*) che permettono lo scambio di metadati sullo stato della rete. In questo modo i nodi possono ragionare sui percorsi potendo vedere un po' più in là del proprio *naso*, ma una vera e propria *onniscenza* non è possibile, per fortuna.

Le tecniche di *instradamento* dei flussi di pacchetti seguono qualche tipo di *algoritmo* 🕮 *di routing* e molti nodi intermedi della rete, quelli che si occupano solo[17] di instradamento prendono infatti il nome di *router* 🕮. Quelle

[16] Per la velocità è, invero, più facile dato che la velocità massima di una catena di canali è data dalla velocità del canale più lento, l'anello più debole.

[17] Finora abbiamo descritto una rete come se fosse fatta di nodi con doppio ruolo (computer per utenti e *macchine instradatrici*), ma nella realtà di oggi l'hardware viene solitamente dedicato ad uno solo dei due.

che noi abbiamo chiamato *strade* vengono in realtà indicate tecnicamente come *rotte*[18].

Ça va sans dire che chi controlla i router controlla la rete. Fortunatamente non esiste un singolo ente che controlli tutti i router del mondo, ma vedremo che il panorama non è roseo, specie se si ragiona a *livello nazione* (cioè a livello di interconnessioni fra paesi).

Ci rimane da quasi-definire un ultimo concetto legato alla rete e poi possiamo addentrarci nei meandri di quello che scopriremo essere un **assurdo universo**.

Il concetto che vorremmo definire, ma non potremo calcolare precisamente, nell'universo Internet è quello di ***distanza*** tra due nodi della rete. I *retisti* definiscono generalmente la distanza, declinata in termini *spaziali* e *temporali*, tra due nodi di una rete come:

- numero di salti/*hop* tra i due nodi;
- tempo di percorrenza di pacchetti *speciali* (ICMP - Internet Control Message Protocol - *echo request*) che vengono inviati e di cui si misura il tempo di ritorno, il cosiddetto *ping time*[19].

Sembra molto facile, no? Purtroppo non lo è, infatti intervengono diverse **distorsioni**, alcune già descritte, che ci impediscono di misurare efficacemente questi parametri, ad esempio:

- i pacchetti *speciali* subiscono comunque l'instradamento;
- i pacchetti *speciali* potrebbero non essere degnati di risposta;
- le rotte possono cambiare da un istante all'altro (per guasti o scelte sistemiche);
- le code sui router potrebbero venir servite *con calma*, cioè non alla massima velocità possibile disponibile sul canale, questo succede se si associano più code allo stesso canale, servite con priorità diverse;

[18] Nel senso nautico del termine, non in quello del verbo *rompere*.

[19] La metafora, non a caso il nome è *ping*, è quella di un sonar che invia un impulso sonoro, attende l'eco (che torna se incontra un oggetto *fono-riflettente*) e calcola la distanza percorsa in base alla velocità del suono. Lo strumento software si chiama proprio `'ping'`.

A dimostrazione dell'impossibilità di avere una misurazione stabile mostriamo un esempio di uso dello strumento `'traceroute'` che combina la funzionalità del `'ping'` con la possibilità di *tenere traccia della rotta* seguita dal flusso di pacchetti. I numeri di 4 cifre separate da un '.' sono indirizzi di rete (cfr. box 0.1.1): identificano un generico nodo in maniera univoca. Con il `'traceroute'` proviamo a tracciare la rotta tra il computer dello scrivente fino a raggiungere *google.it*, eseguito il comando otteniamo:

```
traceroute to google.it (216.58.198.35), 64 hops max
  1   192.168.42.1      0,906ms  0,948ms   0,840ms
  2   192.168.1.254     1,352ms  1,328ms   1,327ms
  3   10.2.3.64        73,236ms 85,416ms  88,793ms
  4   10.250.132.194   93,630ms 99,994ms 104,121ms
  5   151.6.24.2       37,905ms 38,861ms  39,225ms
  6   151.6.2.48       40,432ms 43,488ms  25,163ms
  7   151.6.1.235       8,075ms  8,325ms   7,222ms
  8   93.63.100.182    72,365ms 33,447ms   6,439ms
  9   72.14.204.46      7,380ms  7,686ms   7,154ms
 10   216.239.48.231    8,139ms  7,182ms   7,461ms
 11   216.239.48.229    9,339ms  7,310ms   8,869ms
 12   216.58.198.35     7,185ms  7,091ms   7,200ms
```

Cioè 12 salti e meno di una decina di *ms* (il tempo che ci interessa è quello della riga 12) per il tempo di percorrenza… Però riproviamo dopo soltanto un minuto e stavolta otteniamo:

```
traceroute to google.it (216.58.198.35), 64 hops max
  1   192.168.42.1   1,080ms  0,948ms  1,005ms
  2   192.168.1.254  1,886ms  1,413ms  1,350ms
  3   10.2.3.64      6,218ms  5,336ms  5,784ms
  4   151.6.24.78    7,439ms  5,886ms  6,982ms
  5   10.251.47.186  7,764ms  8,038ms  6,368ms
  6   10.254.12.237  6,754ms  6,520ms  6,903ms
  7   151.6.6.77     7,611ms  6,929ms  7,293ms
  8   74.125.32.80   7,886ms  7,531ms  8,621ms
  9   216.239.48.229 8,672ms  7,799ms  6,715ms
 10   216.58.198.35  7,558ms  8,050ms  6,893ms
```

Cioè una strada completamente diversa per numero di *hop* e tempi di percorrenza.

Stiamo *osservando*[20] l'effetto del *routing* applicato al nostro flusso di informazioni: i vari router lungo il percorso si sono coordinati tra loro (o sono stati orchestrati da uno o più gestori comuni, ma il risultato finale non cambia) per decidere quale strada fosse *migliore* all'istante T_1 e al successivo T_2.

A questo punto il lettore avrà compreso come sia impossibile definire un qualunque concetto di distanza misurabile in maniera riproducibile e stabile nel tempo: infatti non rimane costante alcun fattore, né numero e sequenza di salti, né tempistiche di percorrenza.

C'è da aggiungere un ulteriore e importantissimo aspetto, che peggiora questo quadro già negativamente complesso: le misurazioni effettuate tramite strumenti come `'ping'` e `'traceroute'` sono applicabili al resto del traffico che riceviamo o trasmettiamo successivamente?

La risposta è NO.

Infatti non tutti i pacchetti sono trattati allo stesso modo, ma **è possibile applicare rotte diverse (e gestioni *ad hoc* delle code sui router) a flussi diversi**. Come nella famosa frase "Tutti gli animali sono uguali, ma alcuni sono più uguali degli altri" [Orw45].

Come è possibile? Vediamolo addentrandoci brevemente nella struttura del traffico di rete.

0.1.1 Mini-esegesi di TCP/IP

> `Tutti i pacchetti sono uguali, ma alcuni sono più uguali degli altri.`
>
> *Parafrasi da "Animal Farm" [Orw45]*

Il cuore del ragionamento che stiamo per fare risiede nella definizione di una *funzione di routing*, un artificio

[20] Si fa per dire perché a brevissimo distruggeremo anche il termine *osservare*.

quasi-matematico[21] che ci permetta di capire quali sono i fattori che entrano (o che potrebbero entrare) in gioco nella decisione sulla strada che deve percorrere un pacchetto. La strada (intesa appunto come sequenza di nodi da attraversare) prevista per un pacchetto p all'istante t è una funzione: $strada(t, p, contorno)$

Nel senso che la decisione avviene in base al *quando*, al *cosa* e a qualche fattore esterno (contorno) che si vuole utilizzare per decidere. Il *quando* può essere il giorno della settimana o l'orario attuale. Il *cosa* si riferisce a informazioni contenute nel pacchetto p stesso: i dati e i *metadati*[22]. Il *contorno* può essere la situazione di congestione di traffico su nodi della rete adiacenti o il tempo atmosferico in quel momento[23].

Quindi dobbiamo avere almeno un'idea[24] di cosa possa esserci di tanto interessante in un pacchetto di rete.

Un pacchetto di rete non è altro che una sequenza di *bit* 🕮 di lunghezza finita che viene trasmessa sotto forma di segnale elettrico (rame) o luminoso (fibra ottica) da un nodo all'altro di una rete.

Ogni segmento (detto *campo*) della sequenza ha una ben precisa semantica dipendente dal tipo di protocollo di rete utilizzato, noi ci riferiamo all'insieme di protocolli TCP/IP. Per descrivere i vari campi si usano schemi come quello presentato in figura 2, dove abbiamo estratto[25] solo alcuni dei campi interessanti (ai fini del ragionamento sul *routing*) dei pacchetti che girano in una rete TCP/IP.

La figura 2 ci mostra alcuni campi, quelli che riteniamo esemplificativi per capire come si possano prendere decisio-

[21] Qui la descriviamo con un *formalismo* (molto banale) matematico, nella realtà viene implementata via software.

[22] Usando la metafora della posta fisica (*snail mail*): l'indirizzo del destinatario scritto sulla busta è un metadato, la lettera contenuta è il dato.

[23] Questo è uno scherzo naturalmente, ma nulla vieta di prenderlo in considerazione.

[24] Per approfondimenti cfr. "*Computer Networks*" [TW12]

[25] Rispettivamente dai contesti IP (basso livello OSI), UDP (pacchetti singoli), TCP (sequenze di pacchetti), cfr. il già citato [TW12].

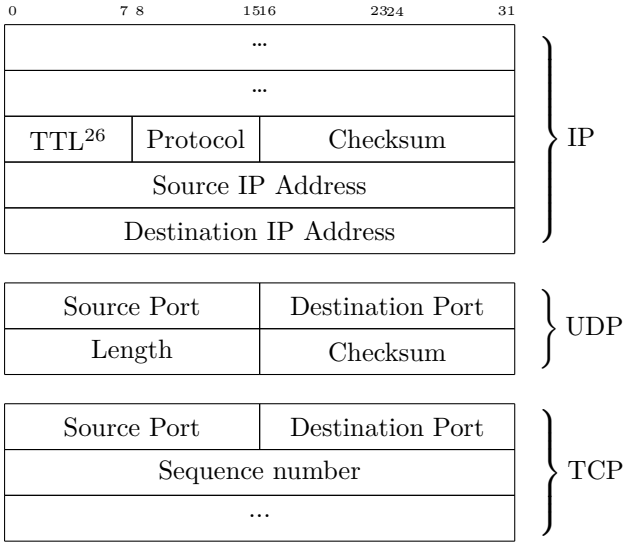


Figura 2: Informazioni *interessanti* nei pacchetti

ni sulla vita (e la morte) dei vari pacchetti, che transitano in rete, vediamoli:

- *TTL (Time To Live)*: un contatore che viene decrementato ogni volta che il pacchetto passa da un router, quando il contatore va a 0 il pacchetto viene scartato e *muore*;
- *Protocol*: tipo di protocollo, informazione che aiuta chi riceve il flusso di dati a capirne la semantica;
- *Checksum*: valore di controllo per capire se il pacchetto è integro;
- *Source IP Address*: indirizzo sorgente (*mittente*), il ricevente di un flusso dati sa da dove arriva (o dichiara di arrivare) l'informazione;
- *Destination IP Address*: indirizzo destinatario;
- *Source Port* e *Destination Port*: il concetto di *porta* serve a differenziare un flusso dati tra due nodi in modo da simulare più sotto-flussi, i.e., i pacchetti che vanno da A a B vengono smistati su code diverse in funzione delle *porte* dichiarate nei pacchetti stessi;

- *Length*: lunghezza, altro dato di controllo;
- *Sequence number*: numero di sequenza, quando un flusso dati generico deve essere *ordinato* (ad esempio i frame di un video che non devono essere visualizzati in ordine sbagliato) il numero di sequenza permette la flessibilità di inviare pacchetti senza *preoccuparsi troppo della strada che faranno* perché lato ricezione sarà sufficiente memorizzarli temporaneamente[27] per poterli riordinare prima di presentarli all'utente.

Cosa può succedere se vengono utilizzati o, peggio, vengono modificati i metadati di un pacchetto durante il suo viaggio attraverso una rete TCP/IP? Facciamo qualche esempio banale e intuitivo, iniziando dalla semplice **lettura** dei metadati:

- **In funzione del destinatario**: un router potrebbe decidere di inviare tutti i pacchetti destinati ad un particolare indirizzo IP (o *range*) scegliendo una via più lenta/veloce, sfavorendo/favorendo **quel destinatario** nella velocità di ricezione dei pacchetti; Esempio: un fornitore di contenuti video potrebbe scegliere strada più lenta[28] verso paesi da cui *estrae* minor profitto;
- **In funzione del mittente**: idem come sopra, ma lato invio;
- **Porta/Protocollo**: è possibile decidere, a parità di coppia mittente-destinatario, di (s)favorire un particolare tipo di protocollo, al limite perfino impedendo in toto l'uso di certi protocolli; frequentissimo è il caso di reti *istituzionali* (aziende, scuole ecc.) che limitano l'uso di protocolli ad una lista minimale (tipicamente HTTP(S) e poco altro) impedendo una fruizione completa dei servizi di rete da parte degli utenti che, ad esempio, possono navigare sul web

[27] In un cosiddetto *buffer*, da cui l'avviso *buffering* che si vede spesso guardando un video in rete.

[28] I protocolli video sono *adattativi*: se misurano basse velocità si adeguano inviando meno informazione, cioè video a risoluzioni e *frame rate* inferiori.

ma non possono inviare posta elettronica o ascoltare musica (se non passando attraverso *gateway* web);

E ora vediamo cosa si può fare **modificando** i metadati:

- **TTL**: un TTL elevato fa sì che il pacchetto possa *andare lontano*, cioè raggiungere destinazioni a molti *hop* di distanza, se si modifica (tipicamente abbassandolo) il TTL si rende un pacchetto meno longevo e lo si *confina* ad un raggio d'azione limitato superiormente;
- **destinatario**: modificare il destinatario in un flusso di pacchetti significa redirigere informazione, mandare dati che erano intesi per un certo ricevente ad un ricevente diverso, senza che il mittente si accorga (a meno che non chieda una conferma, che però può essere *forgiata*[29] dai router che modificano il metadato stesso);
- **mittente**: modificare il mittente implica che il destinatario vede arrivare informazione da un mittente falso o non identificabile facilmente;

E se invece che ai metadati si puntasse al **contenuto**?

Dal punto di vista computazionale analizzare e/o modificare il contenuto di un pacchetto invece dei metadati comporta solo un maggior costo di elaborazione perché il contenuto di un pacchetto consiste in un maggior numero di byte (con formati non sempre standard) da trattare e, salvo l'uso di crittografia, i dati in un pacchetto viaggiano *in chiaro*, cioè sono perfettamente leggibili da chiunque… e un router potrebbe tranquillamente modificare un pacchetto prima di *ruotarlo*[30], operando quello che viene chiamato *Man-In-The-Middle attack*.

Infatti, storicamente, man mano che la potenza computazionale è andata crescendo ha sempre più preso piede e

[29] A meno di non utilizzare particolari tecniche crittografiche.

[30] Pratica valida per scopi utili nel caso delle cosiddette reti *NAT-tate* (da NAT=Network Address Translation) in cui l'indirizzamento interno segue logiche di assegnazione degli indirizzi non vincolate e il traffico verso l'esterno appare provenire da un singolo nodo, il *gateway*.

si è affinata la cosiddetta tecnica del *deep packet inspection* (DPI, ispezione profonda dei pacchetti), che prevede l'analisi non solo dei metadati ma anche del contenuto (tenendo perfino una traccia *storica*) dei pacchetti che vengono instradati. Con la DPI è possibile controllare[31] **ogni** aspetto di tutta l'informazione veicolata su Internet, consentendo quindi - tipicamente ai governi e alle aziende che gestiscono la Rete - di esercitare il **controllo sistematico del contenuto** delle comunicazioni su intere *zone* di Internet e di conseguenza decidere **cosa** può essere comunicato, **chi può comunicare** e **chi può ricevere la comunicazione**.

[31] Ribadiamo: salvo crittografia *robusta*. Ma esistono casi di reti (o proposte di legislazione scellerate) in cui viene bandito il traffico se viene riconosciuto come crittografato.

TECHBOX: Indirizzi IP [0.1.1]

L'*indirizzo* IP è un identificativo **univoco** di un nodo, un computer. La sua forma[a] è una sequenza di 4 numeri, ognuno tra 0 e 255, separata dal carattere `'.'`, ad esempio 192.168.39.12 identifica il il nodo 12 della sottorete 39 della sottorete 168 della sottorete 192 della rete complessiva. Alcuni indirizzi IP hanno significati speciali come 127.0.0.1 che identifica sempre il nodo su cui ci si trova o il numero 255 che identifica tutti i nodi di una sottorete come 192.168.1.255. Esistono anche insiemi di indirizzi che hanno uno scopo convenzionale come quelli della forma 10.x.x.x che indicano una rete locale. Ogni nodo di una rete può in teoria autoassegnarsi un indirizzo, ma dato che l'univocità è una caratteristica fondamentale per non avere *conflitti*[b] solitamente gli indirizzi vengono assegnati da una *autorità centrale* (relativamente ad una sottorete) che tiene traccia degli assegnamenti per non creare duplicati.

[a] Versione IPv4 comunemente usata, non tratteremo IPv6.

[b] Due nodi con lo stesso indirizzo non riescono a comunicare con nessuno perché le informazioni non riescono ad essere, appunto, *indirizzate* correttamente

0.2 Relatività

Eccoci quindi pronti, a valle di una introduzione ai concetti di base, ad affrontare uno dei *princìpi* della Rete che ci preme associare alla Cittadinanza Digitale, mutuato dal mondo della Fisica, cioè l'affermazione che:

La Rete è relativistica

Non possono esistere due osservatori che vedono la Rete allo stesso modo.

Nel mondo fisico relativistico due osservatori non possono osservare un evento nello stesso istante a causa della velocità della luce (massima velocità di propagazione di un'informazione).

Nel mondo digitale si sperimenta un effetto analogo, ma di ben peggiore entità. I fotoni del mondo fisico diventano, metaforicamente parlando, i pacchetti che circolano trasportando informazione e la peggiore entità dell'effetto è dovuta alla enorme variabilità (vista in sezione "*Internet*" - 0.1) della propagazione. Variabilità naturale[32], ma anche imposta *politicamente*, sia nel senso mutuato dall'inglese *policy* che in quello più interessante e critico di *politica* intesa come decisione di un potere politico.

Se aggiungiamo anche la possibilità di **alterazione**[33] dell'informazione ecco che delineiamo un ambiente completamente opposto a quello fisico e prevalentemente trasparente a cui siamo abituati: la Rete è un sistema opaco, dagli echi variabili, difficile da esplorare e in cui non è banale comunicare garantendo l'autenticità e la riservatezza delle comunicazioni. Un universo assolutamente *non euclideo*[34] in cui le *regole geometriche* non sono completamente note, inoltre variano nel tempo e, soprattutto, sono sotto il controllo di poche entità: i gestori delle reti.

[32] Dovuta alla complessità topologica della Rete.

[33] Modifica dei pacchetti (sia dati che metadati) lungo la strada.

[34] Dove ad esempio i concetti di distanza non rispettano i principi classici, ad esempio la distanza fra i punti A e B è diversa dalla distanza fra B e A.

Poniamoci quindi le seguenti domande:

- "se non trovo un sito è perché non esiste?"
- "se i dati arrivano lentamente è colpa del server?"
- "se io vedo un sito lo vedono tutti?"

La risposta è "no" a tutte, vediamo perché.

Intanto distinguiamo cosa si intende con *trovare*, ci sono almeno due accezioni del verbo:

- conosco il nome/indirizzo del sito, mi connetto ed effettivamente *trovo* un servizio che risponde alle mie richieste di informazione;
- non conosco il nome/indirizzo del sito e lo cerco tramite un *motore di ricerca* 🕮 che mi propone un elenco di possibili risultati a fronte di un set di parole chiave che fornisco.

Nel primo caso, a fronte di un *URL* 🕮 che già conosco ottengo (se all'altro capo della connessione c'è qualcuno che risponde) un'informazione, un contenuto.

Nel secondo caso, dato che non conosco l'URL devo prima farmelo dire da qualcuno che lo conosce fornendo alcune informazioni sul contenuto che sto cercando. La *domanda* che posso fare ad un *motore di ricerca* (MdR) è del tipo: "quali URL puntano a contenuti correlati alle seguenti parole chiave?". Il MdR mi fornirà, secondo il suo personalissimo giudizio, un elenco di URL (corredati di un piccolo sunto del contenuto) relativi alle parole chiave inserite, starà a me scegliere dalla lista l'URL che ritengo più utile ai fini della mia ricerca.

Metaforicamente parlando si potrebbe dire:

- conosco l'indirizzo di un luogo dove devo andare, mi ci reco e trovo effettivamente l'edificio che mi aspettavo;
- non conosco l'indirizzo, ma solo un nome (ad es. "Ristorante Da Mario"), lo cerco tramite un call center telefonico (o chiedo ad un vigile o ad un tassista) che mi fornisce l'indirizzo, mi reco all'indirizzo fornito, trovo un posto che corrisponde.

La metafora funziona fino ad un certo punto dato che nel mondo reale è abbastanza facile capire se il luogo dove

siamo stati *indirizzati* è quello che ci aspettavamo o una *sòla*. Su Internet, invece, non è sempre banale riconoscere un sito buono da uno fasullo come ci insegnano i numerosissimi tentativi (che spesso vanno a buon fine!) di *scam* 🕮 che riceviamo via mail e che ci invitano ad *aggiornare le credenziali del conto corrente* indirizzandoci (appunto!) verso siti il cui URL e homepage **assomigliano** al sito reale della nostra banca.

Per il momento ci limiteremo al primo significato di *trovare*: conosco l'URL, mi collego (o quantomeno ci provo).

Aggiungiamo ora alla nostra ricetta anche:

- la conoscenza (cfr. box 0.2.1) di come funziona il meccanismo del DNS;
- tutto ciò che abbiamo detto poco sopra a proposito dell'instradamento dei pacchetti.

Siamo ancora sicuri delle affermazioni fatte sopra? O piuttosto non ci potrebbe venire in mente che:

- un URL viene risolto diversamente a seconda del DNS a cui ci si rivolge?
- a valle di aver risolto un URL in un indirizzo IP raggiungo o meno quel nodo della Rete in funzione del *dove mi trovo* all'interno della Rete stessa?
- anche se raggiungo il nodo correttamente esso mi fornisce contenuti diversi in funzione del *dove mi trovo*, *da dove arrivo*? (questo punto è trattato nel capitolo "*Livello 1 [services]*" - 1)

Al lettore eventualmente ancora scettico vorremmo proporre un piccolissimo esperimento di verifica della raggiungibilità di un sito web censurato. Usando lo strumento `'dig'` è possibile effettuare delle richieste al DNS per sapere l'indirizzo IP di un nodo della Rete conoscendo il suo nome simbolico, ad esempio il risultato di `'dig wikipedia.org'` è: "wikipedia.org → 91.198.174.192".

Se invece proviamo un sito un po' *particolare*, uno che è stato *oscurato* in Italia[35] otteniamo un'informazione *strana*, il risultato di `'dig btmon.com'`[36] è infatti: "btmon.com

[35] Al giugno 2019.

[36] Utilizzando i DNS di *default* 🕮 fornito dal proprio *ISP* 🕮

→ 127.0.0.1" che è strano perché 127.0.0.1 è un indirizzo che nello standard IP si riferisce al computer su cui si sta lavorando, si potrebbe tradurre in italiano con "me stesso". E come mai un tale indirizzo simbolico, che è normalmente registrato[37] per certo, viene *risolto* con un indirizzo inutile[38]?

Succede che il sito è *particolare* perché si riferisce ad un server di scambio file *peer-to-peer* 🕮 e come tale è stato legalmente bandito sul territorio italiano mediante ordinanza di un tribunale, ergo ogni singolo provider, sempre sul territorio italiano (precisione/sottolineatura che diverrà chiara a brevissimo), deve ottemperare e quindi è costretto a fornire **un indirizzo sbagliato di proposito** a fronte di una richiesta DNS. Per avere un'idea di quali e quanti domini/siti siano stati bloccati si veda ad esempio *http://censura.bofh.it/elenchi.html*.

Ecco perché sottolineavamo il *territorio italiano*[39], infatti se effettuiamo la stessa richiesta di informazione aggirando il sistema DNS nazionale, ad esempio usando Tor[40] o dei DNS server sovranazionali come *http://opennic.org* o *http://dns.watch*, ecco che *magicamente* l'URL viene risolto correttamente e quindi appare normalmente aprendolo con un browser (cfr. figura 3). Per dovere di cronaca mostriamo anche il risultato della query DNS effettuata su un server esterno (in particolare *http://dns.watch*):

`'btmon.com → 91.213.8.70'`

Questo è un **perfetto esempio di Rete relativistica**: osservo una topologia/toponomastica diversa in funzione di dove mi trovo, a meno di accorgimenti particolari come rivolgersi a DNS server non di default, usare *proxy* 🕮 ecc.

[37] Si può verificare a chi appartiene usando un altro strumento chiamato `'whois'` che fornisce i dati del *registrante*.

[38] Inutile perché se cerco di aprire un browser puntando *btmon.com* non ottengo nulla di interessante: tipicamente un errore ("non trovato") o una pagina che nulla ha a che vedere col sito in oggetto.

[39] Potrebbe essere anche europeo o altro, dipende da chi emette l'ordinanza

[40] *http://torproject.org*

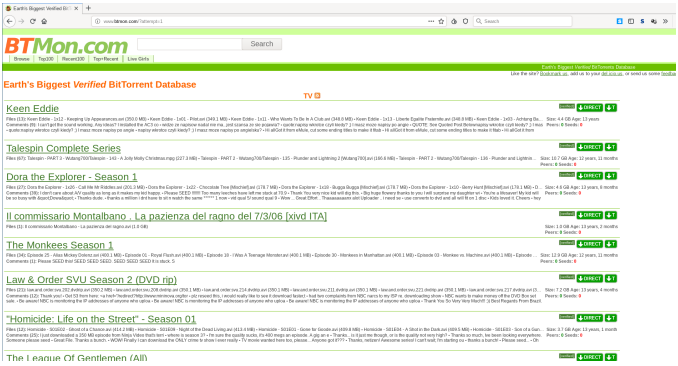


Figura 3: Il sito `btmon.com` raggiungibile via Tor

Oltre al semplice e facilmente aggirabile *filtro DNS*, per nascondere parti della Rete esistono tecniche ben più efficaci, sono i cosiddetti *firewall* 🕮 che decidono se un certo traffico è *lecito* e va quindi permesso, oppure no e viene quindi bloccato: in questo secondo caso i pacchetti **non** vengono instradati e chi ha originato il traffico vede solo dei *timeout* 🕮 di connessione. Lo strumento *firewall* può essere applicato indipendentemente dal *filtro DNS*: il solo firewall senza filtro DNS permette la risoluzione di un URL *illecito* che poi però non viene raggiunto. Usualmente i due strumenti vengono integrati e tutte le richieste verso siti non permessi vengono rediretti ad un cosiddetto *captive portal* (raggiungibile, non bloccato dal firewall), un sito molto semplice che contiene un più o meno dettagliato avviso che spiega il motivo della non raggiungibilità del sito richiesto.

Esempi se ne possono incontrare a iosa, basta farci caso, eccone qualcuno.

Praticamente tutte le **reti aziendali** hanno dei *firewall* anche in uscita: essi servono a regolamentare la consultazione dei siti Web limitatamente a quelli *consentiti* (approvati da una qualche commissione/dirigenza). Molte aziende infatti ritengono che l'accesso incontrollato al Web da parte dei dipendenti sia un *male* per cui decidono a ta-

volino una lista di siti *leciti* (utili a scopo lavorativo, alla *mission* aziendale) che quindi sono visibili dai browser sui PC aziendali. Viene cioè adottato un meccanismo cosiddetto a *whitelist* (tutto bloccato tranne ciò che è presente in lista)[41].

Anche se non propriamente legato al rapporto azienda-dipendente, ma ad un più generico fornitore-utente, sono capitati recentemente (2019) ad uno degli autori dei fatti curiosi o seccanti che illustrano la relatività della Rete:

- curioso: in coda in ufficio postale, dove c'è WiFi gratuito, cliccando su un link in un post Facebook verso Dagospia (sito più o meno legato al *gossip*) lo si è scoperto inaccessibile, per verificare che non fosse *giù* il sito è bastato spegnere il WiFi del telefono e usare la connessione 3G per vedere i contenuti richiesti;
- seccante: in albergo in Francia, tramite il WiFi offerto dalla struttura, impossibilità di connettersi tramite connessione *SSH* 📖;
- seccante: la rete *eduroam*[42] è molto *filtrata* sia in ingresso che in uscita, ad esempio non è possibile collegarsi a molte *web radio* che trasmettono su porte diverse dalla 80.

Purtroppo possiamo citare anche esempi su più larga scala: a livello internazionale ci sono parecchi casi di relatività imposta artificialmente, descritti in sezione "*L'universo distorto*" - 0.2.1.

Rimane da dirimere la questione della velocità di trasmissione percepita ("i dati arrivano lentamente..."). Diciamo che abbiamo volutamente semplificato la domanda/dubbio, in effetti chi frequenta la Rete utilizzandola pesantemente (ad esempio per multimedia) potrebbe sperimentare rallentamenti di vario genere e magari potrebbe attribuirli non solo al server fonte del flusso di dati, ma anche al device in uso o al tipo di connessione (3G vs.

[41] Il meccanismo simmetrico, detto a *blacklist* funziona in maniera opposta: tutto permesso tranne ciò che è presente in lista.

[42] WiFi accademico con login centralizzato valido in tutte le università del mondo.

ADSL vs. VDSL vs. fibra ottica), in effetti ci concentreremo proprio sulle caratteristiche relativistiche della Rete per discutere sui motivi delle prestazioni più o meno buone della fruizione di contenuti.

In quali occasioni mi posso accorgere della velocità di trasferimento dei dati?

- cerco di vedere un video, ad esempio da Vimeo/YouTube/ecc.
- cerco di scaricare una immagine ISO[43]
- voglio mandare un allegato particolarmente grosso[44]
- voglio fare una *conference call* audio/video, in questo caso si noti che il canale viene stressato sia in *giù* (download) che in *su* (upload) perché una video chiamata prevede che entrambi gli interlocutori si possano vedere tramite webcam
- faccio un upgrade del software installato sul mio computer
- apro una pagina web particolarmente *complessa*, ad esempio contenente molto codice *JavaScript* 🕮
- faccio un backup del mio computer verso un mio server

Quali effetti o difetti potrei sperimentare in questi casi? Nel caso di un canale video potrei vedere le immagini *sgranate*[45] o a scatti o con delle pause (il cosiddetto *buffering*), sull'audio potrei sentire la voce diventare metallica o interrotta a tratti, nel caso di download (ISO, upgrade, pagina web) o upload (backup, email con allegati) osserverei tempi *biblici* (ore o addirittura giorni!) di completamento dell'operazione.

[43] Un file tipicamente grosso (da qualche centinaio di MB fino a qualche GB) che rappresenta il contenuto di un CD o un DVD e che si può usare per *bruciare* un CD/DVD fisico da utilizzare in un lettore. Il caso più frequente lo si incontra quando si scaricano le immagini ISO dei CD/DVD di *bootstrap* per installare un sistema operativo.

[44] Anche se molti server email limitano - giustamente - gli allegati a qualche decina di MB.

[45] Molti protocolli di trasmissione video si adattano alla capacità del canale eventualmente riducendo la qualità (risoluzione e/o nr. di *frame* inviati nell'unità di tempo) del flusso stesso.

A chi possiamo attribuire la colpa di questi effetti? La catena di trasmissione del dato è composta dal server produttore di contenuti, dalla rete che connette il server al fruitore e infine dal computer del fruitore. Ognuno di questi anelli della catena può introdurre effetti, ovviamente l'anello più debole è quello che influenzerà la qualità della fruizione:

1. Il server è lento o sovraccarico, caso attualmente raro dato che le maggiori piattaforme di distribuzione contenuti (Vimeo, YouTube ecc.) sono in realtà grossi ammassi (*cluster*) di server contenenti gli stessi media in modo da poter servire un gran numero di richieste senza rallentamenti. Accade solo quando si cerca di fruire un contenuto immagazzinato su server singoli (ad esempio una ISO di un *progettino amatoriale* magari gestito in casa da una piccola *community*), è tutto sommato facilmente diagnosticabile, è fisiologico e non gli associamo alcuna dietrologia, si tratta semplicemente di mancanza di risorse alla fonte.
2. Dispongo di una connessione *ultimo miglio* 🕮 lenta, indipendentemente dalla capacità trasmissiva del server, se la mia connessione a Internet è *debole*, ad esempio sto usando una connessione ADSL da 7Mbit/s (meno di 1MB/s)[46] o sono molto distante dal mio router WiFi, il massimo che potrò ottenere sarà la velocità massima della mia connessione, indipendentemente da qualunque altro fattore. Anche in questo caso è facilmente diagnosticabile: la lentezza è costante e indipendente dal contenuto che si vuole raggiungere. E ancora non vogliamo associare alcuna particolare dietrologia (salvo quella della *scarsità artificiale* di cui parleremo), si tratta semplicemente di mancanza di risorse lato fruitore.
3. Sto usando un PC poco *prestazionale* o magari so-

[46] Il video ad alta risoluzione come il 720p o il 1080p richiede una banda maggiore, rispettivamente 12 Mb/s e 22 Mb/s a meno di non usare protocolli *lossy* 🕮.

vraccarico che non riesce a elaborare il flusso di dati abbastanza rapidamente. Dato l'attuale costo bassissimo dell'hardware questo problema è facilmente risolvibile aggiornandolo con qualcosa di più recente e potente, in alternativa può essere sufficiente la semplice installazione di sistemi operativi più *efficienti* a parità di hardware. Ancora nessuna dietrologia e ancora mancanza di risorse lato fruitore.

4. Router vari sul percorso del flusso dati che *influenzano* la velocità di trasmissione complessiva. Questa è una situazione complicata da diagnosticare, nel senso che non è banale misurare quanta *colpa* è attribuibile al percorso di rete rispetto al resto (inizio e fine) della catena

Approfondiamo l'ultimo punto attraverso qualche cenno economico-politico. Negli ultimi anni, a partire dal 2010 circa, si è mosso un (si fa per dire) sottobosco di grandi aziende verso una monetizzazione sempre più spinta del traffico di rete, spesso a scapito degli utilizzatori finali. La stampa internazionale, molto più attenta rispetto a quella italiana, ha seguito questi tentativi commerciali e politici[47] da vicino. Anche a livello di movimenti *grassroots* (gruppi spontanei auto-organizzati) e di associazioni di categoria l'attenzione è stata alta e alcune organizzazioni a difesa del Software Libero come EFF (Electronic Frontier Foundation[48]) e FSF (Free Software Foundation[49]) negli Stati Uniti hanno promosso petizioni e azioni di (purtroppo blando) *lobbying* nei confronti degli organi di governo.

Lobbying contro cosa? Quali pratiche commerciali, che i big player vogliono rendere legali (ecco il *politicamente*), si possono applicare sul traffico di rete per renderlo più remunerativo? Semplice, basta applicare tariffe differenziate

[47] La tecnologia di rete non è cambiata poi così tanto nel corso degli ultimi anni: sono migliorati i supporti fisici (dal rame alla fibra ottica) ed è quindi aumentata la capacità di trasmettere dati, ma i principi di gestione software sono rimasti gli stessi. Ergo si deve lavorare su altri livelli per *estrarre denaro*.

[48] `http://eff.org`

[49] `http://fsf.org`

rispetto al **tipo di traffico**, un provider di connettività può implementarlo:

1. *lato fornitore*, contrattando con i produttori di contenuti accordi commerciali per favorire il loro traffico rispetto ai produttori che non pagano o pagano meno, in questo caso i produttori minori vengono sfavoriti e rischiano di uscire dal mercato [Eud11b];
2. *lato utente finale*, vendendo abbonamenti differenziati, ad esempio fornendo una connettività di base più un sovrapprezzo per fruire alcune fonti (Netflix, Prime Video ecc.) a velocità maggiore per poter sfruttare risoluzioni maggiori (HD, 4K ecc.), in questo caso gli utenti meno abbienti usufruiscono di un servizio di minor qualità;
3. *ibrido*, nel contesto della telefonia cellulare si assiste spesso al caso di offerte *flat*, cioè con traffico dati incluso nell'abbonamento, fino ad una soglia mensile[50] oltre la quale si comincia a pagare *al MB* o la velocità della connessione scende automaticamente ad un livello di pura *sopravvivenza*[51]. Alcune offerte prevedono che parte del traffico effettuato **non** venga conteggiato nel *cap* mensile così l'utente del contratto telefonico sarà invogliato a utilizzare maggiormente i siti *cap esenti*. Guarda caso i siti esenti sono quelli del primo punto di questa lista.

Un bellissimo video tragicomico[52], realizzato qualche tempo fa da un attivista tedesco[53] spiega perfettamente ciò che stiamo raccontando, riuscirete a vederlo dalla vostra connessione?

Il primo esempio noto è quello di **Comcast** (provider USA) che nel 2006 ha bloccato in toto (l'estremo rallentamento) un certo tipo di traffico, in particolare quello

[50] Quest'anno (2019) gli ordini di grandezza dei *data cap* 🕮 mensili vanno dai 10GB fino a 100GB per alcune offerte top gamma.

[51] Si riesce cioè a malapena a navigare pagine web non troppo pesanti, scambiare mail, eccetera, ma non sufficiente ad esempio a vedere video online.

[52] `http://youtube.com/watch?v=NLKyIhYwyWc`

[53] `http://alexanderlehmann.net`

peer-to-peer 🕮, la già citata EFF in quel periodo realizzò uno studio tecnico che dimostrava che Comcast, nel cercare di bloccare il traffico P2P, degradava la qualità della connessione anche nei confronti di traffico considerato legittimo [Eud11a]. Inoltre la FCC (Federal Communications Commission[54]) aveva anche scoperto che Comcast impediva l'utilizzo di Skype (telefonia via rete, la cosiddetta VOIP - Voice Over IP) ai suoi utenti. Da quella situazione è scaturita una battaglia legale che, purtroppo, dopo alcuni anni ha dato ragione a Comcast. Sempre Comcast, nel 2014, è stata nuovamente indagata dalla FCC per sospetti di *rallentamento artificioso* nei confronti di Netflix[55]. Nel 2009 **AT&T** impedì ai suoi utenti l'accesso a Skype e FaceTime[56]. Nel 2011 **MetroPCS** bloccò in toto lo streaming video tranne che per il traffico proveniente da YouTube[57]. L'ipotesi è che tale scelta fosse il frutto di un accordo [Bro13] *sottobanco* tra MetroPCS e Google[58]. Nel 2012 **Verizon** bloccò l'accesso ad alcune applicazioni mobili [Eha12]. Qualche anno dopo, nel 2015, di nuovo alla carica con l'applicazione del cosiddetto *data cap* 🕮 per indirizzare l'utenza verso fonti *preferite*[59].

L'implementazione di queste tecniche prende il nome di *discriminazione* (per protocollo o per indirizzo IP) sia nel senso tecnico neutro di *differenziazione*, ma soprattutto nel senso più deteriore di *esclusione*: i dati provenienti da (o destinati a) alcune zone della Rete hanno meno diritto di percorrerla… forse non è un caso che ACLU si senta chiamata in causa[60], questa è una forma di *razzismo* applicato

[54] *http://fcc.gov*

[55] *http://vox.com/2014/6/13/5807392/the-fcc-is-investigating-comcasts-treatment-of-netflix*

[56] *http://www.wired.com/2009/10/iphone-att-skype*

[57] *http://www.smithsonianmag.com/innovation/how-other-countries-deal-net-neutrality-180967558*

[58] Youtube è di proprietà di Google/Alphabet.

[59] *http://bgr.com/2015/04/01/verizon-video-service-net-neutrality*

[60] Il lettore ricordi l'Alabama, USA, degli anni '50 del novecento (*http://aclualabama.org/en/news/aclu-archives-selma-montgomery-marches*).

ai *byte* 🕮 e quindi alle informazioni che veicolano. Quando la discriminazione è portata all'estremo prende il nome di **censura**.

Esiste in molte federazioni, Europa compresa, il *diritto di **non** discriminazione*[61] che protegge da discriminazioni razziali[62], che prevede la libera circolazione di *beni, persone, servizi e capitali*[63] e che prevederebbe anche la non discriminazione **fiscale**[64], purtroppo ampiamente depotenziato dalla Corte di Giustizia della Comunità Europea.

Quindi perché non chiedere anche un **diritto di non discriminazione del traffico di Rete**? In effetti esiste un movimento tecnico-politico che chiede a gran voce la cosiddetta **Net Neutrality** che vedremo in sezione "*Net Neutrality*" - 2.4.2.

[61] *http://treccani.it/enciclopedia/discriminazione*

[62] E ci mancherebbe altro!

[63] Anche se, purtroppo, ultimamente si vedono parecchie resistenze da parte dei singoli stati che cercano di limitare questa facoltà dei cittadini europei.

[64] Articolo 90 e seguenti del Trattato CE.

TECHBOX: DNS (*Domain Name System*) [0.2.1]

In Internet i nodi vengono identificati tramite indirizzi IP (vedere box 0.1.1) numerici. Dato che per un essere umano è difficile ricordare tali indirizzi e dar loro una semantica, fin dagli albori della Rete è stato subito implementato un meccanismo di nomenclatura (*naming*) simbolico.
L'implementazione attuale del sistema di gestione dei nomi simbolici si chiama DNS (*Domain Name System*) e consta in un *registro* dei nomi sparso su molti server (a loro volta nodi della Rete) che vengono interrogati ricorsivamente. la Rete viene suddivisa in zone/domini, all'interno di ogni zona esiste un DNS server che gestisce l'informazione sui nomi simbolici della zona. Le zone sono organizzate in forma gerarchica e il nome completo di un nodo rispecchia la sua collocazione logica, ad esempio il nome *www.di.unimi.it* identifica simbolicamente il nodo 'www' che risiede nella zona/dominio 'di' dentro la zona 'unimi' nella zona 'it'. Il dominio 'it' prende il nome di *TLD* 🕮, dominio geografico associato all'Italia. Esistono *TLD* 🕮 geografici come 'fr' (Francia), 'es' (Spagna), 'uk' (Regno Unito) e 'eu' (Europa). Esistono anche *TLD* 🕮 non geografici come 'gov' (enti governativi), 'edu' (enti universitari e formazione) e 'xxx' (porno).
Nella navigazione web, l'esempio più comune di esperienza diretta con l'uso dei nomi simbolici, la traduzione da simbolico a numerico viene fatta dal software di sistema del PC che viene usato: il browser legge l'URL digitato sulla *barra dell'indirizzo*, ne estrae la parte relativa al nome del server da contattare e attiva la cosiddetta *risoluzione* del nome simbolico, solo successivamente aprirà una connessione per chiedere la pagina web effettiva. La risoluzione è un processo iterativo, il PC contatta il

DNS server di zona che a sua volta contatta i DNS server di zone *superiori* fino ad arrivare a quelli del *TLD* 🕮. Quest'ultimo conosce i DNS server delle zone *sottostanti* e quindi la ricerca può *scendere* fino al DNS server della zona *finale*.
Per tornare all'esempio del nome *www.di.unimi.it*: l'informazione su *chi sia* 'www' la conosce solo il DNS server della zona 'di' quindi da fuori bisognerà chiedere a 'it' chi sia il DNS di 'unimi' a cui chiedere chi sia il DNS server di 'di' a cui, finalmente, chiedere l'indirizzo IP di 'www'. Naturalmente questo processo complicato viene spesso reso più veloce tramite meccanismi di *caching* delle informazioni.
La corrispondenza tra indirizzi IP e nomi simbolici non è sempre *1 a 1*, esistono anche i casi:

- **molti nomi simbolici → 1 indirizzo IP**: cioè tanti *alias* per lo stesso nodo della Rete, l'associazione viene usata per ricordare la funzione[a] di un certo nodo della Rete quando quel nodo ha più funzioni, esempio classico gli alias 'mail', 'smtp', 'pop', 'imap' legati ai vari servizi legati alla posta elettronica;
- **1 nome simbolico → molti indirizzi IP**: qui la richiesta di risoluzione di un nome fornisce più di un indirizzo IP, la semantica di questa *multirisoluzione* è da intendersi come "i due indirizzi sono equivalenti" (forniscono lo stesso servizio/contenuto) e si può utilizzare indifferentemente l'uno o l'altro.

Alcuni esempi di *multirisoluzione* (ottenuti con 'dig', strumento per interrogare il sistema DNS):

- google.it → 172.217.21.67
- google.it → 216.58.205.131
- nasa.gov → 52.0.14.116
- nasa.gov → 23.22.39.120

[a] *Name follows function.*

0.2.1 L'universo distorto

Abbiamo citato qualche esempio *locale* di effetto relativistico, ma purtroppo esistono situazioni ben più gravi e di portata *mondiale*, ecco una lista **abbreviata** [65]:

- In Cina il *Great Firewall of China*[66], meno visibile di quello in muratura, ma molto più efficace, filtra tutto ciò che entra/esce dallo stato e controlla praticamente ogni bit che viene scambiato all'interno del paese, è noto da parecchi anni [McG02] e rende quel paese *democratico* di fatto un universo a sé stante: Google e Facebook non sono raggiungibili ed è molto difficile usare una *VPN* 🕮. Infatti nel corso degli anni la *tecno-politica*[67] si è evoluta moltissimo. Ai primordi il *Great Firewall of China* si limitava a bloccare il traffico ritenuto *pericoloso* per il regime, mentre oggi è molto più subdolo [Fri17]: ogni fonte di (contro)informazione come blog indipendenti, siti esteri non graditi e ogni tipo di contenuto che potrebbe svegliare coscienze viene semplicemente *allontanato* (proprio nel senso relativistico del termine) rendendone l'accesso estremamente lento, al limite (anzi, poco sopra) della pazienza degli utenti che, dopo un po' di attesa, *mollano il colpo* preferendo siti molto più veloci e *responsive* come il sito ufficiale di partito, il motore di ricerca ufficiale (*ça va sans dire* controllato dal partito) cinese o siti di *e-commerce* con cui

[65] Estratti, ove non ulteriormente specificato, dai seguenti:
- [sit16; BN16; Can14; Yet14; Pen14; Gri15; Laf11; Kul14]
- *http://mairiedemontsoult.com/countries-where-Internet-is-forbidden-or-limited*
- *http://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_by_country*
- *http://freepress.net/our-response/expert-analysis/explainers/net-neutrality-violations-brief-history*

[66] *http://en.wikipedia.org/wiki/Great_Firewall*

[67] In questo caso termine usato per indicare l'alleanza fra politica (che decide cosa è lecito) e tecnologia (che implementa/forza/obbliga le decisioni).

soddisfare il proprio desiderio di acquisto dell'ultimo modello di scarpa tecnica.

- In Iran milioni di siti sono oscurati e in alcuni casi vengono creati (dal governo) dei finti siti (e motori di ricerca) sostitutivi.
- In Azerbaijan ogni comunicazione è sotto il controllo statale, vengono oscurati tutti i media esteri e disturbati (*jammed*) i satelliti.
- In Etiopia l'unico *ISP* 🕮 di Stato controlla in toto la rete interna e viene bloccata ogni comunicazione ritenuta *pericolosa*.
- In Eritrea la situazione è analoga a quella etiope.
- In India i blocchi selettivi sono all'ordine del giorno[68]
- In Corea del Nord solo i politici di livello elevato hanno accesso a Internet, ai cittadini (limitatamente a scuole e istituzioni) viene propinata una versione ridotta, filtratissima e *rimaneggiata più volte*[69] per adattarla alla storia *ufficiale* del paese. Alcuni tentano di captare qualche segnale *WiFi* dalla vicina Cina (incappando in altrettanta censura!) rischiando l'arresto dato che è reato sia possedere smartphone che connettersi all'Internet *normale*.
- In Turchia la Rete è stata ripetutamente bloccata, uno dei più recenti eventi è l'oscuramento di Twitter.

Un quadro della situazione viene riportato in figura 4[70], elaborata da J. Ogden a partire da vari documenti di *Reporters Without Borders*[71], di *OpenNet Initiative*[72],

[68] Si veda l'ottimo blog di Carola Frediani (*http://guerredirete.substack.com/p/guerre-di-rete-newsletter-disinformazione-ffe*) che cita il sito indiano dedicato al monitoraggio cronologico dei blocchi: *http://Internetshutdowns.in*

[69] Forse a qualcuno questo procedimento ricorderà il famoso *Ministero della Verità* [Orw45] di orwelliana memoria.

[70] La cui versione precedente e meno aggiornata aveva però un bellissimo *filename* evocativo: *http://commons.wikimedia.org/wiki/File:Internet_blackholes.svg*, a proposito di mondo della Relatività!

[71] *http://rsf.org*

[72] *http://opennet.net*

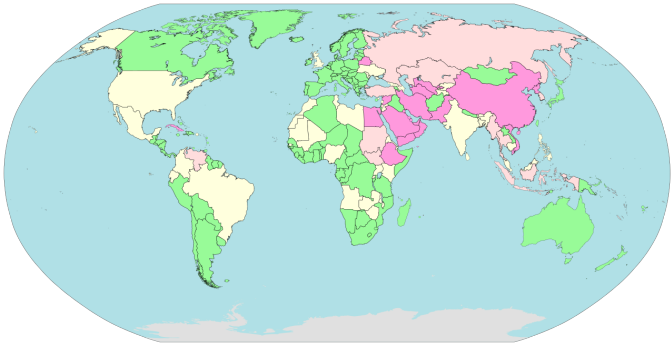


Figura 4: Mappa della censura online nel mondo (Wikipedia)

di *Freedom on the Net*[73] e infine dai *Country Reports on Human Rights Practices* (U.S. Department of State)[74].

Legenda:

- lilla: Pervasive (Cina, Cuba)
- rosa: Substantial (Russia)
- giallo: Selective (USA)
- verde: Little or none (Italia)
- grigio: Unclassified / No data

Un altro report interessante, limitato al filtraggio dell'accesso alle *VPN* 🕮, aggiornato a giugno 2019, si trova su: *http://privacyaustralia.net/vpn-banned-list*.

Si sappia che è facilissimo controllare il traffico entrante/uscente da una nazione: le connessioni interstatali si riducono a pochissimi *grossi cavi*[75] gestiti da *super-ISP* che sottostanno (e ottemperano senza fiatare, si veda sezione "*DataGate*" - 0.4) alle legislazioni nazionali e alle legittime[76] richieste di accesso e controllo dei rispettivi governi.

[73] *http://freedomhouse.org/report-types/freedom-net*

[74] *http://state.gov/reports-bureau-of-democracy-human-rights-and-labor/country-reports-on-human-rights-practices*

[75] Nel caso delle connessioni sottomarine intercontinentali, ad esempio, parliamo di numeri da *dita di una mano*, cfr. figura 5.

[76] Anche se spesso ingiuste.

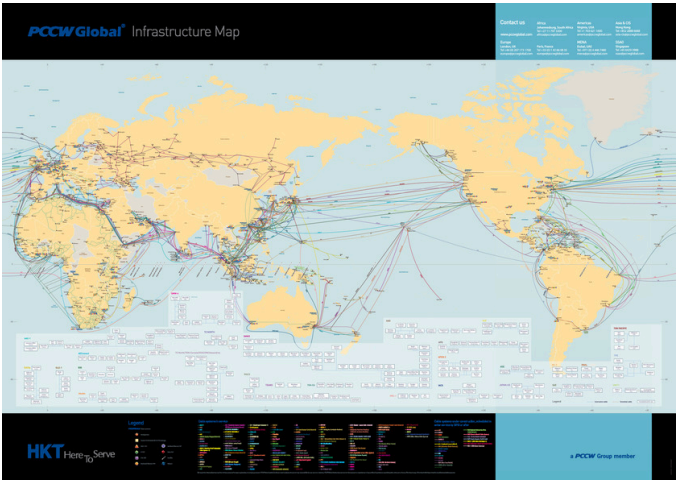
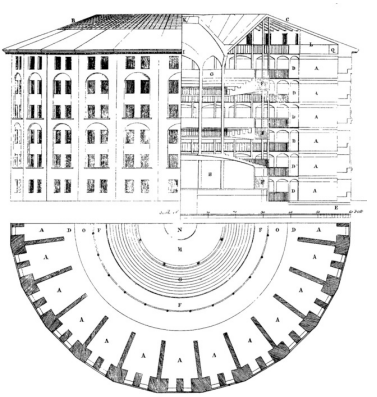


Figura 5: Mappa interconnessioni mondiale (PCCW global)

Nota bene

I concetti appena illustrati si basano sulla manipolazione dei percorsi e del contenuto dei pacchetti **durante** il tragitto che fanno in rete. Nulla abbiamo ancora detto sul potere che ha un *produttore di contenuti* di presentare informazioni diverse a richiedenti diversi: si tratta di una estensione del concetto di rete relativistica applicato ai servizi più che al traffico di rete stesso. Riprenderemo la trattazione nel capitolo "*Livello 1 [services]*" - 1.

0.3 Il Principio di Locard digitale



Il Panopticon del XVIII secolo di Jeremy Bentham

Prima di articolare questo principio dobbiamo farci una domanda preliminare: **quando muore un *bit* 🕮?**

0.3.1 Vita di un bit

Il lettore ci permetta di partire un po' da lontano nel dare una risposta: prima di trattare il contesto digitale vediamo cosa succede alle informazioni nel mondo fisico. Il termine *informazione* è generico ai più, riferiamoci per il momento ad una incarnazione ovvia: un testo scritto su supporto *cartaceo*[77]. Le parole scritte su un supporto *vivono* fino a quando vive il supporto che le… supporta. Esistono supporti molto duraturi, ad esempio:

- **pietra** - parecchi secoli - ad esempio la Stele di Rosetta ha più di duemila anni, pur non essendo il

[77] Nel corso della storia sono stati usati materiali molto diversi a cui affidare uno scritto ai posteri, dalla pietra alla pelle animale, dalla cera al papiro e al metallo… fino ad arrivare alla carta a base cellulosa che oggi conosciamo.

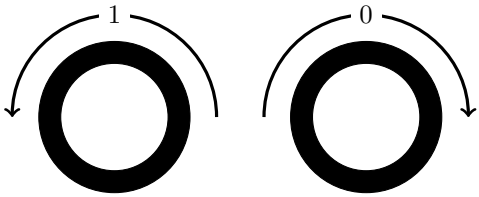


Figura 6: Memorizzazione dei bit negli anelli di ferrite. Le frecce indicano la direzione del campo magnetico.

più antico esempio è comunque in ottimo stato di conservazione

- **pelli/cartapecora** - alcuni secoli - ad esempio la pergamena di Ein Gedi (la più antica ad oggi nota) ha anch'essa poco più di duemila anni, ma è estremamente fragile
- **cera** - qualche giorno - le tavolette di cera venivano usate per appunti temporanei dato che era facile (scaldandole) lisciarle cancellando ciò che si era scritto
- **metallo** - potenzialmente secoli - in funzione del metallo è possibile ottenere supporti molto duraturi, l'esempio che ci viene alla mente sono le targhe messaggio affisse sulle sonde Pioneer (alluminio dorato) e i dischi incisi inseriti nelle Voyager (rame dorato), supporti previsti per resistere alle sollecitazioni di viaggi nello spazio anche di migliaia di anni
- **carta comune** - qualche secolo - il più antico scritto su carta noto oggi ha circa mille anni, ma come supporto è molto fragile sia agli elementi (è igroscopica e prende fuoco facilmente) sia nei confronti degli animali (insetti, ratti) che la utilizzano come cibo o riparo (tritandola e facendo nidi)

Fatta questa mini panoramica dei supporti analogici possiamo, per rispondere alla domanda iniziale, analizzare la situazione digitale iniziando col capire dove viene scritto un bit.

La più piccola unità di informazione, il bit, potreb-

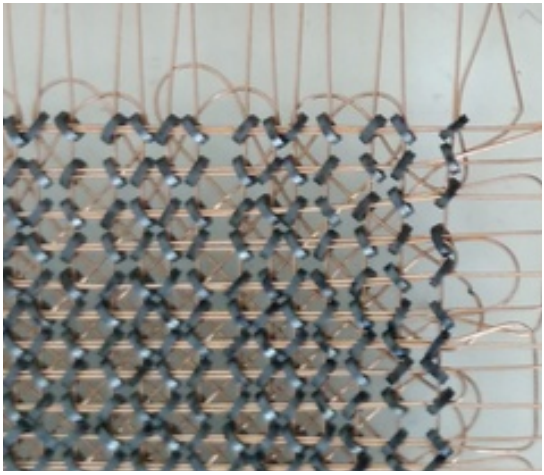


Figura 7: Banco di memoria ad anelli di ferrite

be anche essere scritto su carta[78], ma normalmente viene *scritto* su supporti magnetici sotto forma di magnetizzazione polarizzata di una zona del supporto stesso. Facciamo l'esempio di un supporto ora non più in uso, ma utile alla comprensione per il lettore non tecnico: un anello di ferrite (materiale ferroso magnetizzabile). In figura 6 vengono rappresentati due anelli di ferrite, *anticamente*[79] ogni bit era memorizzato su un piccolo anello di ferrite in cui passavano dei cavi (per la magnetizzazione e per la lettura della stessa), facendo passare corrente nei fili si poteva magnetizzare l'anello e il senso della magnetizzazione dipendeva dalla polarità della corrente con cui si effettuava la *scrittura*. Cucendo tanti anelli di ferrite con cavi elettrici invece che cotone venivano costruiti i primi banchi di memoria per i computer: nella foto 7 un particolare del banco di memoria così "tessuto".

[78]Esempio: *1001* questo numero, che in binario rappresenta il numero 9, è scritto sulla pagina che state leggendo.

[79]In informatica il termine *antico* si riferisce a poche decine di anni orsono, nel caso delle memorie a ferrite ci stiamo riferendo agli anni '50 del novecento.

Ai fini della nostra trattazione possiamo abbandonare la storia dei computer per ragionare sulla *caducità* di un supporto magnetico. Un bit memorizzato su un anello di ferrite risulta leggibile se la magnetizzazione è sufficientemente *forte* da influenzare una corrente che passa in un filo infilato nell'anello stesso: la cosiddetta *operazione di lettura*. Attenzione che la corrente di lettura **distrugge** il bit leggendolo! Cioè siamo davanti ad un caso di supporto leggibile una sola volta! Nelle memorie a ferrite i circuiti di supporto erano quindi costretti a **riscrivere** il dato una volta letto, per non perdere informazione. Un meccanismo simile si trova anche nelle attuali memorie RAM (*Random Access Memory*), non più basate sul magnetismo ma sulla conservazione della carica elettrica. Inoltre magnetizzazione e capacità di conservazione della carica elettrica dei materiali sono sensibili a vari fattori esterni come campi elettromagnetici e temperatura ambientale[80] che possono cancellare le informazioni sui supporti di memorizzazione.

La situazione nei supporti di memorizzazione odierni è molto meno problematica, nel senso che l'informazione sul supporto[81] non necessariamente va riscritta ogni volta che viene letta e la sensibilità alle sollecitazioni (magnetiche, termiche, elettriche) esterne è tutto sommato relativamente bassa.

Ma anche per il supporto odierno più robusto si deve tener conto della sua *caducità*: uno dei parametri che viene misurato e dichiarato dai costruttori è il cosiddetto MTBF (*Mean Time Between Failures*)[82].

L'MTBF è una misura indiretta della durata dell'infor-

[80] Esiste il cosiddetto *punto di Curie*: temperatura oltre la quale un materiale ferromagnetico perde la sua magnetizzazione. Il punto di Curie ci preoccupa poco perché per i materiali (ferrosi) usati in questo campo si tratta di temperature di alcune centinaia di gradi (6-700C°), se si porta un computer a una temperatura simile i problemi sono altri.

[81] Oggi si usano supporti magnetici, ottici ed elettronici (circuiti che immagazzinano informazione sotto forma di piccole cariche elettriche).

[82] O il suo successore AFR (*Annualized Failure Rate*).

mazione in esso contenuta[83], indica che se si lascia passare troppo tempo si rischia[84] di perdere dati.

Quindi un bit vive per (circa) un MTBF?

No, molto di più.

Infatti nell'equazione entra in gioco, ad esempio, una tecnologia chiamata RAID (*Redundant Array of Inexpensive Disks*) (vedere box 0.3.1) che di fatto rende, se correttamente gestita, **immortale** un insieme di dati. Se il *contenitore* che usiamo è un RAID (o simili) e tale contenitore viene *manutenuto* (cambiando i dischi proattivamente) le informazioni in esso contenute saranno disponibili **indefinitamente**.

[83]Non è verissimo, ma è sufficiente per il discorso. Il parametro misura la probabilità di fallimento del device nella sua interezza. Ad esempio, nel caso di un disco fisso magnetico si può avere un fallimento dell'hardware che controlla la lettura/scrittura senza per questo avere perdita di dati. Infatti il disco magnetico interno può essere ancora integro, ma il recupero dei dati diventa molto costoso dato che laboratori specializzati devono smontare (in camera a zero polveri) il disco vero e proprio e rimontarlo in un altro device. L'ordine di grandezza dei costi di recupero è di parecchie centinaia di euro per device.

[84]MTBF è infatti una misura probabilistica.

TECHBOX: RAID, persistenza dei dati [0.3.1]

Le tecnologie di oggi permettono l'immagazzinamento di grandi quantità di dati per tempi virtualmente infiniti. Solo l'utente di computer più sprovveduto perde i propri dati quando un disco fisso muore. Intendiamoci, ogni *storage device* (periferica di immagazzinamento dati) prima o poi smette di funzionare, fa parte della normale usura degli oggetti. Tutto sta nel prevedere[a] la decadenza degli oggetti e difendersi con la **ridondanza**. Sia che i dati siano memorizzati su supporto magnetico, ottico, flash o *SSD* 🕮, oggi è facilissimo mettere in atto tecniche di *mirroring* (copia del dato in tempo reale) che proteggono dal fallimento di una periferica. Ad esempio, la tecnica più nota è il cosiddetto RAID (*Redundant Array of Inexpensive Disks*): vengono raggruppati (collegati allo stesso computer) più dischi e il software di gestione li tratta come un disco unico, scrivendo gli stessi dati su più dischi contemporaneamente. In caso di rottura di un disco il sistema continua a funzionare normalmente (perché i dati sono presenti sui dischi funzionanti) segnalando che "c'è un disco da cambiare", l'operatore può a questo punto cambiare il disco[b] e il sistema di gestione del RAID aggiornerà il nuovo disco con i dati dei/l vecchi(o). In questo contesto, cambiando prontamente i dischi che si rompono, l'unico modo di *perdere* un file è cancellandolo esplicitamente.

Qui sopra una batteria di dischi RAID, gli incavi che si vedono sono per estrarli facilmente, a mani nude, in caso di sostituzione.
Esistono analoghe tecnologie di ridondanza dei dati che però si applicano a gruppi di computer in rete (veloce) fra loro. Il meccanismo è analogo a quello del RAID: ogni computer immagazzina un insieme di dati ridondato (i.e., in copie multiple) rispetto agli altri, se un computer si guasta è sufficiente sostituirlo e il software di gestione ricostruirà il dato globale usando i dati degli altri nodi mentre il nodo nuovo viene *riempito* per tornare al livello di ridondanza originale.

[a] Nel senso di *si vis pacem para bellum*.

[b] Nei sistemi più recenti e avanzati l'operazione viene completata senza nemmeno spegnere il computer, il cosiddetto *hot swapping*.

0.3.2 Edmond Locard

Edmond Locard (1877-1966) è stato un criminologo francese pioniere di quella scienza forense [Loc25] alla base delle indagini della Polizia Scientifica.

Da "*About forensics*"[85]: Edmond Locard è noto per la formulazione del Principio di Scambio che prese il suo nome, relativo al trasferimento di tracce tra (s)oggetti, afferma che "ogni contatto lascia una traccia". Quando due (s)oggetti entrano in contatto l'uno con l'altro, ognuno prenderà qualcosa dall'altro (s)oggetto o vi lascerà qualcosa.

Edmond Locard morì nel 1966, ma il suo Principio di Scambio è stato molto influente nella scienza forense, ed è frequentemente citato tuttora:

> *Ovunque passi, qualunque cosa tocchi, qualunque cosa lasci, anche inconsciamente, fungerà da silenzioso testimone contro di lui. Non solo le sue impronte digitali o dei suoi passi, ma i suoi capelli, le fibre dei suoi vestiti, il vetro che rompe, il segno dello strumento che lascia, la vernice che graffia, il sangue o il seme che deposita o raccoglie. Tutto questo e molto altro, rendono muta testimonianza contro di lui. Queste prove non perdonano. Non si tratta di un testimone confuso dall'eccitazione del momento. Non è assente perché lo sono i testimoni umani. È una* ***prova concreta***[86]*. L'evidenza fisica non può essere sbagliata, non può contraddirsi. Solo l'incapacità umana di trovarlo, studiarlo e capirlo, può ridurne il valore. [Kir53]*

Un soggetto (ai tempi di Locard ci si riferiva ad un criminale) che attraversa un ambiente ne assorbe una piccola parte e abbandona qualcosa di sé. Esaminando **con**

[85] *http://aboutforensics.co.uk/edmond-locard*

[86] Grassetto nostro, vedremo a breve il motivo, nel mondo digitale è... complicato.

cura l'ambiente[87] è possibile trovare le tracce del criminale. Esaminando un soggetto è possibile trovargli addosso tracce degli ambienti che ha frequentato[88]. Il *con cura* è d'obbligo dato che il materiale scambiato è spesso esiguo e fragile, si pensi a peli, capelli, cellule epiteliali, impronte digitali, saliva ecc.; bisogna quindi stare molto attenti a:

- trovare tali tracce
- non distruggerle durante raccolta e conservazione

Nel mondo digitale la situazione è ben diversa. Si può trasporre il Principio di Locard nel mondo digitale definendo il seguente:

Principio di Locard *digitale* della Rete

Un'informazione immessa nella Rete:

- lascia sempre tracce
- tutt'altro che esigue
- indistruttibili

Ricordiamo il funzionamento di Internet spiegato in sezione "*Internet*" - 0.1 **e aggiungiamo ora il fatto che ogni singolo router tiene traccia del traffico** che instrada sotto forma di *log* 🕮. Questi *log* possono essere molto dettagliati[89], normalmente indicano orario (al millisecondo), IP mittente, IP destinatario e altre informazioni al contorno. Spazio di archiviazione permettendo[90] si può

[87] I lettori appassionati di *crime* conoscono perfettamente il termine *walk the grid* citato in tanti libri scritti da Jeffrey Deaver con protagonista Lincoln Rhyme.

[88] E qui la mente va a Sherlock Holmes (precedente e forse ispiratore di Locard) che *indovinava* il quartiere di residenza di una persona esaminandogli le (tracce di terra sulle) scarpe.

[89] Qui un micro esempio, una riga del log di un firewall (qualche campo è stato omesso per privacy): [7066.794707] [UFW BLOCK] IN=wlp1s0 OUT= MAC=<omesso> SRC=92.119.160.145 DST=<omesso> LEN=40 TOS=0x04 PREC=0x00 TTL=241 ID=32147 PROTO=TCP SPT=40103 DPT=51023 WINDOW=1024 RES=0x00 SYN URGP=0

[90] E c'è chi può permetterselo, si veda la sezione "*DataGate*" - 0.4.

registrare persino il **contenuto** di ogni pacchetto transitato[91] e non solo i metadati. Ogni pacchetto che noi immettiamo sulla Rete lascia queste tracce, quindi ogni volta che ognuno di noi naviga in rete anche solo consultando siti web sta lasciando una traccia, ben chiara e **indelebile** (perché di solito viene registrata con le già citate tecniche di tipo RAID).

Ed ecco che il principio di scambio di Locard diventa un **meccanismo più affidabile nel contesto digitale che in quello fisico**.

A prima vista questa affidabilità potrebbe apparire perfetta nella lotta contro il crimine, ma c'è un pesantissimo retro della medaglia legato all'interpretazione del dato (semantica) e alla sua autenticità.

Semantica di una sequenza di bit

Un'*informazione digitale* viene rappresentata e immagazzinata attraverso una sequenza di bit memorizzata su un supporto. Il termine che dovremmo usare è in realtà quello di *dato*, anche se ancora non siamo scesi abbastanza in basso nei livelli di astrazione. Un *dato*[92] è poco più di una sequenza di simboli cui è attribuibile un significato se viene specificato anche il **formato**. Una sequenza di simboli non *porterà informazione* fino a che non le verrà associato un formato e un **interprete**. Al numero '21' possiamo associare ben poco fino a che non aggiungiamo qualcosa, ad esempio un simbolo '°' (metadato) che all'essere umano mediamente istruito (l'interprete che immaginiamo per quella sequenza) fa pensare ad una temperatura. In informatica l'interprete di un simbolo è una generica **Macchina di Turing** (si veda box 0.3.2) che *elaborando* il simbolo stesso e comportandosi di conseguenza gli attribuisce una semantica, vale a dire un significato: il simbolo diventa dato, informazione, messaggio.

[91] Si ricordi che molti protocolli prevedono l'invio di pacchetti *in chiaro*, non crittografati.

[92] *http://treccani.it/vocabolario/dato*

La semantica[93] **di un messaggio è data solo da chi lo legge.** Vale anche per le lingue *umane*[94], a maggior ragione per una generica sequenza di bit.

Ci interessa rimarcare questo concetto perché se le tracce digitali non sono altro che sequenze di bit (in un log ad esempio) utili a *trovare criminali*, cioè le vogliamo usare come *evidence* (prove), dobbiamo porci il problema della loro inequivocabilità: proprietà che **non** hanno!

Per i log esistono formati standard e ormai assodati, ma nessuno obbliga ad aderirvi. Per altri tipi di dato la situazione potrebbe essere anche peggio, potremmo avere sottomano dati parziali[95] o che non seguono alcun formato noto.

Facciamo un esempio pratico, la sequenza di simboli "Y2lhbwo=" ai più non richiama alcun significato particolare, al massimo può sembrare una password *robusta*[96], magari generata da qualche programma di gestione password[97] secondo uno schema prefissato[98]; purtroppo dobbiamo deludere il lettore, la *stringa* 🕮 di simboli è semplicemente la parola "ciao" codificata in *base64*[99].

Quindi, per concludere: **trovare una traccia digitale non implica poterle attribuire un significato univoco**.

[93] Significato.

[94] Si veda il film *Windtalkers* del 2002, che racconta la storia dei nativi americani usati come cripto-codificatori umani durante la Seconda Guerra: l'idioma *indiano* era completamente incomprensibile a chi non fosse un *pellerossa*.

[95] Recuperati da un disco parzialmente rovinato o catturati da traffico in rete di cui però non si aveva visibilità completa.

[96] I.e., difficile da indovinare per tentativi.

[97] Ad esempio `http://keepassxc.org`.

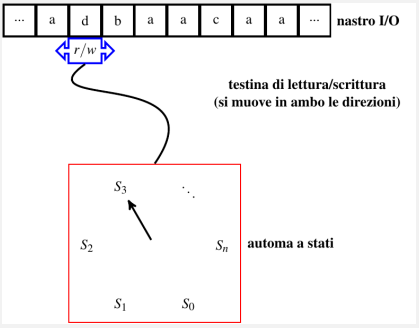
[98] Ad es. almeno una maiuscola, almeno un numero, almeno un simbolo non alfanumerico, ecc.

[99] `http://wikipedia.org/wiki/Base64`

TECHBOX: La Macchina di Turing [0.3.2]

La MdT (Macchina di Turing) [HMU06], un esempio è rappresentato in figura, è un artificio matematico inventato da Alan Mathison Turing negli anni '30 del Novecento. La MdT serve a ragionare formalmente sui linguaggi (non solo quelli di programmazione dei computer) e sugli interpreti potendo stabilire regole di composizione, teoremi di equivalenza e altre interessanti proprietà come la calcolabilità/computabilità degli algoritmi.
Una MdT è una macchina ideale composta da:

- uno o più *nastri di lavoro* su cui possono essere scritti simboli da un alfabeto arbitrario
- (per ogni nastro) una testina di lettura/scrittura dei simboli
- una *macchina a stati* che reagisce ai simboli che le vengono presentati



In tale configurazione una MdT esegue in continuazione il seguente *loop*:

- legge il simbolo sotto al cursore (*fetch*)
- *interpreta* il simbolo secondo la macchina a stati caricata (*execute*), l'interpretazione del simbolo può comportare:
  - un cambio di stato interno
  - una scrittura sul nastro

– uno spostamento del cursore (aggiornamento *program counter*)

I simboli presenti sul nastro determinano il comportamento della MdT.

La stessa sequenza di simboli scatena comportamenti diversi se letta da MdT diverse.

Una architettura semplice che si può immaginare per un computer è una più o meno elaborata MdT in cui la macchina a stati è la CPU, il nastro è la memoria, l'alfabeto dei simboli sul nastro è rappresentato da numeri binari (di dimensione arbitraria, es. 8/16/32 bit) e i movimenti sul nastro sono di lunghezza arbitraria compatibilmente con la lunghezza finita del nastro, ovvero la dimensione della memoria. In particolare, sia la cosiddetta architettura di Von Neumann [Gol80] (un personal computer odierno) che la Harvard (ad esempio l'odierna *board* Arduino molto nota nel mondo *Maker*) prevedono la possibilità di rappresentare la definizione della macchina a stati sotto forma di numeri binari scritti su un nastro in modo che all'*accensione* la MdT possa *caricare* (*boot*) dal nastro di lavoro (eventualmente su un *nastro interno*) la definizione del proprio comportamento e poi implementare tale comportamento. Per cambiare comportamento (programma) bisogna sospendere il *loop*, riscrivere la parte di nastro contenente il programma e riavviare la MdT. È anche immaginabile il caso in cui il programma possa modificare se stesso (l'esempio canonico è il linguaggio LISP [Ste90], ma il principio di funzionamento non cambia.

Impronte sui bit?

Nell'esaminare un documento cartaceo (mondo analogico-fisico) posso tentare di stabilire se è stato manomesso: cerco tracce di cancellazioni e riscritture, cerco impronte digitali (o altre particelle lasciate sul foglio, cfr. sempre Locard!) per capire chi lo ha maneggiato. Posso anche cercare di capire se è un documento originale verificando la calligrafia (se è stato scritto a mano) e confrontandola con esemplari di provenienza nota. Posso valutarne l'età mediante datazione (carbonio e altri procedimenti).

E su una sequenza di bit?

Posso capire se un bit è stato manomesso?

O chi l'ha *scritto*?

O quando?

I tecnici ci perdonino l'esplicitazione di domande tanto puerili, ma è importante rimarcare il concetto che **un bit non ha storia, non ha calligrafia, non gli posso trovare addosso particelle di materiale, non ha età**. Un bit è come un atomo, è il simbolo più piccolo immaginabile e non può portare alcuna informazione ulteriore rispetto al suo stato: 1 o 0.

Lo scaltro lettore potrebbe obbiettare che di un file si hanno alcune informazioni tipo la data di creazione, l'autore, ecc. Già, peccato che queste informazioni, che prendono il nome tecnico di **metadati**, siano a loro volta sequenze di bit di cui non possiamo sapere autore, data di creazione, ecc.

L'**informazione digitale è cioè facilissimamente *forgiabile***, termine tecnico informatico che usa la metafora della forgia metallurgica per indicare un dato creabile alla bisogna e secondo la forma desiderata. È veramente banale creare una traccia digitale che rappresenti un *log* valido indistinguibile da uno effettivamente generato da un comportamento in rete di una persona.

Perché dichiariamo questa ossessione per la forgiabilità delle tracce digitali? Perché ci[100] spaventano?

[100]Noi autori, ma speriamo vivamente di trasmettere questa paura

Perché le tracce digitali sono utilizzate *anche* come *prove* digitali in sede investigativa e processuale. E se non ci si può fidare della veridicità di una prova crolla tutto l'impianto accusatorio. Viceversa, se ci si fida ciecamente della prova digitale e questa è stata forgiata *ad hoc* per puntare il dito contro un capro espiatorio…

Un esempio: nelle indagini per *scambio di materiale multimediale illecito* si cerca di capire quali utenti stanno generando il traffico di rete incriminato. Per farlo vengono chiesti i *log* dei router ai vari provider di connettività. A meno di procedure particolari[101] l'integrità e la veridicità del *log* che viene consegnato dall'*ISP* 🕮 agli investigatori **non** sono garantite da nessuno, vale solo la *parola* del provider. Anche senza pensare ad un *forging* vero e proprio sarebbe molto facile per il provider **escludere** dai log consegnati tutti i dati relativi al traffico di amici e conoscenti, *proteggendoli* dall'indagine in corso.

Davvero è *ottimo*?

Siete ancora convinti che poter raccogliere dati **non verificabili e non interpretabili** ma indistruttibili sia *ottimo*? Non sarebbe doveroso invece limitare la raccolta, la conservazione e l'utilizzabilità (investigativa e processuale) di queste *informazioni*?

Noi (autori) lo vorremmo, i governi vogliono esattamente l'opposto. Molti governi, nel desiderio di controllare i propri cittadini e con la scusa della lotta al terrorismo[102] col passare degli anni hanno cercato (e continueranno), spesso riuscendoci, di allungare a dismisura i tempi di conservazione dei dati raccolti in massa: la famigerata ***data retention***.

al lettore.

[101] Log certificati e datati, depositati presso terzi (di cui ci si deve fidare) o distribuiti con tecniche simil-*blockchain* 🕮. Nel caso delle *blockchain* ci si affida al consenso di un gran numero di *terzi* che devono orchestrarsi (ed è difficile se il numero è elevato) per forgiare un dato.

[102] L'*11/09/2001* è stata la data *pivotale*: quando il terrorismo ha in effetti vinto la guerra.

Leggi sulla conservazione dei dati sono in vigore in moltissimi paesi, vediamo qualche esempio tratto da "*Parliamo di Russia, ma la vera anomalia sul "data retention" è l'Italia*" [Bar18]. La direttiva **Europea** del 2006 fissa la conservazione da minimo sei mesi fino ad un massimo di 24 (derogabile dagli stati membri). Dopo il termine massimo il titolare dei dati deve assicurarsi che questi vengano effettivamente cancellati. Non ottemperare all'obbligo di cancellazione è rischioso dato che un'eventuale fuga/furto di dati vedrebbe il titolare responsabile di violazione della privacy. La **Francia** ha fissato la conservazione a 12 mesi. In **Germania** la durata è molto minore: 10 settimane i dati del traffico telefonico e navigazione in rete, i dati sulla geo-localizzazione dei device mobili solo 4 settimane. In **Belgio** dai 6 ai 9 mesi. In **Spagna** 12 mesi che possono essere ridotti a 6 mesi o estesi a 2 anni, a seconda dei casi. Per motivi di sicurezza, in **Russia** da luglio 2018 vengono registrate tutte le comunicazioni telefoniche e verranno conservate per sei mesi.

In **Italia**, record mondiale, nel 2017 l'obbligo venne prolungato fino a **settantadue** mesi[103]!

Fuori dall'Europa citiamo l'Australia, dove la durata della conservazione dei dati di traffico telefonico e traffico Internet è di 2 anni. Tratteremo gli **USA** nella sezione "*DataGate*" - 0.4.

Nota bene

Come detto a proposito della Rete relativistica, questi meccanismi si basano sul tracciamento **durante** il tragitto in rete. Quasi nulla abbiamo ancora detto sul potere che ha un *produttore di contenuti* di memorizzare/analizzare informazioni generate dall'interazione degli utenti coi servizi (siti web): si tratta di una estensione del Principio di Locard *digitale* applicato ai servizi più che al traffico di rete stesso. La raccolta

[103] *http://www.privacyitalia.eu/vigore-la-legge-impone-la-data-retention-6-anni/5463*

dati sul traffico di rete è infatti costosa e complicata. Molto più semplice affidarsi a tecniche di raccolta dati diretta, basate sulle applicazioni/programmi (installati di buon grado da utenti ignari o *embedded* negli elettrodomestici acquistati) e sui servizi web che possono analizzare direttamente il comportamento degli utenti. Riprenderemo il tema nel capitolo "*Livello 1 [services]*" - 1.

0.3.3 Profilazione

`Data is the new oil`

Clive Humby

Abbiamo evidenziato un uso delle tracce digitali del tutto simile al contesto fisico: *ex post*, indagare su un fatto avvenuto. Ma esistono modi molto più fantasiosi (e pericolosi a volte) di utilizzare quei dati:

- commerciale
- sorveglianza anticrimine e antiterrorismo
- previsione comportamenti criminali

Con **commerciale** si intende l'estrazione di informazione utile a (pre)vedere spazi di mercato e commercializzazione. Osservando le abitudini di navigazione degli utenti, i movimenti (fisici, geo-localizzati) che fanno le persone o il traffico verso certi siti piuttosto che altri è possibile ipotizzare quale tipo di prodotto/servizio/sito avrà successo in una determinata zona geografica. Oppure è possibile avere indicazioni sull'andamento (anche borsistico) di una particolare azienda in funzione del traffico web che genera.

Con **sorveglianza anticrimine** si intende il monitoraggio delle azioni in Rete[104] di gruppi circoscritti di persone *attenzionate* dalle forze dell'ordine. Questi soggetti potrebbero non aver ancora commesso reati, ma sono stati associati ad azioni criminali e vengono sorvegliati per

[104]O dei movimenti fisici, tracciando i telefoni, anche quelli non *smart* tramite i collegamenti alle torri/celle.

conoscere **con anticipo** eventuali mosse a danno della collettività.

Con **previsione comportamenti criminali** si intende il monitoraggio delle azioni in Rete[105] di **grandi gruppi di persone** *tout court*, senza bisogno di un *attenzionamento* da parte delle forze dell'ordine. Questi soggetti, potenzialmente tutti i cittadini (vedremo qualche numero in sezione "*DataGate*" - 0.4), vengono sorvegliati per **prevedere** chi tra loro potrebbe diventare un pericolo per la collettività.

Il primo uso ci può dar fastidio ideologico perché ci fa capire che c'è qualcuno che ne sa commercialmente più di noi e che quindi avrà sempre un vantaggio competitivo.

Il secondo uso comincia a farci alzare un sopracciglio perché ci potremmo domandare se le procedure di *attenzionamento* sono state effettuate garantendo i diritti civili degli *attenzionati*.

Il terzo uso prende il nome di *pre-crime* [Wei11; Van17; Das13; MP09], cioè la pretesa di prevedere[106] le intenzioni e i comportamenti delle persone sulla base di alcune loro azioni, pensieri espressi sui social, movimenti sul territorio, e così via.

Quest'ultimo uso dovrebbe scandalizzarvi come scandalizza noi, stiamo parlando di monitoraggio pervasivo di massa alla ricerca di comportamenti che potrebbero (condizionale d'obbligo) portare a detrimento[107] della società.

Ecco il motivo del riferimento al Panopticon riportato nell'epigrafe della sezione "*Il Principio di Locard digitale*" - 0.3, viviamo purtroppo in un ambiente sotto costante osservazione e analisi dei nostri comportamenti: ma quanti se ne rendono conto?

[105] O dei movimenti… (idem).

[106] Non stiamo parlando del film "*Minority Report*", ma di una tecnologia reale e utilizzata estensivamente **ora**.

[107] La definizione di *detrimento* è molto relativa: un omosessuale in una nazione fondamentalista islamica è considerato un detrimento da punire, a volte con la morte.

Profilazione fatta in casa

Per dare un piccolo esempio di quali informazioni si possono estrarre dai dati di traffico/accesso alla Rete consigliamo di leggere l'appendice "*Profilazione WiFi*" - A in cui mostriamo un lavoro di analisi effettuata *in casa* con pochissimo sforzo.

0.4 DataGate

> No person shall be subject, except in cases of impeachment, to more than one punishment or trial for the same offense; *nor shall be compelled to be a witness against himself*; nor be deprived of life, liberty, or property, *without due process of law*; nor be obliged to relinquish his property, [*his data,*] where it may be necessary for public use, without just compensation…
>
> *Quinto emendamento, Costituzione degli Stati Uniti, corsivi e una "piccola" aggiunta tra '[]' degli autori*

Ringraziamenti

Questa sezione è ispirata a "*Behind DataGate*" [ML15] di Chiara Marchetti e Matteo Longeri, redatto nell'ambito del Corso di Cittadinanza Digitale e Tecnocivismo: li ringraziamo per il prezioso contributo.

Sopra abbiamo illustrato i principi generali di funzionamento della Rete, le possibilità di manipolarla attraverso

la relatività fino a vere e proprie operazioni di censura di interi *pezzi* di Internet, trasformandola in un *universo distorto*. Esaminiamo ora cosa è stato possibile fare grazie al fatto che in Internet la *profilazione* è *connaturata*: lo scandalo DataGate.

DataGate è il nome con il quale alcune testate giornalistiche [108] definiscono la serie di notizie - pubblicate a partire dal mese di giugno del 2013 - che rivelano i dettagli relativi ad alcune operazioni di **sorveglianza di massa** messe in atto dalla agenzia statunitense NSA (*National Security Agency*) con la collaborazione attiva di agenzie di *intelligence* che fanno parte della rete *Five Eyes* 📖.

Secondo la testimonianza resa di fronte al Congresso degli Stati Uniti da Keith B. Alexander, direttore della NSA (*National Security Agency*), lo scopo principale della raccolta massiva di dati è quello di immagazzinare tutte le registrazioni telefoniche (e le comunicazioni in Internet, n.d.r.) in un posto che ne consenta la ricerca e l'analisi in ogni momento[109].

Nel corso della narrazione citeremo link a vari articoli sull'argomento, ma le fonti principali di approfondimento sono i due libri "*Permanent Record*" [Sno19], "*No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*" [Gre14] e il famoso documentario del 2014 "*Citizenfour*" di Laura Poitras[110].

0.4.1 Gli attori

Edward snowden

L'identità di "*gola profonda*" dello *scandalo Watergate di questo millennio* questa volta non è rimasta sconosciuta per decenni.

[108] Si veda ad esempio *http://wired.it/topic/datagate* oppure *http://internazionale.it/notizie/2015/06/25/datagate-snowden-spionaggio*

[109] *http://bigstory.ap.org/article/senators-limit-nsa-snooping-us-phone-records*

[110] Nel 2016 è stato tratto anche un film, "*Snowden*" che è la versione romanzata della storia del DataGate.

Nel 2006 Snowden cominciò a collaborare con la CIA (*Central Intelligence Agency*) come esperto informatico[111] e a girare il mondo grazie alla sua competenza. Nel 2007, durante il suo periodo sotto copertura in Svizzera, era considerato il maggior esperto in cyber-sicurezza locale tanto da essere selezionato dalla CIA per supportare il presidente statunitense durante il summit NATO nel 2008 in Romania.

Dal 2008, stando alle sue dichiarazioni, cominciò a comprendere che il ruolo del governo USA nel mondo non era quello nel quale gli avevano insegnato a credere e cominciò a coltivare il progetto di divulgare pubblicamente ciò che conosceva.

Nel 2009 Snowden iniziò una nuova collaborazione con la NSA alle dipendenze di Dell Corporation che gestiva i sistemi informatici di diverse agenzie governative: in questo nuovo ruolo riuscì ad ottenere credenziali avanzate che gli consentirono di accedere ad informazioni con un livello di segretezza ancora maggiore. Fu negli uffici CIA del Maryland che Snowden verificò direttamente quanto fosse esteso e profondo il programma di sorveglianza globale messo in atto da NSA, mediante un accumulo tale di dati da determinare l'eliminazione di qualsiasi forma di riservatezza a livello mondiale.

Quando nel 2012 Snowden venne assegnato all'ufficio Dell nelle Hawaii come responsabile tecnologico della NSA riuscì ad ottenere le credenziali per accedere agli ultimi documenti prima di rendere pubblica a tutto il mondo l'intera vicenda.

Nel Gennaio del 2013 Snowden riuscì a mettersi in contatto con Glenn Greenwald - all'epoca editorialista per The Guardian - grazie all'intermediazione di Laura Poitras, documentarista statunitense[112]. Sia Greenwald che Poitras si erano distinti per il proprio lavoro in merito ad alcune inchieste su programmi di sorveglianza globale, questo

[111] *http://wired.com/2014/08/edward-snowden*

[112] *http://nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html*

convinse Snowden a contattarli per rivelare loro ciò che sapeva, supportato dai molti documenti che egli aveva nel frattempo trafugato.

Nel Maggio 2013 Snowden prese alcuni giorni di ferie raccontando ai suoi supervisori che stava tornando in continente per un trattamento dell'epilessia[113], ma lasciò le Hawaii per Hong Kong dove arrivò il 20 Maggio.

I primi documenti trafugati da Snowden furono pubblicati il 5 Giugno 2013 da Greenwald sul Guardian, nell'articolo "*La NSA sta raccogliendo giornalmente i tabulati telefonici di milioni di clienti Verizon*"[114]

Il 14 Giugno del 2013 i giudici federali degli Stati Uniti accusarono Snowden di furto di proprietà governative e due violazioni del "Espionage Act" - legge sullo spionaggio - del 1917, attraverso la comunicazione non autorizzata di informazioni riguardanti la difesa nazionale e divulgazione intenzionale di comunicazioni riservate di intelligence a una persona non autorizzata.

Il 23 Giugno 2013 Snowden lasciò Hong Kong verso un non meglio precisato paese latino americano su un volo con scalo a Mosca. Al suo arrivo a Mosca le autorità riscontrarono che il suo passaporto statunitense era stato revocato, così fu trattenuto per 39 giorni nella zona di transito dell'aeroporto al termine dei quali gli venne concesso asilo politico temporaneo per un anno, poi prorogato fino al 2022.

Glenn Greenwald

Greenwald iniziò la propria carriera[115] nel 1994 come avvocato, occupandosi principalmente di casi riguardanti problemi di costituzionalità e diritti civili.

[113] *http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance*

[114] *http://theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order*

[115] *http://salon.com/news/opinion/glenn_greenwald/profile/index.html*

Nel 2005 diede il via al proprio blog "*Unclaimed Territory*" dedicato ad articoli di giornalismo investigativo. Si occupava di vicende politiche controverse dell'epoca, tra le quali un programma di sorveglianza della NSA conosciuto come *warrantless-wiretapping*, ovvero la possibilità per NSA di sorvegliare le comunicazioni senza ottenere specifica autorizzazione dalla corte preposta, la *FISA* 📖[116].

Nel 2012 iniziò a scrivere per The Guardian, dove il 5 Giugno 2013 pubblicò il primo articolo sul DataGate[117].

Le rivelazioni continuarono per tutto il 2013 e una **piccola porzione dell'intero archivio**[118] di documenti venne successivamente pubblicata da altri mezzi di comunicazione, tra i principali: The New York Times (USA), la Canadian Broadcasting Corporation, la Australian Broadcasting Corporation, Der Spiegel (Germania), O Globo (Brasile), Le Monde (Francia), L'espresso (Italia), NRC Handelsblad (Olanda), Dagbladet (Norvegia), El País (Spagna) e Sveriges Television (Svezia)[119]. Le serie di articoli che Greenwald contribuì a pubblicare consentirono a The Guardian e a The Washington Post di vincere il premio **Pulitzer** per il servizio pubblico nel 2014[120].

NSA e la coalizione *Five Eyes* 📖

La NSA (*National Security Agency*) è una agenzia di intelligence del Dipartimento della Difesa USA ed è responsabile del monitoraggio, raccolta ed elaborazione di dati e informazioni; specializzata nella disciplina conosciuta co-

[116] *http://glenngreenwald.blogspot.com/2006/02/nsa-legal-arguments.html*

[117] *http://theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order*

[118] Non è nota l'esatta dimensione dell'archivio ma le stime fornite da diversi funzionari dei governi coinvolti parlano di 1,7 milioni di files dall'intelligence USA, 58000 dal Regno Unto e 15000 dall'Australia.

[119] Per un elenco completo e aggiornato si veda l'apposita pagina curata dalla EFF *http://eff.org/nsa-spying/nsadocs*

[120] *http://theguardian.com/media/2014/apr/14/guardian-washington-post-pulitzer-nsa-revelations*

me *SIGINT* 🕮, ad essa è anche affidata la protezione delle reti informatiche e di comunicazione degli USA.

La NSA si avvale di diverse tattiche per svolgere la propria missione, alcune di queste[121] includono furto, intercettazioni telefoniche ed effrazione in obiettivi ad elevato valore strategico quali *uffici presidenziali, istituzionali o ambasciate.* Pratiche contrarie alle disposizioni della Convenzione di Vienna sulle Relazioni Diplomatiche del 1961.

Five Eyes 🕮 è una alleanza di agenzie di spionaggio anglofone che comprende Australia, Canada, Nuova Zelanda e Regno Unito, che aderiscono al trattato *UKUSA* 🕮 del 1946 per la cooperazione in operazioni di *SIGINT* 🕮.

I documenti trafugati da Snowden nel 2013 hanno rivelato che le agenzie del *Five Eyes* 🕮 hanno spiato i cittadini degli altri paesi aderenti e condiviso tra loro le informazioni raccolte al fine di eludere le normative nazionali in merito alla sorveglianza dei propri cittadini[122] Per esempio, Der Spiegel ha rivelato come il servizio di intelligence straniera (in tedesco "*Bundesnachrichtendienst*") trasferisca massicce quantità di dati intercettati alla NSA[123]. Mentre la televisione svedese ha rivelato che l'agenzia governativa nazionale di intelligence FRA forniva alla NSA i dati dalla propria connessione cablata, in accordo con un trattato segreto siglato nel 1954 per la cooperazione bilaterale alla sorveglianza[124]. Altre agenzie di intelligence e sicurezza che sarebbero coinvolte nelle pratiche di sorve-

[121] *http://www.telegraph.co.uk/news/worldnews/northamerica/10150905/NSA-surveillance-US-bugged-EU-offices.html*

[122] Si vedano: *http://theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data*, *http://theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens*, *http://theguardian.com/politics/2013/jun/10/nsa-offers-intelligence-british-counterparts-blunkett* e *http://uk.reuters.com/article/2013/06/21/uk-usa-security-britain-idUKBRE95K10620130621.*

[123] *http://spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html*

[124] *http://svt.se/ug/nsafra4*

glianza globale includono ad esempio quelle di: Australia (ASD)[125], Canada (CSEC)[126], Danimarca (PET)[127], Francia (DGSE)[128], Norvegia (NIS)[129], Spagna (CNI)[130], Singapore (SID)[131] e Israele (ISNU)[132], che riceve dalla NSA dati grezzi e non filtrati su cittadini USA.

Ci preme inoltre aggiungere una considerazione da "Cittadinanza Digitale e Tecnocivismo": NSA - con l'aiuto di altre agenzie alleate - intercetta e conserva le comunicazioni elettroniche di oltre un miliardo di persone in tutto il mondo e traccia i movimenti di centinaia di milioni di persone utilizzando i dati raccolti per fornire al governo USA vantaggi strategici, militari, **economici e politici**.

Nella propria Mission and Values[133] la NSA scrive chiaramente che intende usare le proprie risorse "in order to gain a decision advantage for the Nation and our allies under all circumstances" (al fine di ottenere un vantaggio decisionale per la nazione e i suoi alleati in ogni circostanza). Che le "circostanze" per le quali ottenere un vantaggio includano anche quelle economiche è noto da tempo agli addetti ai lavori. Il rapporto del 1999 Sviluppo della Tecnologia della Sorveglianza e Rischi di Abuso dell'Informazione Economica[134] pubblicato a seguito di una indagine del Parlamento Europeo durata anni, analizza i rischi di

[125] *http://abc.net.au/news/2013-11-08/australian-nsa-involvement-explained/5079786*

[126] *http://cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886*

[127] *https://www.vpnmentor.com/blog/understanding-five-eyes-concept*

[128] *http://lemonde.fr/technologies/article/2013/11/29/la-france-precieux-partenaire-de-l-espionnage-de-la-nsa_3522653_651865.html*

[129] *http://wsj.com/news/articles/SB10001424052702303985504579207500439*

[130] *http://theguardian.com/world/2013/oct/30/spain-colluded-nsa-spying-citizens-spanish-el-mundo-us*

[131] *http://smh.com.au/technology/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html*

[132] *http://theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents*

[133] *http://www.nsa.gov/about/mission-values*

[134] *http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf*

abuso dello spionaggio per ottenere vantaggi economici. Edward Snowden, in una intervista del 2014, afferma che la NSA è direttamente coinvolta in attività di spionaggio industriale[135] e alcune inchieste giornalistiche rivelano seri indizi che, oltre che nei confronti di paesi geo-politicamente distanti[136], questa pratica fosse rivolta anche a paesi alleati[137] degli USA. Su questo aspetto vi invitiamo anche a leggere la conclusione della sezione "*Tutto ciò è già accaduto*" - 0.4.3.

Le aziende coinvolte

La collaborazione tra la NSA e le maggiori aziende statunitensi nel settore delle telecomunicazioni - se ne contano fino a cento - risale agli anni '70 dello scorso secolo e si è sviluppata all'interno del programma *Special Source Operations* (SSO) [GP13].

Nei mesi seguenti allo scoppio del DataGate l'analisi dei documenti rivelò inequivocabilmente che le aziende che controllano la maggior parte del mercato mondiale sono coinvolte assieme ad NSA nell'implementazione dei vari programmi di sorveglianza, che - ciascuno a proprio modo - necessitavano l'accesso di NSA ai server o alle infrastrutture gestite da quelle aziende.

Le aziende coinvolte in uno dei programmi di maggiore estensione, PRISM (vedi nel seguito), sono: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube e Apple.

Al programma TEMPORA (idem) invece hanno collaborato le aziende che assieme gestiscono una notevole porzione dei cavi trans-oceanici in fibra ottica che costituiscono il *backbone* (spina dorsale) di Internet: BT, Verizon

[135] *http://www.bbc.com/news/25907502*

[136] *http://web.archive.org/web/20130911074801/http://www.reuters.com/article/2013/09/09/us-usa-security-snowden-petrobras-idUSBRE98817N20130909*

[137] *http://www.spiegel.de/international/germany/german-intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html*

Business, Vodafone Cable, Global Crossing, Level 3, Viatel e Interoute [BG13; Gar14].

Sebbene inizialmente la maggior parte delle aziende coinvolte abbiano tentato di negare di essere a conoscenza dei programmi di sorveglianza che *Five Eyes* 🕮 stava conducendo **anche** attraverso le loro infrastrutture [GM13; Rus13; Far13], successive rivelazioni hanno confermato che erano perfettamente a conoscenza del loro coinvolgimento attivo in uno o più di quei programmi [Ack14].

Alcune importanti collaborazioni di aziende statunitensi sono confermate **anche** da una sentenza dell'Ottobre 2011 della corte speciale *FISA* 🕮 che è stata de-segretata nel Agosto 2013. Un documento interno NSA evidenzia che le aziende coinvolte nella sentenza hanno dovuto sostenere costi aggiuntivi per l'adeguamento dei propri sistemi e per questo sarebbero state **rimborsate** per importi dell'ordine di alcuni milioni di dollari [Mac13].

L'ultima e a nostro avviso più interessante considerazione in merito alle aziende coinvolte riguarda i cosiddetti **contractors**, ovvero i fornitori privati che lavorano a stretto contatto con i governi per la gestione di parte dei loro servizi, difesa inclusa. Edward Snowden fu in grado di sottrarre i documenti NSA mentre lavorava per l'azienda Booz Allen Hamilton, uno dei maggiori contractor della difesa e dei servizi segreti statunitensi.

Non conosciamo i motivi che hanno spinto le aziende a collaborare con NSA e i *Five Eyes* 🕮: sono state costrette senza possibilità di scelta o hanno avuto convenienza a farlo? In ogni caso è importante ribadire che NSA e *Five Eyes* 🕮 sono in grado di implementare i propri programmi soprattutto grazie alla collaborazione delle aziende che controllano la quasi totalità del mercato occidentale dei cosiddetti *servizi in cloud* e *social networks*, nonché dell'Internet *backbone*. I segreti raccolti in questo modo sono inoltre *custoditi e condivisi* con una serie di soggetti privati **statunitensi**.

0.4.2 Programmi di sorveglianza

Le rivelazioni del DataGate dimostrano l'esistenza di diversi programmi di sorveglianza globale, ciascuno dei quali sfrutta contemporaneamente le *debolezze tecniche* e la forte *asimmetria di potere* derivante dalle circostanze storiche nelle quali è stata progettata e implementata Internet.

In questa sezione abbiamo scelto di descrivere solo le tecniche e i relativi programmi che a nostro giudizio sono più significativi in quanto meglio rivelano la natura **globale** della sorveglianza, tralasciando invece i programmi per intercettazioni mirate e quelli che non hanno coinvolto l'abuso dell'infrastruttura Internet o la compromissione **indiscriminata** di software o hardware.

Intercettazione fibra ottica

NSA e *Five Eyes* 🕮 sono in grado di catturare e registrare una quantità massiva di dati attraverso tecniche di intercettazione dei cavi in fibra ottica o di controllo diretto dei nodi di terminazione dei cavi, parte integrante del *backbone* Internet.

Attraverso la tecnica denominata *boomerang routing* - ovvero la capacità di far transitare il traffico Internet su nodi sorvegliati manipolando le *rotte* di comunicazione (si veda sezione "*Internet*" - 0.1) - le agenzie di spionaggio sono in grado di far transitare i dati negli USA anche se origine e destinazione della trasmissione sono in paesi esteri [OC13]; in questo modo l'intercettazione è soggetta alle leggi statunitensi[138]. Questa tecnica è stata utilizzata nei seguenti programmi:

RAMPART-A[139], accesso ai cavi di connessione in fibra ottica che connettono i principali punti strategici da cui passa la maggior parte del traffico Internet mon-

[138] Notoriamente piuttosto permissive - in questo periodo storico - quando si tratta di intercettare le comunicazioni di cittadini stranieri piuttosto che di cittadini americani.

[139] *http://en.wikipedia.org/wiki/RAMPART-A*

diale (cfr. figura 5), al fine di poter intercettare tutte le comunicazioni che vi transitano[140].

Tempora[141], intercettazione e raccolta in territorio britannico e in oceano dei cavi in fibra ottica per ottenere accesso massivo e indiscriminato ad un enorme quantità di dati personali[142].

FAIRVIEW[143], analogo a Tempora, intercettazione e raccolta di dati telefonici, comunicazioni via Internet e email attraverso l'intercettazione delle terminazioni statunitensi dei cavi transoceanici in fibra ottica e dei nodi di connessione interna[144].

Raccolta dati presso i fornitori di servizi.

NSA e Five-Eyes sono in grado di raccogliere grandi quantità di dati accedendo direttamente ai server dei maggiori fornitori di servizi tra i quali: Microsoft, Yahoo!, Google, Facebook, YouTube, Skype, Apple. I dati raccolti comprendono: email, teleconferenze video e voce, file video, foto, conversazioni voice-over-IP, documenti e dettagli dei profili di social networking. I progetti più *interessanti*:

PRISM[145], raccolta del contenuto delle comunicazioni e dei documenti direttamente dai server dei maggiori fornitori di servizi statunitensi[146].

[140] *http://information.dk/udland/2014/06/nsa-third-party-partners-tap-the-Internet-backbone-in-global-surveillance-program*

[141] *http://en.wikipedia.org/wiki/Tempora*

[142] *http://theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden*

[143] *http://en.wikipedia.org/wiki/Fairview_(surveillance_program)*

[144] *http://nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-Internet-traffic.html*

[145] *http://en.wikipedia.org/wiki/PRISM_(surveillance_program)*

[146] *http://theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google*

MUSCULAR[147], analogo a PRISM, raccolta dei dati intercettando i dati non crittografati in transito tra i data centre distribuiti di Yahoo! e di Google[148].

DISHFIRE[149], raccolta di informazioni provenienti da varie parti del mondo, giornalmente erano registrati: settantaseimila geo-localizzazioni, ottocentomila transazioni finanziarie, 1,6 milioni varchi di frontiera, 5 milioni di avvisi di chiamate perse[150], 200 milioni di messaggi SMS[151].

Indicizzazione e analisi dei dati raccolti

Tutti i dati e **metadati** raccolti dai programmi di sorveglianza globale sono indicizzati in modo tale da poter essere ricercati e analizzati anche a distanza di tempo. Dal 2017 i dati disponibili in questo enorme database sono consultabili anche da sedici agenzie governative statunitensi, oltre che alla NSA e ai propri diretti alleati[152] attraverso:

Xkeyscore[153], sistema di ricerca e recupero dati composto da una serie di interfacce utente per interrogare tutti i dati raccolti attraverso gli altri programmi di sorveglianza.

Boundless Informant[154], sistema di visualizzazione e analisi dei metadati raccolti dai programmi di sorveglianza.

[147] *http://en.wikipedia.org/wiki/MUSCULAR_(surveillance_program)*
[148] *http://web.archive.org/web/20131106231842/http://washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data*
[149] *http://en.wikipedia.org/wiki/Dishfire*
[150] *http://theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep*
[151] *http://bbc.com/news/world-us-canada-25770313*
[152] *http://theintercept.com/2017/01/13/obama-opens-nsas-vast-trove-of-warrantless-data-to-entire-intelligence-community-just-in-time-for-trump*
[153] *http://en.wikipedia.org/wiki/XKeyscore*
[154] *http://en.wikipedia.org/wiki/Boundless_Informant*

Grazie a queste tecniche è possibile effettuare sofisticate analisi in merito alle persone applicando tecniche di *ingegneria sociale* [MSW11].

Compromissione della crittografia

NSA e GCHQ (*Government Communications Headquarters*) - la controparte britannica - hanno adottato una serie di metodi per compromettere sistematicamente la **crittografia**, ciò che loro ritengono essere uno dei *maggiori ostacoli* alla propria capacità di raccogliere e analizzare tutto quello che viene trasmesso su Internet.

Una presentazione di GCHQ del 2010 recita[155]:

> *Vaste quantità di dati Internet crittografati che fino ad ora sono state scartate ora possono essere sfruttate.*

Vogliamo qui notare che, sebbene i programmi e le tecniche utilizzate per compromettere la crittografia siano tuttora di estrema segretezza, una delle specifiche missioni della NSA è: compromettere la crittografia per ottenere vantaggi rispetto agli *avversari*[156]. Prendiamo nota: **avversari** qui noi leggiamo **cittadini**.

Il principali programmi in questo campo sono:

TURMOIL[157], azioni sotto copertura per **controllare gli standard crittografici da parte degli organismi preposti**, compromissione delle chiavi attraverso attacchi *brute force* nei confronti di software che usano algoritmi *appositamente* indeboliti, inserimento di backdoors nel software crittografico[158]. GCHQ ha un programma chiamato Edgehill, analogo a TURMOIL.

[155] *http://theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security*
[156] *http://propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-Internet-encryption#odni-response*
[157] *http://en.wikipedia.org/wiki/Turbulence_(NSA)*
[158] *http://theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security*

BULLRUN[159], serie di misure per ottenere la compromissione della crittografia, incluso l'utilizzo di intrusione remota delle reti per ottenere chiavi crittografiche, **indebolimento** degli standard di **crittografia** e inserimento di **backdoor** negli stessi[160].

0.4.3 Passato e futuro

Il DataGate racconta di fatti relativamente recenti, ma esiste un precedente molto famoso che dimostra come l'ingordigia informativa delle grandi organizzazioni statali (e oggi anche quelle commerciali) genera ingordigia ulteriore.

Tutto ciò è già accaduto

ECHELON è il capostipite dei sistemi di sorveglianza globale; venne rivelato per la prima volta al mondo nel 1971 da una intervista a Winslow Peck [Hor72] - al secolo Perry Fellwock, analista della NSA - e fu oggetto di diverse altre rivelazioni e inchieste giornalistiche fino a quando, nel Marzo 1999, il governo Australiano ammise ufficialmente l'esistenza di ECHELON [CH99; Cam00].

Il programma - creato alla fine degli anni 60 per monitorare le comunicazioni militari e diplomatiche dell'Unione Sovietica e i suoi alleati del *blocco di Varsavia* durante la *guerra fredda* - venne formalmente istituito nel 1971.

Due bollettini interni della NSA del Gennaio 2011 e Luglio 2012, pubblicati come parte del DataGate da The Intercept il 3 Agosto 2015, confermarono per la prima volta che la NSA utilizzò il nome in codice ECHELON e chiarirono che ECHELON era parte di un programma più ampio - nome in codice FROSTING - che venne istituito dalla NSA nel 1966 per raccogliere e analizzare dati dalle comunicazioni satellitari; i due sottoprogrammi FROSTING erano: ECHELON per l'intercettazione delle trasmissioni

[159] *http://en.wikipedia.org/wiki/Bullrun_(decryption_program)*

[160] *http://theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security*

satellitari Intelsat, all'epoca gestita da una organizzazione intergovernativa per fornire servizi agli 81 paesi aderenti, e TRANSIENT per l'intercettazione delle trasmissioni satellitari Intersputnik, fondata dall'Unione Sovietica assieme ad altri otto paesi del blocco di Varsavia [NSA12; NSA11].

La maggior parte dei rapporti su ECHELON si focalizzano sull'intercettazione satellitare, tuttavia testimonianze di fronte al Parlamento Europeo indicano che erano attivi programmi analoghi - da parte della coalizione oggi conosciuta come *Five Eyes* 🕮 - per il monitoraggio delle comunicazioni attraverso i cavi sottomarini, le microonde e altre linee di comunicazione[161].

Questo scenario è confermato anche dal Parlamento dell'Unione Europea che nel Luglio del 2000 istituì una speciale commissione di inchiesta su ECHELON. L'inchiesta si concluse con la redazione - e successiva approvazione il 5 Settembre 2001 da parte del Parlamento - del rapporto 2001/2098 (INI) [Com01].

Sebbene all'epoca non erano noti altri programmi analoghi che solo tredici anni più tardi vennero rivelati dal DataGate, il rapporto stabilisce che ECHELON[162] era in grado di intercettare e ispezionare il contenuto delle conversazioni telefoniche, fax, email e altro traffico dati con estensione globale, attraverso l'intercettazione dei mezzi che veicolano le telecomunicazioni quali: trasmissioni satellitari, rete telefonica (che all'epoca trasportava la maggior parte del traffico Internet) e collegamenti a microonde [Com01].

Emerge quindi chiaramente che, parallelamente all'evoluzione della tecnologia delle telecomunicazioni, alla fine del ventesimo secolo il sistema si era evoluto ben oltre le sue origini militari e diplomatiche trasformandosi in un sistema globale di intercettazione delle comunicazioni private ed economiche - si veda a pagina 13 del rapporto della commissione d'inchiesta [Com01] - ovvero un vero e

[161] *http://cryptome.org/echelon-nh.htm*

[162] Citiamo testualmente dal rapporto:"si può presumere che il sistema o parte di esso sia stato, almeno per qualche tempo, denominato in codice "ECHELON"" (pag. 13).

proprio **sistema di sorveglianza globale e spionaggio industriale**.

Non è chiaro se e quando il programma ECHELON - o meglio FROSTING - sia stato definitivamente abbandonato, tuttavia appare del tutto evidente che sia stato via via **sostituito da nuovi e più sofisticati strumenti** di intercettazione, basti notare che RAMPART venne istituito nel 1992, da quando cioè progressivamente il ruolo dei satelliti è stato via via soppiantato dai *cavi*[163]: si stima che nel 2006 il 99% del traffico mondiale di voce e dati fosse trasportato lungo connessioni in fibra ottica[164].

Alla luce delle rivelazioni del DataGate, appare quindi plausibile concludere che la NSA abbia messo in campo un articolato insieme di programmi, tecniche e risorse economiche per **colmare i limiti del sistema di intercettazione** illustrati nel rapporto del parlamento EU 2001/2098 (INI) [Com01], limiti descritti testualmente così[165]:

> *Considerando che il sistema di sorveglianza si basa in particolare sull'intercettazione globale delle comunicazioni via satellite; che tuttavia nelle aree ad elevata densità di comunicazioni solo un volume estremamente ridotto di queste viene trasmesso tramite satellite; che in tal modo la maggior parte di esse non può essere intercettata dalle stazioni di terra, bensì solo* ***inserendosi nei cavi*** *o captando le trasmissioni via radio, operazioni, queste, che - come hanno dimostrato le ricerche riportate nella relazione - sono possibili solo entro limiti ristretti; che* ***l'impiego di personale per l'analisi*** *finale delle comunicazioni intercettate comporta ulteriori limiti; che di conseguenza gli Stati*

[163] Agli albori di Internet, la rete NSFNET era connessa con cavi telefonici e cavi coassiali

[164] *http://web.archive.org/web/20140714124934/http://news.cnet.com/NSA+eavesdropping+How+it+might+work/2100-1028_3-6035910.html*

[165] Grassetti aggiunti dagli autori.

> *UKUSA* 🕮 *hanno* ***accesso solo ad una parte molto esigua delle comunicazioni via cavo*** *e via radio e sono in grado di analizzare solo una percentuale ancor più ridotta delle comunicazioni; che, per ingenti che siano le risorse disponibili e le capacità di intercettazione delle comunicazioni, il numero elevatissimo delle stesse rende in* ***pratica impossibile un controllo esaustivo*** *e dettagliato di tutte le comunicazioni.*

Dulcis in fundo, giusto per mettere in chiaro **definitivamente** che le attività in questione hanno riguardato *anche* lo spionaggio industriale, riportiamo testualmente quanto scritto nel rapporto sopra citato, che ricordiamo essere datato 11 Luglio **2001**:

> *Sullo spionaggio economico*
>
> *...*
>
> *P. considerando che i servizi informativi degli Stati Uniti non si limitano a far luce su questioni economiche di ordine generale, ma ascoltano nei dettagli anche le comunicazioni fra imprese al momento dell'assegnazione di appalti, giustificandosi con la lotta contro i tentativi di corruzione; che con un'intercettazione dettagliata si rischia che le informazioni non vengano utilizzate per lottare contro la corruzione, ma a fini di spionaggio nei confronti della concorrenza, anche se gli Stati Uniti e il Regno Unito sostengono di non farlo; che il ruolo dell'Advocacy Center del ministero per il Commercio statunitense continua ad essere poco chiaro e che è stato annullato un incontro con lo stesso che avrebbe dovuto chiarirne la funzione,*
>
> *...*
>
> *S. considerando che, nel corso della visita della delegazione della commissione tempo-*

ranea sul sistema d'intercettazione ECHELON negli USA, delle fonti autorizzate hanno confermato la relazione Brown del Congresso degli Stati Uniti, indicando che il 5% delle informazioni raccolte attraverso fonti non pubbliche è utilizzato per scopi economici; che le stesse fonti stimano che tale sistema di controllo delle informazioni potrebbe consentire alle imprese statunitensi di guadagnare fino a 7 miliardi di dollari in termini di contratti,

...

U. considerando che la consapevolezza in materia di rischio e sicurezza nelle piccole e medie imprese è spesso insufficiente e che esse non si rendono conto dei pericoli connessi con lo spionaggio economico e l'intercettazione di comunicazioni,

V. considerando che presso le istituzioni europee (ad eccezione della Banca centrale europea, della Direzione generale per le relazioni estere del Consiglio e della Direzione generale per le relazioni estere della Commissione) la consapevolezza in materia di sicurezza non è molto sviluppata e che occorre pertanto intervenire,

Futuro

Il progresso della tecnologia, finora non controllato da chi la subisce, cioè dai **cittadini**, ha solo affinato le tecniche e potenziato la capacità di osservazione di questi enti, ora sta a noi riprendere il controllo, se vogliamo.

Avremmo potuto aggiungere una sezione "Tutto ciò potrebbe accadere", ma sinceramente non sapevamo immaginarci un contesto peggiore di quello che abbiamo descritto. In passato un autore di fantascienza, Bob Shaw, aveva immaginato una situazione simile a quella in cui viviamo oggi, nell'appendice B riportiamo alcuni frammenti interessanti del libro "*Altri giorni altri occhi*" [Sha73] commentando-

ne i collegamenti con il tema qui trattato, a monito per il futuro.

0.5 Avete rotto Internet

Nei precedenti capitoli abbiamo illustrato come funziona la Rete, partendo dai suoi protocolli di comunicazione e - passando per la comprensione degli aspetti relativistici e delle tecniche di profilazione - siamo arrivati al DataGate, grazie al quale è ormai chiaro **oltre ogni ragionevole dubbio** che le comunicazioni attraverso Internet sono oggetto di una sorveglianza globale senza precedenti nella storia dell'umanità, che in pochi anni comprenderà sempre più ampi spazi della *nostra esistenza fisica* grazie allo sviluppo *perverso* dell'*IoT* 🕮. Per dirla con Bruce Scheiner[166]:

> *Manomettendo Internet ad ogni livello per renderla un vasta piattaforma di sorveglianza la NSA (e non solo, n.d.r.) ha minato i fondamenti della nostra società. Non possiamo più fidarci delle aziende che gestiscono l'infrastruttura, quelle che fabbricano l'hardware e il software o delle aziende che ospitano i nostri dati. Questa non è l'Internet di cui il mondo ha bisogno o quella che i loro inventori hanno immaginato. Dobbiamo riprendercela.*

Come mai è stato possibile *manomettere* Internet nonostante le ingenti risorse impiegate, in termini economici e di competenze tecniche? La ragione sostanziale è che l'attuale implementazione di Internet si basa *sulla reciproca fiducia* - come abbiamo visto ampiamente tradita - che le trasmissioni non vengano intercettate e alterate da terzi.

[166] *http://theguardian.com/commentisfree/2013/sep/05/government-betrayed-Internet-nsa-spying*

0.5.1 Internet è guasta

Comprendere cosa tecnicamente renda Internet tanto vulnerabile è materia oggettivamente complessa, richiede competenze in reti di telecomunicazione e crittografia delle quali in questo volume abbiamo solo potuto fornire cenni. Però siamo convinti che comprendere la *natura del problema* sia **alla portata di ciascuno di noi e quindi un dovere civico**.

L'attuale implementazione di Internet è una stratificazione di protocolli sviluppati a partire dagli anni '70 per rispondere alle esigenze della comunità dell'epoca, che si interconnetteva per scambiarsi informazioni **in chiaro** senza troppe preoccupazioni di verificarne l'autenticità e la riservatezza, basandosi appunto su un principio di *reciproca fiducia*.

Con l'espandersi di Internet e l'adozione da parte di un numero sempre più ampio di utilizzatori le esigenze di comunicazione sono cambiate drasticamente, si sono evolute: comunicazioni istituzionali e personali private, commercio elettronico, sistemi di pagamento online e via discorrendo hanno posto in primo piano l'esigenza di garantire autenticità e riservatezza di tali comunicazioni.

Per rispondere a queste nuove esigenze e allo stesso tempo non interrompere la compatibilità con il resto di Internet, vennero sviluppati ulteriori protocolli *stratificati* su quelli esistenti: purtroppo questi *strati* si sono rivelati soltanto meri *rappezzi* per tentare di correggere la sostanziale insicurezza alla base di Internet.

Potete approfondire in che modo ciascuno strato dell'infrastruttura della Rete è guasto leggendo, appunto, "*Internet è guasta*"[167] del progetto *secushare.org* di cui qui di seguito riassumiamo i punti fondamentali.

Il peccato originale di Internet

Internet è guasta perché **non garantisce l'autenticità** delle trasmissioni tra due nodi: una o più entità terze con

[167] *http://secushare.org/broken-Internet*

sufficiente potere di controllo su alcuni nodi importanti nella Rete sono in grado di intercettare, manipolare e ritrasmettere i pacchetti che transitano su Internet, in alcuni casi aggirando anche i protocolli di crittografia.

Lo studio della storia relativa alle prime fasi di sviluppo di quella che successivamente divenne Internet lascia trasparire che con tutta probabilità il protocollo IP - alla base dell'intera Internet - avrebbe potuto includere la crittografia end-to-end, ma ciò fu impedito per una serie di ragioni storiche[168]. Secondo la serie di articoli "*Net of Insecurity del Washington Post*"[169], gli inventori avrebbero proposto di introdurre una forma di crittografia end-to-end direttamente nel protocollo, garantendo almeno l'*autenticità della trasmissione*, se non del contenuto; Ma l'uso della crittografia fu impedito perché all'epoca - e per diversi anni a venire - questa era considerata uno *strumento militare* dal governo USA (ed altri) e per questo sottoposta a un rigido controllo di esportazione al di fuori del territorio nazionale. Solo nel 1996 le norme furono sostanzialmente modificate per consentire il libero utilizzo in ambito commerciale della crittografia, pur mantenendo alcune restrizioni per casi particolari[170].

Quando venne concepita, quindi, non solo Internet era *in chiaro* 🕮 di *default* 🕮 ma anche **insicura di default**, poiché - come ampiamente illustrato nella sezione "*Internet*" - 0.1) - la provenienza o il contenuto di qualsiasi pacchetto IP possono essere modificati. Questa è la causa fondamentale per la quale è stato necessario *tentare di aggiustare* i protocolli utilizzati su Internet, introducendone di nuovi per garantire l'autenticità delle trasmissioni e la riservatezza attraverso la crittografia con protocolli quali

[168] Ciò ha costretto le generazioni di sviluppatori successive a rappezzare i vari protocolli di rete aggiungendo a posteriori strati eterogenei di crittografia che *non risolvono* il problema dell'autenticità delle comunicazioni.

[169] *http://washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1*

[170] *http://en.wikipedia.org/wiki/Export_of_cryptography_from_the_United_States*

HTTPS per il web o SMTPS e IMAPS per le email anche se, purtroppo quei protocolli non risolvono del tutto i problemi per i quali sono stati concepiti.

Manipolazione del routing

Il *routing* dell'intera Internet - il cui concetto abbiamo illustrato in sezione "*Mini-esegesi di TCP/IP*" - 0.1.1 - si basa sul protocollo BGP (*Border Gateway Protocol*) che, oltre a soffrire di alcuni problemi tecnici di stabilità e scalabilità, consente a qualsiasi Internet Service Provider o altro ente con sufficiente potere di dirottare interi intervalli di indirizzi IP, consentendo l'intercettazione e la manipolazione del traffico prima che questo sia consegnato all'indirizzo di destinazione.

Questa *caratteristica* di BGP, che si basa sulla reciproca fiducia tra tutti i gestori di router, è considerata il vero e proprio tallone di Achille di Internet fin dal 1998, quando un gruppo di hacker testimoniò di fronte al congresso USA su come sarebbero stati in grado di interrompere l'intera Internet in 30 minuti sfruttando le debolezze di progettazione del protocollo [Zet08].

La lista di *incidenti* storici pubblicamente noti[171] è abbastanza esplicativa in merito al fatto che questo tipo di dirottamenti sono piuttosto frequenti in Internet, tuttavia recenti ricerche [Goo13] suggeriscono che la tecnica del dirottamento del traffico potrebbe essere usata sistematicamente senza che venga scoperta, come ampiamente documentato anche grazie alle rivelazioni del DataGate.

Niente anonimato

Anonimato è una parola con diversi significati, cerchiamo di metterci d'accordo subito su cosa intendiamo noi con anonimato: la protezione delle informazioni in merito a *chi sta comunicando con chi*, per difendere il principio costituzionale di libertà di associazione in un mondo sempre

[171] *http://en.wikipedia.org/wiki/BGP_hijacking#Public_incidents*

più oggetto di sorveglianza globale[172] (i.e., da parte di terzi non esplicitamente coinvolti nella comunicazione).

Su Internet l'anonimato è sostanzialmente impossibile poiché DNS, SMTP, XMPP e la stragrande maggioranza dei protocolli usati su Internet trasmettono i *metadati* in chiaro anche se il contenuto della comunicazione è crittografato: chi è in grado di controllare il traffico su Internet è in grado di conoscere in ogni istante chi sta parlando con chi[173]. In altre parole, terze parti sono in grado di identificare tutti i partecipanti di una comunicazione attraverso Internet.

La mancanza di riservatezza dei metadati relativi alle nostre comunicazioni a prima vista potrebbe non sembrare un problema perché *si tende a pensare che i metadati non dicano poi molto* in merito alle nostre vite. Infatti, molti governi e aziende vorrebbero farci credere che la raccolta sistematica dei metadati non violi la privacy di nessuno. Tuttavia un interessante studio [Zwa14], condotto tramite un volontario che ha accettato di trasmettere i propri metadati per una settimana a un gruppo di ricercatori, ha dimostrato che tali informazioni **rivelano moltissimo** su di noi: i nostri studi, il nostro impiego e le ricerche di lavoro, il nome dei nostri cari, i video che guardiamo sul web, cosa ci piace fare nel nostro tempo libero, le organizzazioni delle quali facciamo parte, comprese ovviamente le nostre *attività politiche*.

Carente riservatezza

La maggior parte dei protocolli di comunicazione sicura, vale a dire crittografata, utilizzati su Internet basano la

[172] Va da sé che ciascuno dei partecipanti alla comunicazione può chiedere di conoscere l'identità (o lo pseudonimo) dei partecipanti ed eventualmente rifiutarsi di proseguire nella comunicazione, si pensi ad esempio ad una transazione commerciale che implica la conoscenza dell'identità del cliente

[173] Ogni comunicazione su Internet avviene tra due nodi con un indirizzo IP noto, l'Internet Provider conosce l'intestatario di ogni indirizzo IP e queste informazioni sono a disposizione di diversi altri enti con sufficiente potere o autorità.

propria sicurezza su certificati crittografici a chiave pubblica emessi secondo lo standard X.509[174] e gestiti per mezzo di una *PKI* 🕮 globale.

Le debolezze architetturali e di implementazione delle *PKI* 🕮, oltre ai problemi legati alla fiducia nei confronti delle aziende e organizzazioni che emettono i certificati, sono da tempo ben note agli esperti di sicurezza e documentate in letteratura [ES00] e *di per sé* basterebbero ad illustrare perché l'intero sistema di crittografia pubblica andrebbe messo da parte. A chiarire definitivamente lo stato di affidabilità di tali sistemi, esistono studi che dimostrano quanto questi siano facilmente aggirabili da chi ha sufficiente potere per operare una *manipolazione del routing* (vedi sopra) e riuscire così ad ottenere falsi certificati [Bir+17], riuscendo successivamente ad inserirsi nelle comunicazioni crittografate con la tecnica di attacco *MITM* 🕮 e intercettare il traffico (che viene così trasformato *in chiaro*) senza che le parti ne siano consapevoli.

0.5.2 Provare a difendersi

Con Internet che ha raggiunto questo livello di *compromissione* e senza avere già a disposizione la *prossima Internet* (si veda nel seguito) la cosa migliore da fare è quella di **limitare i danni** o, per dirla citando "*Il capitalismo della sorveglianza*" [Zub19b]: "trasformare l'atto di nascondersi in una scienza e un'arte" e, aggiungiamo noi, *contemporaneamente* **esercitare la nostra cittadinanza facendo pressione politica affinché i problemi vengano riconosciuti e risolti**.

In primis abbiamo quindi necessità di strumenti di *misura e di aggiramento/protezione/difesa*.

Appurato che ciascuno di noi ha una visione della Rete differente a causa della sua relatività, il primo passo per difendersi è misurarne il livello di *distorsione*, per decidere eventualmente quali strumenti utilizzare per correggere il difetto *oculistico* di cui soffriamo.

[174] *http://www.itu.int/rec/T-REC-X.509*

Citiamo un paio di progetti interessanti che si dedicano alla **misurazione** del grado di relatività della Rete:

- OONI Probe[175] è un software che permette di misurare diversi indicatori in merito allo stato della propria connessione:
  - blocco di siti web;
  - blocco di applicazioni di instant messaging: WhatsApp, Facebook Messenger e Telegram;
  - blocco di strumenti di aggiramento della censura, tipo Tor;
  - presenza di sistemi nella propria rete che potrebbero essere responsabili di censura;
  - velocità e performance della propria rete.

  OONI Probe consente anche di condividere (*crowdsourcing* 🕮), su base volontaria, i dati raccolti al fine di misurare il livello globale di censura, questi dati sono visibili[176] sul sito del progetto.
- Un altro strumento di misura della relatività della Rete è l'applicazione Wehe[177]. Questa applicazione permette di verificare se il proprio ISP applichi limitazioni alla banda di specifiche applicazioni per favorirne altre, violando quindi il principio della *net neutrality* (che vedremo in sezione "*Net Neutrality*" - 2.4.2). É stato per esempio osservato come alcuni operatori telefonici che nelle proprie offerte includono streaming illimitato su alcune piattaforme, diminuiscano[178] anche di 3/4 la velocità di trasmissione da/verso piattaforme concorrenti. Anche con Wehe possiamo contribuire a creare un dataset[179] pubblico relativo al comportamento dei fornitori di servizi di telecomunicazioni in merito alla net neutrality.

Invece per **proteggere il contenuto** delle proprie comunicazioni è necessario crittografare i dati in modo tale che solo i destinatari del messaggio siano in grado di

[175] *http://ooni.org*
[176] *http://explorer.ooni.org*
[177] *http://dd.meddle.mobi*
[178] Effettuano il cosiddetto *tune down*.
[179] *http://wehe-data.ccs.neu.edu*

leggerne il contenuto, mentre chi non è autorizzato vedrà solo indecifrabili sequenze di bit. La tecnica migliore è quella genericamente chiamata della *crittografia a chiave pubblica*[180] o *asimmetrica*: un ipotetico soggetto "Mario" genera una coppia (matematicamente relazionata) di chiavi, la parte pubblica può essere divulgata al mondo mentre quella privata va custodita gelosamente. Un altro ipotetico soggetto "Laura" che voglia inviare dei dati privati a Mario li dovrà codificare usando la chiave pubblica di Mario. A questo punto solo Mario sarà in grado di decifrare quei dati perché è la chiave privata che può decodificare i dati crittografati con la chiave pubblica, cioè la chiave pubblica si usa per codificare mentre quella privata per decodificare.

Il dato ancora oggi più scambiato[181] è la email, ma la percentuale di utenti che usa sistemi crittografici in questo contesto è molto molto bassa[182] (praticamente lo 0% di chi usa la posta elettronica attraverso un'interfaccia web). Per crittografare **le email** consigliamo di seguire la comoda guida "*Autodifesa email*"[183] curata dalla Free Software Foundation. Discorso analogo per i sistemi di *instant messaging* (WhatsApp, Telegram ecc.), molti di questi offrono un certo livello di crittografia, ma non tutti lo fanno di *default* e non sempre lasciano all'utente il controllo delle chiavi, vanificando totalmente lo scopo primario della crittografia stessa[184].

Ulteriore tecnica di difesa[185] è quella delle cosiddette *reti overlay*, meccanismi per costruire una *rete sopra un'altra rete*: il traffico dati *importante* viene *incapsulato* (codificato, spesso anche crittografato) dentro ad un traffico dati *di trasporto* per essere portato a destinazione. Per dirla con una metafora: un'organizzazione di "fattorini" che

[180] *http://www.britannica.com/topic/public-key-cryptography*

[181] Non in termini di volume di dati: da questo punto di vista è lo *streaming video* a farla da padrone.

[182] *http://www.virtru.com/blog/arent-people-using-email-encryption*

[183] *http://emailselfdefense.fsf.org/it*

[184] Se la chiave privata è nota al provider del servizio esso potrà leggere **tutte** le conversazioni senza alcuna difficoltà.

[185] Non alla portata di tutti, purtroppo.

utilizzasse i mezzi pubblici di una città sarebbe una rete di distribuzione (pacchi, buste ecc.) *overlay* sopra una rete di trasporto pubblico, quest'ultima non avrebbe conoscenza di ciò che trasportano i singoli fattorini, cioè **non saprebbe chi sta mandando pacchi a chi**. Una *rete overlay* introduce quella che potremmo chiamare "contro-relatività" controllata dall'utente finale.

Le implementazioni digitali più note sono le cosiddette *VPN* 🕮, come OpenVPN[186] o Wireguard[187] Dopodiché esistono particolari reti *overlay* specificamente progettate per fornire anche protezione dall'identificazione di mittenti e destinatari (e non solo per la protezione dei contenuti) da parte di terzi, parliamo delle cosiddette *reti anonimizzanti*[188].

Il più noto strumento di questo tipo è **Tor**[189], acronimo derivato dal nome originale del progetto, "*The Onion Router*", che evidenzia la sua principale caratteristica di *rete a cipolla*. Lo scopo di Tor è quello di proteggere la riservatezza e la libertà degli utenti consentendo loro di navigare sul web[190] sfruttando una rete *di copertura*[191] composta da migliaia di nodi di instradamento: ad ogni passaggio i pacchetti vengono incapsulati in modo tale da nascondere, crittografandoli, i dati sensibili della comunicazione[192] e garantendo che una volta raggiunta Internet non sia possibile rilevare la reale ubicazione dell'utente o effettuare l'analisi del traffico. La consegna finale dei pacchetti al nodo di destinazione su Internet è effettuata da speciali nodi Tor chiamati *exit node* (cfr. ottima animazione esplicativa[193] sul sito di EFF). Ci teniamo comunque a sottolineare che Tor non può impedire a un servizio online

[186] *http://openvpn.net*
[187] *http://www.wireguard.com*
[188] *Feigenbaum2015*
[189] *http://torproject.org*
[190] Ha altre applicazioni più avanzate come ad esempio gli *hidden services* che però non tratteremo qui.
[191] In gergo tecnico una *overlay network*
[192] Ad esempio il reale IP del mittente *o* del destinatario e altri metadati preziosi.
[193] *http://www.eff.org/pages/tor-and-https*

di verificare che il traffico provenga dalla sotto-rete Tor[194] ed eventualmente decidere di bloccare l'accesso[195]. In altre parole Tor protegge la riservatezza dell'utente ma non nasconde al destinatario *il fatto che stia usando Tor*, pur non rivelandone il vero indirizzo IP. A ciò si aggiunge il fatto che il vostro provider di connettività, l'ISP, può decidere di **bloccare l'accesso alla rete Tor** utilizzando specifiche tecniche di analisi del traffico: in questo caso Tor mette a disposizione uno speciale meccanismo, chiamato Pluggable Transport[196], inglobato nel Tor Browser[197].

Un altro strumento pensato per proteggere l'anonimato in rete e aggirare la censura è **I2P**[198], simile a Tor ma che usa una variante degli algoritmi di instradamento chiamata *Garlic Routing*[199]. I2P è considerato ancora *beta software*, tuttavia è abbastanza maturo da poter essere utilizzato come strumento *non critico*. Normalmente può essere utilizzato come server *proxy* locale[200] da qualsiasi browser[201]. In questa modalità gli utenti possono quindi navigare in modo del tutto analogo a quanto permette di fare Tor. I2P però va oltre, includendo anche *applicazioni dedicate* che funzionano solo comunicando all'interno della rete I2P: un sistema di chat (server IRC locale), diverse applicazioni per file sharing, email, instant messaging, pubblicazione di contenuti[202], file sharing. In questo modo gli utenti possono **proteggere meglio la propria privacy** nei confronti, per esempio, di chi pubblica contenuti o condivide files: nella rete I2P né il mittente né il destinatario han-

[194] *http://check.torproject.org/exit-addresses*

[195] Alcune banche italiane hanno deciso di non accettare login di utenti, **pur legittimi**, se provengono dalla rete Tor.

[196] *http://2019.www.torproject.org/docs/pluggable-transports.html.en*

[197] *http://torproject.org/download*

[198] *http://geti2p.net*

[199] Letteralmente instradamento ad aglio: ironici!

[200] Ovvero un servizio funzionante sul proprio computer, al quale indirizzare le comunicazioni.

[201] Tutti i browser moderni, ma anche altri programmi che sfruttano la rete, consentono di impostare un proxy per la connessione in rete.

[202] Stile blog e forum con piccoli allegati multimediali.

no bisogno di rivelare il proprio indirizzo IP, nemmeno ad eventuali osservatori lungo la catena di instradamento, ma comunicano utilizzando identità crittografiche[203].

Si distingue rispetto ai precedenti il progetto **Freenet**[204]: si tratta di una piattaforma *peer-to-peer* 🕮 per la comunicazione che utilizza un database distribuito e decentralizzato per immagazzinare e consegnare le informazioni. Ogni nodo che partecipa alla rete Freenet contribuisce con spazio disco per il database distribuito e fornendo funzioni di instradamento per gli altri partecipanti. La piattaforma Freenet, quindi, fornisce l'infrastruttura peer-to-peer attraverso la quale le applicazioni specificamente sviluppare possono immagazzinare e trasmettere le informazioni; ad oggi sono disponibili alcune applicazioni Freenet per attività di: microblogging, condivisione file, pubblicazione siti e blog *statici*. É importante sottolineare che Freenet **non funziona da proxy** per il World Wide Web ma può essere utilizzato solo per accedere al contenuto che è stato pubblicato nel database decentralizzato attraverso le proprie applicazioni dedicate. Freenet utilizza un metodo di instradamento peer-to-peer che normalmente prevede che il nodo richiedente (il contenuto) non si connetta direttamente al nodo che lo ha a disposizione ma che la sua richiesta venga instradata attraverso diversi intermediari, nessuno dei quali conosce quale nodo ha effettuato la richiesta o quale nodo ha il contenuto. Il risultato è che complessivamente il trasferimento delle informazioni e dei file è più lento, specialmente per i contenuti consultati più raramente.

[203] Essenzialmente una coppia di chiavi pubbliche.
[204] *http://freenetproject.org*

0.5.3 Riprogettare Internet

> `Un viaggio di mille miglia comincia sempre con il primo passo`
>
> *Lao Tzu*

Considerando quanto illustrato nella sezione "*Internet è guasta*" - 0.5.1, appare ormai evidente che voler riparare Internet introducendo strumenti che **tentano** di risolvere i problemi aggiungendo *strati sani* su un substrato *guasto* equivale a prolungare una sorta di **lenta agonia**. Internet deve essere rifatta da capo, mantenendo *solo* l'infrastruttura fisica e sostanzialmente rimpiazzando *quasi* tutti i protocolli utilizzati per trasmettere informazione.

I progetti illustrati in sezione "*Provare a difendersi*" - 0.5.2 purtroppo si appoggiano a meccanismi che li rendono vulnerabili ad attacchi per comprometterne l'anonimato; nel seguito citiamo alcuni di questi attacchi:

- *sybil attacks*[205]: si compromette il sistema di reputazione dei nodi che si occupano del routing, sostituendoli con nodi sotto il proprio controllo ricavando i metadati delle trasmissioni;
- *traffic shaping* e *traffic analisys*: si sfrutta la possibilità di manipolare la banda di trasmissione e di analizzare sia il traffico entrante che quello uscente dalla rete Tor[206];
- *web fingerprinting*: consente a un osservatore in grado di intercettare il traffico generato da un browser su un canale crittografato - ovvero HTTPS - di determinare le attività svolte sul web [Tao16].

[205] Si veda *http://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack* e *http://arstechnica.com/information-technology/2014/07/active-attack-on-tor-network-tried-to-decloak-users-for-five-months*

[206] *http://arstechnica.com/information-technology/2016/08/building-a-new-tor-that-withstands-next-generation-state-surveillance*

C'è un progetto che invece ha deciso di affrontare le questioni della sicurezza nelle trasmissioni di rete *riscrivendo* i protocolli alla base delle trasmissioni in rete, si tratta di GNUnet.

GNUnet

Il progetto GNUnet[207] non è ancora in grado di sostituire l'attuale Internet, tuttavia sta sviluppando un insieme completo di nuovi protocolli con lo scopo di costruire applicazioni sicure, distribuite e rispettose della riservatezza e dell'anonimato di chi comunica attraverso la Rete.

GNUnet è una rete di tipo *mesh*: ogni nodo si connette direttamente con il maggior numero di altri nodi e collabora per instradare efficientemente i pacchetti, senza che sia necessario conoscere la destinazione finale o il contenuto dei pacchetti stessi e quindi nemmeno i metadati. Questo principio di funzionamento è sostanzialmente differente da quello dell'attuale Internet, dove la necessità di instradamento dei pacchetti a nodi con indirizzi **in chiaro** consente ad un insieme di nodi *autorevoli* di manipolare e ispezionare il traffico.

I *concetti di base* della nuova architettura di rete possono essere così riassunti:

- Internet e i suoi protocolli insicuri vengono usati come *mezzo di trasporto*[208] per connettere un nodo a GNUnet, con l'aggiunta di un criterio per *garantire* che l'indirizzo IP di ciascun nodo non sia falsificato[209].
- Tutte le comunicazioni avvengono attraverso nodi *mutuamente autenticati* con criteri crittografici di tipo *perfect forward secrecy*[210].

[207] *http://gnunet.org*

[208] Considerandolo comunque inaffidabile.

[209] *http://docs.gnunet.org/handbook/gnunet.html#Address-validation-protocol*

[210] Criteri crittografici che garantiscono che le precedenti comunicazioni non siano compromesse nel caso di compromissione di una chiave privata.

- L'identità di un nodo corrisponde alla propria chiave pubblica, **non al proprio indirizzo IP**: essere in grado di falsificare un indirizzo IP è sostanzialmente irrilevante in GNUnet.
- L'*allocazione di risorse* da parte di ciascun nodo viene effettuata sulla base di un meccanismo di misura del contributo che ciascuno di essi fornisce al resto della rete, in questo modo è possibile minimizzare l'impatto di possibili attacchi di saturazione della banda disponibile da parte di potenziali attaccanti[211].
- La *confidenzialità* delle comunicazioni è garantita dal fatto che i messaggi sono crittografati a livello di *connessione*, questo garantisce che solo mittente e destinatario sono in grado di conoscere in contenuto della trasmissione, poiché qualsiasi tecnica di analisi dei pacchetti è impraticabile.
- L'*anonimato delle comunicazioni* è reso possibile dal fatto che le comunicazioni tra due nodi sono *nascoste* nel flusso tra gli utenti, rendendo cioè indistinguibile il traffico generato da quello inoltrato per conto di altri nodi; in questo modo nemmeno attaccanti in grado di controllare un discreto numero di nodi sarebbero in grado di ricavare la vera provenienza dei pacchetti, anche utilizzando tecniche di analisi del traffico.
- Il *sistema dei nomi* dei domini GNS (*GNU Naming System*) non si basa su una gerarchia centralizzata - come il tradizionale DNS - ma su una architettura decentralizzata, in cui la validità dei nomi è garantita dalla firma crittografica di chi gestisce quello *spazio di nomi* (in gergo: una zona).

Attraverso l'applicazione di questi principi, che si basano su una pluriennale ricerca accademica[212], gli sviluppatori GNUnet sperano di poter costruire **solide fondamenta** per quella che sarà la nostra Rete del futuro.

[211] *http://grothoff.org/christian/ebe.pdf*
[212] *http://bib.gnunet.org*

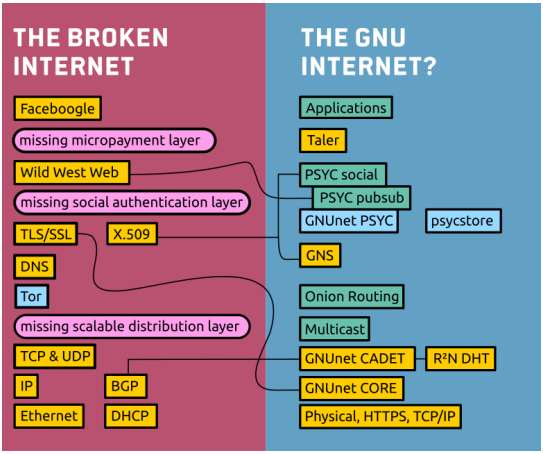


Figura 8: Comparazione tra Internet e GNU Internet (secushare)

La prossima Internet

Per dirla con le parole degli sviluppatori del progetto secushare[213], immaginate di avere le funzioni di Facebook, WhatsApp, Gmail e Skype in una unica applicazione ma *senza controllo centrale* né sorveglianza.

Utilizzando GNUnet per la crittografia end-to-end e l'instradamento anonimo delle comunicazioni, *secushare* aggiunge un nuovo protocollo[214] di trasmissione dei dati al fine di creare un *grafo sociale* distribuito, senza cioè necessità di *server centralizzati* per l'immagazzinamento e lo smistamento delle informazioni. Assieme, queste tecnologie consentono applicazioni distribuite e sicure per email, chat, scambio di contenuti e documenti web; potrebbe essere utilizzata anche come mezzo di comunicazione sicuro per l'IoT (*Internet of Things*)[215].

L'idea generale del progetto è schematizzata nella figura 8. Nel riquadro di sinistra, "The Broken Internet", i

[213] `http://secushare.org`
[214] In realtà esiste da anni ma è poco conosciuto, si chiama *PSYC* (`http://psyc.eu`)
[215] `http://box.secushare.org`

riquadri gialli rappresentano i principali componenti tecnologici dell'attuale rete, partendo da quelli più "fisici" in basso; sono indicati anche i *missing*, ovvero gli "strati mancanti" nell'attuale architettura. Nel riquadro di destra, "The GNU Internet?" i riquadri gialli rappresentano il *core* della nuova Internet[216], quelli verdi e azzurri i "pezzi mancanti" di cui esistono prototipi in fase di sviluppo.

Attraverso la *GNU Internet*[217] gli utenti godranno della velocità di server che sono in grado di *operare senza sapere nulla* in merito alla propria identità, avranno garanzia dell'*autenticità delle proprie relazioni* sociali in un contesto di *effettiva riservatezza*; diventerebbero cioè *indipendenti da infrastrutture centralizzate* e sarebbero tranquilli sapendo che solo i reali destinatari sono in grado di leggere le informazioni che trasmettono.

Secushare è ancora in fase di ricerca e sviluppo e non è ancora disponibile un prototipo. Lo scopo ambizioso di combinare il nuovo *stack* di rete con applicazioni distribuite alternative a quelle in cloud richiede ancora tempo, risorse e competenze per essere raggiunto.

I ricercatori e gli sviluppatori del progetto *secushare* non sono gli unici ad essere convinti che sia necessario riprogettare profondamente Internet, anche la Commissione Europea, all'interno della strategia per il "*Digital Single Market*", si è fatta promotrice dell'iniziativa Next Generation Internet[218] che, attraverso una consultazione pubblica[219] e uno studio appositamente commissionato[220], ha portato alla redazione del rapporto "*Next Generation Internet 2025*"[221] - nel quale viene presentata una analisi

[216] Corrispondono precisamente a quanto si sta sviluppando nel progetto GNUnet e GNU Taler.

[217] In inglese Gnu (l'animale) e *new* (nuovo/nuova) si pronunciano allo stesso modo. Troviamo sia un gioco di parole divertente, gli anglosassoni lo etichettano di solito con la dicitura: *pun intended*.

[218] *http://ec.europa.eu/futurium/en/node/1460*

[219] *http://ec.europa.eu/digital-single-market/en/news/consultation-next-generation-Internet*

[220] *http://www.ngi.eu/about/ngi-study*

[221] *http://ec.europa.eu/digital-single-market/en/news/next-generation-Internet-2025-final-report-study*

in merito alle tecnologie chiave per la futura Internet e le raccomandazioni per la gestione delle iniziative di sviluppo - e all'avvio del programma ufficiale "*Next Generation Internet*"[222].

Sulla pagina di presentazione ufficiale dello studio sopra citato si legge, *testualmente* (traduzione a cura degli autori, grassetto originale)[223]:

> *Sappiamo che la sicurezza di Internet è stata deliberatamente sovvertita dal governo USA fin dagli inizi. Le rivelazioni scioccanti dei whistleblower* 🕮 *hanno svelato le vulnerabilità di fondo che necessitano di essere affrontate urgentemente, si tratta di un compito immenso. Inoltre, abbiamo visto come un piccolo insieme attori molto grossi siano riusciti ad utilizzare il loro vantaggio di essere stati i primi per dominare i nostri mercati interni in modi molto sfavorevoli e indesiderabili. É assolutamente chiaro che la combinazione delle due questioni significa che la sopravvivenza stessa dell'Europa come attore globale di rilievo è a rischio.*
>
> *Lo studio NGI esamina come affrontare questa* ***urgente crisi con molteplici sfaccettature*** *e supporterà la Commissione Europea a comprendere come riprogettare Internet e di conseguenza a* ***ricostruire la fiducia*** *in una Internet post-Snowden — ove necessario ripartendo da capo.*

[222] `http://www.ngi.eu`
[223] `http://www.ngi.eu/about/ngi-study`

Capitolo 1

Livello 1 [*services*]

"Tempi Moderni" di Charlie Chaplin

Il **Livello 1** [***services***] affronta l'aspetto *servizi digitali* (online, via rete) delineandone caratteristiche desiderate, attenzioni verso i problemi che potrebbero introdurre e considerazioni progettuali.

La disponibilità di servizi online che rispecchiano quelli *fisici*, che definiamo *analogici* per contrasto con quelli *digitali*, può avere un **impatto significativo sui diritti di cittadinanza**, soprattutto per quelli erogati dalla P.A. (Pubblica Amministrazione) dei quali non esiste un'alternativa *analogica*[1]: se per pagare le tasse o chiedere una licenza non c'è altra scelta che passare attraverso un sito web di un ente, mi devo adeguare alle modalità e agli strumenti richiesti. Però anche al di fuori della P.A., ad esempio nel contesto commerciale, servizi digitali mal progettati e mal realizzati possono rendere difficile la vita dei clienti, con fastidiose *restrizioni* quali ad esempio:

- vincolare l'accesso ad un conto corrente al possesso di uno *smartphone*;
- prevedere la compilazione di moduli di richiesta e più in generale accettare solo documenti prodotti tramite software *proprietari* (si veda sezione "*Software Libero*" - 3.4.1);

[1] O una soluzione digitale alternativa, ad es. una mail in caso di malfunzionamento di un sito web.

- pubblicare le informazioni sulla propria attività utilizzando una piattaforma social[2].

Il modo in cui vengono forniti i servizi online deve soddisfare gli standard di usabilità e non richiedere competenze o conoscenze speciali (cfr. capitolo "*Livello 3 [education]*" - 3), deve garantire la privacy dei cittadini - per altro protetta da specifiche leggi in diverse legislazioni nazionali - e la trasparenza dell'amministrazione. L'impatto di un progetto inadeguato è ben rappresentato dal fallimento del sito web della riforma sanitaria del Presidente Obama [SS13] anche se gli obiettivi erano alti e il sistema doveva integrare basi di dati grandi ed eterogenee[3]. Altri esempi eclatanti sono i siti dei vari concorsi pubblici italiani che *cadono* (i.e., non reggono il picco di lavoro) proprio a ridosso delle scadenze per le presentazioni delle domande. O ancora, siti web che vengono creati con grande dispendio di risorse economiche e **solo successivamente** si cerca affannosamente di trovargli uno scopo come nel caso *italia.it*[4].

1.1 Digitalizzazione dei servizi

Il termine *digitalizzazione dei servizi* indica il processo per cui un servizio tradizionalmente espletato o fornito in forma analogica viene implementato attraverso tecnologie digitali.

Servizio va qui inteso nella sua accezione più generale: qualunque funzione venga realizzata da enti, aziende, persone e fornita (venduta o meno) ad altri soggetti secondo un protocollo più o meno formalizzato e standardizzato:

- qualche esempio **analogico**:

[2] Alcuni piccoli negozi/ristoranti/ecc. hanno il *vizio* di presentarsi solo su Facebook o Instagram, stupidamente tagliando fuori chi non ha un *account* su tali piattaforme.

[3] *http://archive.nytimes.com/www.nytimes.com/interactive/2013/10/13/us/how-the-federal-exchange-is-supposed-to-work-and-how-it-didnt.html*

[4] *http://it.wikipedia.org/wiki/Italia.it*

  - il classico certificato richiesto presso gli uffici del proprio Comune
  - un bonifico effettuato presso lo sportello di una banca
  - l'iscrizione all'università presso la segreteria
  - chiedere l'ora ad un passante
  - entrare in una pizzeria d'asporto e ordinare tre pizze da portar via
  - andare in un locale per fare nuove conoscenze
  - acquistare un paio di scarpe in un negozio
  - chiedere un parere ad un amico/conoscente
  - prenotare un ristorante
  - leggere un libro cartaceo
- qualche esempio **digitale**:
  - un bonifico effettuato via web (o via *app* 🕮)
  - l'iscrizione all'università via web (o tramite *app*)
  - avere al polso un orologio sincronizzato via radio[5] o guardare un cellulare sincronizzato via rete[6]
  - ordinare tre pizze via web (o tramite *app*) con consegna a domicilio
  - iscriversi e frequentare un sito web per incontri
  - ordinare un paio di scarpe in un negozio online
  - chiedere un parere in un forum
  - prenotare un ristorante via web (o tramite *app*)
  - leggere un libro digitale (ebook)

Esaminando queste due liste e prendendo esempi tratti dalla propria esperienza si può ragionevolmente pensare che l'implementazione digitale di molti servizi sfrutti il canale web o un'*app* per eliminare *una parte* dell'interazione fisica, sia essa di persona che per telefono.

Inoltre esistono casi di servizi nati direttamente in forma digitale perché non immaginati prima o non realizzabili in forma tradizionale, ad esempio la gestione remota delle apparecchiature di casa o l'effettuazione di un backup via

[5] *http://www.ptb.de/cms/en/ptb/fachabteilungen/abt4/fb-44/ag-442/dissemination-of-legal-time/dcf77.html*

[6] Protocollo NTP (*http://www.ntp.org*).

rete su un server remoto.

Ogni servizio, sia digitale che tradizionale, ha almeno due macro-componenti: il *frontend*, cioè l'interfaccia verso gli utenti, e il *backend*, cioè la parte del sistema che svolge effettivamente la funzione. Per un servizio tradizionale il *frontend* può essere uno sportello a cui rivolgersi mentre il *backend* è composto dagli uffici amministrativi che poi portano avanti il lavoro. Nel caso di un servizio digitale l'esempio classico del *frontend* è la pagina web che va aperta per accedere al servizio (e in cui probabilmente si compila un *form*, un modulo) mentre il *backend* potrebbe essere un server che implementa la funzione richiesta[7].

Quando si *digitalizza* un servizio tradizionale, cioè lo si implementa attraverso un processo informatizzato, si può decidere di rendere digitale il *frontend*, il *backend*, o entrambi. Può anche accadere che alcune parti del *backend* rimangano analogiche per motivi organizzativi, risorse economiche o impossibilità di digitalizzare o automatizzare l'operazione. In questi casi il processo globale potrebbe soffrire di rallentamenti dato che gli umani sono meno veloci delle macchine o, peggio, lavoratori umani potrebbero venire spinti a modalità e turni di lavoro *inumani* come nel famoso caso Amazon[8] che ci ha suggerito l'immagine in epigrafe.

Infine si può decidere di affiancare il servizio digitale a quello tradizionale oppure sostituire completamente quello tradizionale con quello digitale.

Ispirandoci alle domande fondamentali del giornalismo, le famose *5W+1H* - Who, What, When, Where, Why, How - definiamo che gli aspetti fondamentali di un servizio da analizzare sono i seguenti:

- **chi**: chi può chiederlo, chi è il fornitore o l'intermediario,
- **cosa**: qual'è la natura della funzione fornita,

[7] N.B. *frontend* e *backend* sono software, sovente *girano* su server differenti.

[8] *http://www.huffingtonpost.co.uk/2013/11/25/amazon-staff-investigation_n_4335894.html*

- **quando**: quali sono le tempistiche di accesso e fornitura,
- **dove**: "luogo" di erogazione, non necessariamente un luogo fisico,
- **quanto**: prezzi e costi,
- **come**: formati e canali di comunicazione, device da usare, informazioni di processo.

Per puro esercizio di ragionamento applichiamo questi criteri ad un servizio tradizionale come la richiesta di un certificato anagrafico[9]:

- **chi:** può chiederlo un cittadino, viene fornito dagli Uffici Anagrafe del Comune
- **cosa:** viene prodotto un certificato stampato su carta semplice o bollata
- **quando:** la richiesta deve avvenire in orario di sportello, tipicamente viene fornito immediatamente
- **dove:** va richiesto presentandosi agli sportelli
- **quanto:** tariffa dipendente dalla eventuale presenza del bollo
- **come:** interlocuzione a voce, certificato prodotto su carta (a volte filigranata o timbrata a secco)

Vediamo però anche la sua versione digitale, utilizziamo[10] il Comune di Milano, pagina relativa alla richiesta di certificati online[11] e chiediamo un certificato di nascita:

- **chi:** può chiederlo un cittadino, viene emesso direttamente dal server dell'anagrafe
- **cosa:** viene prodotto un certificato in PDF, scaricabile dalla pagina web di richiesta e inviato per email
- **quando:** la richiesta può avvenire in qualunque orario, viene fornito immediatamente
- **dove:** va richiesto autenticandosi (ad esempio via *SPID* 🕮) alla pagina web relativa alle richieste di cer-

[9] Si potrebbe definire l'*Hello World* 🕮 dei servizi.

[10] Abbiamo chiesto un certificato reale durante la stesura di questo paragrafo, tempo impiegato: circa 2 minuti. Avendo già un *account* 🕮 *SPID* 🕮.

[11] *http://www.comune.milano.it/servizi/certificati-di-cittadinanza-residenza-stato-civile-e-stato-di-famiglia*

tificato, chiaramente indicata nella pagina principale del sito del comune
- **quanto:** gratuito, l'eventuale bollo[12] va apposto a cura dell'interessato
- **come:** si compila un modulo web, certificato prodotto su file PDF firmato digitalmente

Già da questo esempio minimale vediamo come la versione digitale del servizio ha il notevole vantaggio del **risparmio di tempo**: invece di uscire di casa e raggiungere il Comune, fare la coda allo sportello, parlare con l'operatore mostrandogli un documento, pagare e tornare a casa, è bastato aprire un *browser*, andare su una pagina web, digitare poche informazioni e dopo pochi secondi il certificato era già pronto da stampare (se proprio necessario). Pochi minuti contro qualche ora[13]. Inoltre non si è vincolati ad orari di sportello e l'oggetto ricevuto è già digitale e può quindi essere inviato via email o web senza bisogno di scansionarlo o peggio *inviarlo via fax*.

Ovviamente ci sono dei **però**. Per usufruire del servizio digitale abbiamo dovuto dotarci di un po' di tecnologia: un computer o uno smartphone, una connessione Internet[14], un *account* SPID, un indirizzo di mail e infine la capacità di gestire un file PDF. Chi legge questo testo ha molto probabilmente tutte le dotazioni qui elencate, ma non tutti i cittadini sono nelle stesse condizioni: se uno smartphone con traffico Internet incluso è ormai appannaggio di buona parte della popolazione italiana (includendo anche gli anziani[15]) non è altrettanto vero per lo *SPID* 🕮 che a oggi[16] conta poco meno di 5 milioni[17] di registrazioni. Stiamo quindi evidenziando quanto i vari aspetti (*chi*, *cosa*, …)

[12] Acquistabile presso rivendita Valori Bollati.

[13] Per il Comune di Milano, nei comuni piccoli la situazione delle code è migliore.

[14] Non filtrata da firewall verso il sito del Comune, cfr. Livello 0 dell'Arcobaleno.

[15] *http://www2.deloitte.com/it/it/pages/technology-media-and-telecommunications/articles/mobilesurvey-italy-tmt.html*

[16] Ottobre 2019

[17] *http://avanzamentodigitale.italia.it/it/progetto/spid*

siano legati tra loro: ad esempio la scelta tecnologica sul *come* influenza il *chi*.

Occorre quindi progettare bene un servizio digitale che andrà a sostituirne uno analogico: le scelte tecnologiche hanno forte impatto sull'efficacia, sull'utilità, sull'usabilità e sull'accessibilità da parte di utenti finali, ma anche da parte di enti terzi che vogliano costruire *servizi integrati su altri servizi*[18]. Vediamo quindi alcuni aspetti importanti.

1.1.1 *Fallback*

Qualunque meccanismo si può rompere o inceppare. In questo contesto ci riferiamo all'insieme dei componenti e delle persone che concorrono alla implementazione di un servizio.

Un meccanismo può anche essere molto complicato da interpretare e utilizzare e in alcuni casi estremi, come utilizzatore, potrei non essere disposto ad adattarmi alle procedure. Un meccanismo rigido, che non ammette eccezioni, si inceppa più facilmente di uno flessibile. Invece uno implementato da persone permette un certo grado di tolleranza: l'essere umano può usare il proprio libero arbitrio per integrare minime mancanze, come ad esempio una data mancante su un modulo cartaceo. Quando un processo viene realizzato da un sistema informatico la flessibilità tende[19] a diminuire. Basta fare caso quando si compilano i moduli online, a volte si incontrano regole di validazione dei campi troppo rigide:

- indirizzi email che non vengono accettati se non sono di provider noti (i.e., diversi da Gmail, Yahoo, Aruba, Hotmail… raro ma è capitato)

[18] Si pensi ai *broker* di voli e hotel come Trivago e Kayak che si appoggiano a servizi come Expedia e Booking.

[19] Dipende da come viene programmato il sistema, purtroppo è più semplice implementare procedure rigide, ad es. è esperienza comune incontrare form web i cui campi sono da compilare secondo *pattern* stabiliti e rigidi, a volte così rigidi che rendono impossibile il portare a termine l'operazione.

- targhe non più accettate perché nel frattempo era cambiata la struttura della Provincia (caso in cui è incappato uno degli autori, da provincia di Milano a Monza-Brianza, ma con targa "MI")

Nella realizzazione in forma digitale di un servizio bisogna tenere conto di quali vincoli stiamo imponendo all'utilizzatore, se tali vincoli sono eccessivi[20] il servizio è inutilizzabile o è utilizzabile da meno utenti di quelli stimati in fase di progettazione.

Se invece la funzionalità offerta da un servizio prevede **canali alternativi** allora viene ampliata la cosiddetta *base utenti* perché ogni utente può scegliere il canale a lui più congeniale. E se un canale non funziona, anche solo temporaneamente, è possibile usarne uno alternativo: il cosiddetto *fallback* (ripiego, riserva, alternativa).

Potremmo anche definirlo il ***diritto di scegliere come** usufruire di un servizio*: via web, allo sportello, per posta[21], per telefono, per delega, a domicilio ecc. Chiaro che non è necessario prevedere tutti i canali possibili e immaginabili, ma offrire un ventaglio di opportunità aumenta la fruibilità del servizio stesso.

Nulla osta il fatto che le varie possibilità siano offerte a prezzi differenti, beninteso sempre nei limiti della piena accessibilità per tutte le categorie di censo, specie se si tratta di *servizi di cittadinanza* (di cui ragioneremo nel capitolo "*Livello 2 [access]*" - 2).

Un caso frequente è quello in cui si *digitalizza* un servizio analogico esistente: per avere una **alternativa inclusiva** sarà sufficiente mantenere un certo numero[22] di sportelli attivi che funzioneranno da *rete di sicurezza*: è la strada attualmente seguita da banche, poste e in ge-

[20] Anche solo soggettivamente oltre che tecnicamente/oggettivamente, in questo ambito la cosiddetta UX (User Experience) fa da padrone, se una procedura risulta *difficile/difficoltosa* per l'utente è stata progettata male.

[21] Nei paesi anglosassoni era comune richiedere servizi, certificati o documenti via posta tradizionale.

[22] Minore rispetto alla situazione originale, nella speranza che buona parte dell'utenza migri al servizio digitale.

nerale tutti quegli enti fornitori di servizi *di sportello* che stanno migrando verso canali digitali per l'interazione con l'utenza.

Ovviamente esistono servizi per cui è difficile mantenere una alternativa analogica, si pensi ai vari sistemi di *sharing* (bike, car e ora i monopattini) per cui è naturale l'implementazione attraverso *app* per cellulari[23] ed è difficile pensare a soluzioni analogiche.

Ma esistono anche servizi digitali che vengono *pensati male*, a questo proposito ad ogni corso universitario di CDT proponiamo un esercizio ai nostri studenti: trovare servizi digitali carenti in termini di alternativa. Ecco qualche esempio:

- **Documento di Gara Unico Europeo** (DGUE): nella procedura standard per (auto)certificare i requisiti per la partecipazione alle gare di appalto, dopo un periodo di transizione scaduto nel 2018, viene previsto solo il caricamento online in forma digitale[24].
- **Deposito di Sentenza Penale**: da gennaio 2019 le nuove disposizioni prevedono che l'avviso di deposito della sentenza penale debba avvenire solo online[25].
- **Comune di Bisceglie, comunicazioni attività produttive**: a partire da gennaio 2019, in ottemperanza all'art. 2 del D.P.R. n. 160 del 2010[26] queste comunicazioni vanno inviate solo online[27].

[23] Agli *albori* alcuni servizi (ad es. Enjoy e il Comune di Milano) offrivano l'accesso attraverso *call center*, ma è stato rapidamente dismesso perché antieconomico e macchinoso.

[24] *http://www.codiceappalti.it/DLGS_50_2016/Art__85_Documento_di_gara_unico_europeo/8464*

[25] *http://www.responsabilecivile.it/sentenze-penali-dal-1-gennaio-avviso-deposito-solo-online*

[26] "le domande, dichiarazioni, segnalazioni e comunicazioni concernenti le attività produttive, di prestazione di servizi, e quelle relative alle azioni di localizzazione, realizzazione, trasformazione, ristrutturazione o riconversione, ampliamento o trasferimento, ed i relativi elaborati tecnici e allegati, devono presentarsi esclusivamente online."

[27] *http://www.comune.bisceglie.bt.it/istituzionale/organigramma/sportello-unico-attivita-produttive*

- **Sportello studenti dell'Università degli Studi di Milano, procedure di iscrizione**: iscrizione ai corsi, comunicazioni varie, registrazione agli esami e prenotazioni appuntamenti per accedere allo sportello sono possibili solo online[28].
- **Dichiarazione di successione**: da gennaio 2019 avverrà solo per via telematica; nota ulteriormente dolente è che per utilizzare il servizio bisogna scaricare un software dedicato[29] (dichiarato compatibile con Windows, Mac e alcune versioni di Linux, ma non con i cellulari, ergo serve per forza un personal computer) di cui non viene specificata la licenza e di cui non si può verificare quindi la *sanità* (assenza di pericoli per il proprio device e dati).
- **Autostrada Pedemontana**, "Autostrada a pedaggio Free Flow senza barriere con obbligo di pagamento del pedaggio entro 15 giorni dal transito"[30]: fra le prime autostrade in Europa ad aver eliminato i caselli autostradali grazie all'uso di telecamere che rilevano le targhe dei veicoli in transito. Chi non ha il *Telepass* (in tal caso l'addebito è automatico) può effettuare il pagamento del pedaggio autostradale esclusivamente per via telematica (sito o app). Inoltre la segnaletica che avvisa di questo obbligo non è perfettamente chiara (di notte, per gli stranieri, per gli anziani) e può quindi implicare multe o lettere di ingiunzione di pagamento.
- **Nove25**, negozio di gioielli d'argento molto usato dai giovani: le uniche modalità di contatto col fornitore sono via email, WhatsApp e Messenger[31], non esiste un *call centre*.

[28] *http://www.unimi.it/studenti/segreterie/2462.htm*

[29] *http://www.agenziaentrate.gov.it/wps/content/Nsilib/Nsi/Schede/Dichiarazioni/Dichiarazione+di+successione/SW+Comp+dichiarazione+successioni+telematiche/?page=dichiarazionicitt*

[30] *http://www.pedemontana.com*

[31] *http://www.nove25.net/it/cms/contatta-nove25*

1.1.2 Protocolli

Ci riferiamo qui ai *protocolli di rete*, cioè a quelle specifiche che definiscono come un programma, solitamente chiamato *client*, deve comunicare con un altro programma, solitamente chiamato *server*. La specifica di un protocollo tipicamente prevede quale debba essere il formato dei dati (binari o testuali), le regole di validazione e le sequenze temporali (cioè in che ordine i messaggi vanno scambiati) che i due *soggetti* debbono utilizzare per potersi trasmettere dati.

Ad esempio il protocollo HTTP[32], quello che viene usato dal browser per recuperare contenuti in rete, prevede una serie di comandi come `GET`, `POST`, `PUT` ecc. che permettono l'interazione tra il browser e il web server nella richiesta di pagine web. L'utente finale che naviga in rete non vede nulla di tutto ciò, ma quando si digita un *URL* 📖 nella barra dell'indirizzo di un browser viene attivata una sequenza di azioni:

- l'*URL* 📖 viene scomposto nelle sue componenti, ad esempio "http://tools.ietf.org/html/rfc7231" contiene informazioni su:
  - protocollo da usare per la connessione: *HTTP*
  - sito da contattare: *tools.ietf.org*
  - directory in cui trovare il documento: *html*
  - documento richiesto: *rfc7231*
- viene aperta una connessione verso il sito individuato
- al sito viene inviato un comando HTTP che contiene tra le altre cose la richiesta `'GET /html/rfc7231'`
- il server fornisce il documento (o un errore)
- il browser a questo punto riceve il contenuto HTML e lo visualizza sullo schermo dell'utente

Siamo entrati nel merito tecnico di questo piccolo esempio per evidenziare il fatto che se un protocollo è definito in un documento tecnico[33] e se la sua implementazione non

[32] *http://tools.ietf.org/html/rfc7231*

[33] La già citata RFC (Request For Comments) nel caso del protocollo HTTP. Si noti inoltre che HTTP è anche *human readable* (comprensibile da un essere umano) perché i comandi sono parole

è vincolata da brevetti o normative ostative, chiunque ne abbia le competenze e le risorse può realizzare software che *parla* quel protocollo, potendo quindi interagire col servizio in oggetto.

Non è un caso che, essendo HTTP un protocollo libero[34], **oggi esistano molti programmi**[35] che lo utilizzano e che l'utente può scegliere liberamente secondo le sue aspettative e preferenze. Si realizza cioè una situazione di naturale concorrenza fra diversi produttori di software che allarga il ventaglio delle opzioni e che abbassa i prezzi[36] di accesso al servizio.

Un **esempio negativo**, cioè di protocollo *segreto*, e delle sue conseguenze lo possiamo fare citando il caso delle termo-valvole Bluetooth Eqiva[37] di eQ-3. Queste termovalvole controllano la temperatura di un ambiente regolando l'afflusso di acqua calda al calorifero a cui sono applicate, ma aggiungono la possibilità di essere programmate per impostare temperature diverse in orari e giorni diversi. La programmazione si effettua tramite bottoni e cursori sulla valvola stessa oppure utilizzando una *app Android o iOS* (si veda figura 1.1). L'applicazione Android non è perfetta[38], ma purtroppo non ci sono alternative: il protocollo di comunicazione tra valvola e smartphone è segreto... Questa era la situazione fino all'anno 2016 quando uno degli autori del presente testo ha fatto da relatore di una tesi sul *reverse engineering* 🕮 del protocollo delle termo-valvole. Tale tesi ha avuto successo nonostante il rifiuto da parte dell'azienda di divulgare informazioni sul protocollo ed è

inglesi e non astruse/oscure sequenze di caratteri.

[34] Approfondiremo il tema della libertà del software, hardware, protocolli e formati nel capitolo "*Livello 3 [education]*" - 3.

[35] I vari browser, liberi e non, disponibili sul mercato: Chrome/-Chromium, Firefox, Opera, Edge, Safari, Lynx, elinks, w3m, dillo, alice, ...

[36] Spesso azzerandoli.

[37] *http://www.eq-3.com/products/homematic/detail/bluetooth-smart-radiator-thermostat-uk-351.html*

[38] Ad esempio costringe l'utente a selezionare ogni singola valvola da configurare con un determinato programma settimanale, non c'è modo di programmare tutta la casa in un colpo solo.

Figura 1.1: Interazione termo-valvola ↔ Android app (Sergio Alberti)

persino sfociata in un progetto finanziato dal GSoC (*Google Summer of Code*). Così oggi è disponibile[39] il software *libero* (vedi sezione "*Software Libero*" - 3.4.1) per integrare tali valvole all'interno di un sistema domotico. In altre parole le valvole si possono programmare anche da un computer normale, senza bisogno dell'applicazione specifica del produttore, è stato quindi eliminato il fattore *lock-in* (cfr. sezione "*Lock-in*" - 1.1.5).

1.1.3 Formati

Un formato dati è concettualmente simile ad un protocollo, ma si riferisce alla memorizzazione dei dati in un file. Invece che specificare un linguaggio di interscambio fra programmi, specifica l'organizzazione dei dati su un supporto di immagazzinamento: dischi fissi, chiavette USB ecc.

Il lettore avrà sicuramente notato, durante la sua vita di utente di programmi vari, che i file prodotti dagli strumenti di produttività personale terminano con le cosiddette *estensioni*: .doc, .xls, .txt, .mp3, .mp4, .odt ecc. Tali

[39] *http://sergioalberti.gitlab.io/gsoc/debian/2018/09/24/reveng.html*

desinenze rappresentano un meccanismo **convenzionale** di riconoscimento del **formato del file** in oggetto.

Pensiamo anche che avrà notato come sia possibile *aprire* (elaborare) uno stesso file con programmi diversi ottenendo risultati identici o molto simili, ad esempio è sicuramente possibile ascoltare un file *mp3* con diversi programmi tipo *mplayer* su GNU/Linux, *Windows Media Player* su Windows o quelli integrati nei *device* come iPod, smartphone o le varie smartTV; in maniera analoga è anche possibile elaborare un foglio elettronico in formato *xls* sia con *Microsoft Excel* che con *LibreOffice* o *Gnumeric*.

Quello che sta succedendo è che i vari programmi sono realizzati in modo da **concordare su uno stesso formato per i dati che elaborano**. Come avviene questa *concordanza*? Tipicamente in due modi:

- *De iure*, tramite accordi espliciti e formali tra produttori che si organizzano in enti di standardizzazione[40]: attraverso processi di proposta e revisione assembleari i vari standard vengono approvati e pubblicati e vengono considerati, appunto, *standard* per determinati contesti applicativi. Il processo può essere attivato in assenza di software già disponibili (quindi *a priori*) oppure nascere da un'esigenza di standardizzazione di una situazione di mercato *disordinato*, in cui ogni produttore ha stabilito[41] il proprio formato. Nessuno standard è un obbligo, ma chi non segue gli standard e non ha la forza di mercato per imporne uno rischia di perdere clienti (cfr. effetto *lock-in* poco più avanti). Un esempio di formato di questo tipo è HTML, standard del W3C.
- *De facto*, un formato molto utilizzato ma mai passato attraverso una formale e ufficiale approvazione da parte di qualche ente standardizzatore. Capita spesso nel mondo del Software Libero (cfr. sezione "*Soft-*

[40] Citiamo alcuni enti standardizzatori mondiali famosi: IEEE (*http://ieee.org*), ISO (*http://iso.org*), W3C (*http://w3c.org*), IETF (*http://ietf.org*), ECMA (*http://ecma-international.org*).

[41] E spesso cercato di imporre con tattiche monopolistiche.

ware Libero" - 3.4.1) dove i formati di memorizzazione dei dati sono pubblici e liberamente implementabili[42], quando non addirittura ben documentati. Può accadere che un particolare programma per computer diventi leader di mercato nel suo campo. Se il formato dei dati non è segreto ed è liberamente implementabile è possibile che altri produttori creino programmi alternativi che supportano lo stesso formato dei dati, così gli utenti possono scegliere liberamente programmi diversi in funzione delle prestazioni senza timore di dover rifare tutto il lavoro.

- *De visu*[43], tramite *reverse engineering* 🕮 è possibile *scovare* le informazioni necessarie per ricostruire il formato dei dati e utilizzarle per scrivere software in grado di elaborare i file in quel formato. Questo tipo di attività è di solito particolarmente dispendiosa e viene utilizzata in alternativa alle altre due citate precedentemente, ovvero quando il formato non è documentato perché tenuto segreto.

Per approfondimenti si veda "*Apriti standard!: Interoperabilità e formati aperti per l'innovazione tecnologica*" [Ali14].

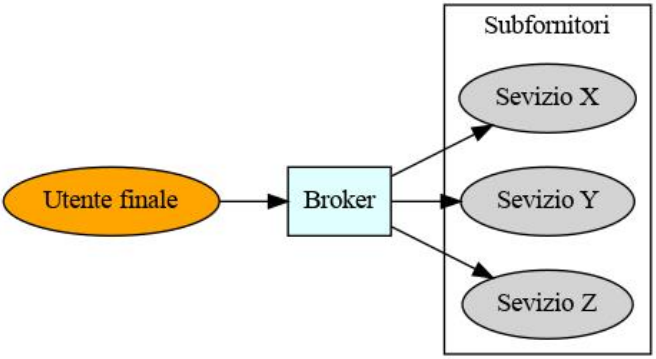
1.1.4 Interoperabilità

Applicando le *5W+1H* viste in sezione "*Digitalizzazione dei servizi*" - 1.1 si potrebbe riassumere il tema *protocolli e formati* con la frase: la scelta sul **come** alza o abbassa il *gradino* di ingresso per sviluppatori terzi e quindi riduce o aumenta la possibilità di ampliare l'offerta di software per accedere ad un servizio, cioè di fatto restringe o amplia il **chi**. Il concetto di *interoperabilità* è in fondo una generalizzazione di ciò che abbiamo visto nelle sezioni "*Protocolli*" - 1.1.2 e "*Formati*" - 1.1.3 e ci porta ad allargare questo *chi* a ogni tipo di entità: dalla persona fisica (utente finale di un

[42] Il formato è implementato attraverso software di cui è disponibile il sorgente, quindi si può ricavare avendo le necessarie competenze.

[43] Termine nostro.

servizio) fino ad una azienda che vuole costruire un proprio servizio basandosi su servizi esistenti. L'esempio classico in quest'ultimo caso sono i *broker* di servizi, come Trivago[44] o Kayak[45], che selezionano offerte comparando prezzi da fornitori diversi, lo schema è in fondo molto semplice:



All'utente viene presentata tipicamente un'interfaccia web che viene costruita interrogando (quasi in tempo reale) altri servizi esterni al *broker*.

Perché questo schema funzioni c'è bisogno che i vari sistemi (del broker, ma soprattutto dei fornitori terzi) siano *interoperabili* cioè che permettano un'interazione non solo da parte di una persona[46], ma anche *digitale*, *machine to machine* o anche b2b (*business to business*). In questi casi l'interazione tra il *broker* e i servizi dei sub-fornitori si serve di protocolli di comunicazione *ad hoc*, il più noto è REST (*REpresentational State Transfer*). Con questi protocolli è possibile accedere *programmaticamente*, tramite le cosiddette API (*Application Programming Interface*), ai sub-servizi implementando sovra-servizi integrati. A volte, anche per ovvi scopi di monetizzazione di un sub-servizio, tale accesso *b2b* è vincolato ad un pagamento proporzionale al volume di richieste che vengono sottoposte al sistema.

[44] *http://trivago.it*
[45] *http://kayak.it*
[46] L'utente finale che consulta direttamente il sito web di Expedia.

Come valutare il livello di interoperabilità di un sistema? Esso è alto quando il sistema soddisfa tutti questi requisiti:

- utilizza **formati standard** e liberi quindi i dati che genera possono essere esportati senza troppi problemi verso altri sistemi;
- supporta **protocolli standard** e liberi quindi è accessibile usando software sviluppati da terzi;
- impone **poche limitazioni** di accesso:
  - economiche;
  - temporali[47];
  - di provenienza[48];
  - di licenza d'uso [PCA18].

Un esempio positivo[49] di interoperabilità lo si trova in molti siti *opendata* 🕮[50]. La creazione di questi servizi è un requisito di legge per la P.A. e, sebbene con alterne fortune, negli ultimi anni si sta assistendo ad un certo *fervore* nella pubblicazione e pubblicizzazione[51] di *dataset opendata* 🕮. I dati immagazzinati in questi portali sono accessibili sia mediante scaricamento (*download*) che mediante interrogazione diretta (*query*) tramite API (figura 1.2).

Purtroppo è facile trovare anche esempi negativi: citiamo il recente (2019) caso di Trenitalia[52] che ha iniziato una battaglia legale[53] contro i creatori dell'*app* Trenit[54] accu-

[47] Ad esempio limitando il numero di richieste che si possono sottomettere per unità di tempo.

[48] Ad esempio limitando la sottomissione delle richieste per regioni (indirizzi IP) di provenienza.

[49] Che riprenderemo quando parleremo di trasparenza nel secondo volume.

[50] Citiamo: *dati.lombardia.it*, *data.gov.uk*, *data.gov*.

[51] L'uso da parte di terzi diventa infatti sia un *vanto* che un fattore di KPI nella valutazione oggettiva dell'operato degli enti. Si veda ad esempio la pagina in cui la Regione Lombardia elenca gli usi che vengono fatti dei dati che pubblica: *http://hub.dati.lombardia.it/stories/s/Analisi-dei-dati-e-Data-Visualization/mmj4-svtr*.

[52] *http://trenitalia.com*

[53] *http://www.wired.it/lifestyle/mobilita/2019/07/29/trenitalia-trenit-dati-treni*

[54] *http://trenit.app*

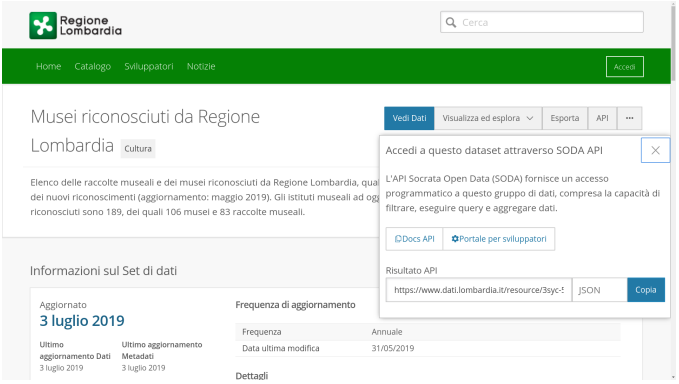


Figura 1.2: Portale Open Data Regione Lombardia, dettaglio API

sandoli di utilizzare illegalmente i dati pubblicati sul sito Trenitalia (in particolare da *viaggiatreno.it*). L'*app* usa i dati di Trenitalia per rendere più fruibile le informazioni sui treni ai viaggiatori e offre la possibilità di acquisto dei biglietti **rimandando l'utente al sito di Trenitalia**[55] ponendosi quindi come un *broker positivo*, un aggregatore di informazioni che probabilmente veicola ulteriori clienti al fornitore originale del servizio, Trenitalia appunto.

Concludendo possiamo affermare che l'aumento di interoperabilità di un servizio abbassa il *gap* (gradino) d'ingresso per altri fornitori di servizi e quindi aumenta la concorrenza globalmente migliorando l'esperienza[56] del cliente.

1.1.5 *Lock-in*

Il concetto di *lock-in*[57] è il contrario dell'interoperabilità: si dice che un sistema è affetto[58] da *lock-in* quando è poco o

[55] Che non brilla per usabilità.

[56] Dal punto di vista meramente finanziario, ma anche di fruibilità (più canali → posso scegliere quello che mi è più comodo).

[57] Dall'inglese: intrappolare, costringere, chiudere dentro.

[58] Usiamo di proposito il termine medico normalmente riferito alle malattie.

per nulla interoperabile ed è chiuso in se stesso. Scegliere di realizzare un servizio con un sistema ad alto *lock-in* implica la quasi totale impossibilità di passare, magari mantenendo lo storico delle operazioni fatte e dei dati creati, ad altro sistema qualora si rivalutassero le opzioni implementative. Questo avviene perché chi realizza sistemi ad alto *lock-in* lo fa utilizzando combinazioni di formati e protocolli non standard o non liberi[59], rendendo molto difficile agli utenti il passaggio ad altro sistema senza perdita di dati pregressi.

Un esempio eclatante lo troviamo in Outlook, il programma di gestione della posta elettronica di Microsoft. Chi lo usa (forse non) sa che tutti i propri dati, cioè tutta la posta elettronica archiviata nel corso del tempo, vengono immagazzinati in alcuni file il cui formato è **proprietario e non documentato**. L'eventuale intenzione di passare ad altro software di gestione della *mail* viene frustrata dalla difficoltà[60] di trasferire il lavoro fatto fino a quel punto. Per contro, utilizzando formati di archiviazione standard e aperti come *mbox*[61] e *maildir*[62] si può addirittura avere un archivio della propria corrispondenza utilizzabile **contemporaneamente** con più programmi diversi[63].

Se il *lock-in* è una caratteristica negativa, perché viene introdotta nei sistemi informatici? Perché una caratteristica negativa per l'utente non necessariamente lo è per chi produce e distribuisce software, anzi il produttore di *software proprietario*[64] tende ad alzare quanto più possibile il

[59] Vale a dire non implementati per mezzo di software libero.

[60] In passato sono esistiti strumenti software di conversione (realizzati mediante *reverse engineering* 🕮) verso altri standard, ma i formati dei file di Outlook sono variati nel tempo, ad oggi (2019) gli autori non sono a conoscenza di strumenti aggiornati. L'unico meccanismo, però macchinoso, di migrazione passa attualmente per un *pivoting* su un *mailserver* esterno… che abbia **capienza sufficiente**, infatti non è difficile raggiungere volumi di alcuni GB per anno, specie se nel proprio lavoro si scambiano documenti *voluminosi*.

[61] `http://tools.ietf.org/html/rfc4155`

[62] `http://cr.yp.to/proto/maildir.html`

[63] Esempi di programmi, tutti **liberi**, che supportano quei formati standard: Mozilla Thunderbird, mutt, Claws Mail, Evolution, notmuch, alot, alpine, balsa, kmail.

[64] Nell'ecosistema del Software Libero è esattamente l'opposto.

livello di *lock-in* in modo da rendere difficile per gli utenti *migrare* ad altri software: ciò che è un vincolo per l'utente diventa un vantaggio strategico per il produttore.

Vediamo qualche ulteriore esempio nel contesto dell'hardware, nei *device* che usiamo tutti i giorni.

Da ormai molti anni ci siamo *abituati* (*obtorto collo*) ai *toner* e alle cartucce di inchiostro per le stampanti venduti a prezzi artificiosamente elevati[65]: spesso l'intera stampante costa meno del toner o della cartuccia. Questo avviene perché i produttori hanno inserito dei meccanismi[66] di autenticazione[67] che impediscono il funzionamento della stampante con inchiostri non *certificati* dal produttore. Ovviamente questi meccanismi non sono documentati per cui un eventuale concorrente ha molta difficoltà a produrre toner e cartucce compatibili. La stampante può essere venduta anche sottocosto, il guadagno lo si fa sui *consumabili*, che vengono acquistati regolarmente al contrario della stampante.

Anche il mondo di cavi e alimentatori è un buon esempio **negativo** di campo di battaglia tra interoperabilità e *lock-in*. La guerra è iniziata molto tempo fa con armi primitive che sono state oggetto di grande evoluzione: i connettori (gli *spinotti*). Con l'avvento dei semiconduttori nei dispositivi di uso comune (inizialmente radioline e televisori, poi videocamere, lettori di musica, computer ecc.) l'industria ha dovuto fornire alimentazioni a basse tensioni[68] per i vari prodotti. Dato che i trasformatori erano pesanti e gli apparati erano sempre più piccoli e leggeri, ad un certo punto si pensò di scindere le due funzioni: apparecchio e alimentatore. Ma per non perdere ricavi bisognava impedire ai clienti di utilizzare alimentatori *universali*,

[65] Mitigati dall'arrivo sul mercato di prodotti *compatibili* realizzati per *reverse engineering* 🕮.

[66] Circuiti elettronici che diventano veri e propri *anti-interoperability-chips*.

[67] `http://www.wired.com/2016/09/hp-printer-drm`

[68] Nell'éra delle valvole le tensioni erano elevate e ogni apparato conteneva una sezione di alimentazione la cui fonte era la tensione di rete (115/220V) e che provvedeva a convertire in varie alimentazioni per tensione anodica e filamenti.

magari venduti dalla concorrenza. Per cui cominciò la produzione di alimentatori *dedicati* ad ogni singolo apparato: bastava variare di poco la tensione richiesta[69] per rendere univoco l'accoppiamento tra apparato e alimentatore. La situazione è andata peggiorando negli anni tanto che ad un certo punto alcuni organismi internazionali come l'Unione Europea hanno affrontato il tema studiando normative di omogeneizzazione[70]. Normative che sono state osteggiate da alcuni produttori anche in maniera subdola: ad esempio inserendo *chip* di riconoscimento[71] nei cavi, usando lo stesso principio visto per le cartucce e i toner, in modo da rendere inutili i cavi prodotti da terze parti.

L'ultimo macro-esempio, il più recente e temibile, di meccanismo di innalzamento del livello di *lock-in* è rappresentato dalla tendenza alla *appificazione* dei servizi. Ai *bei tempi* del web (sia 1.0 che 2.0), prima dell'avvento degli smartphone iper-pervasivi[72], col termine *digitalizzazione di un servizio* si intendeva l'implementazione di un sito web che permettesse l'accesso alla forma digitale del servizio stesso. Oggi purtroppo si osserva una predilezione per la realizzazione di *app* per telefono che fa passare quasi in secondo piano l'implementazione del sito web. Ciò è dovuto principalmente al tentativo di inseguire le abitudini di acquisto dei clienti (figura 1.3) che preferiscono usare il cellulare rispetto ad un PC fisso o portatile, potendo così sfruttare i tempi morti di un trasferimento sui

[69] Chi scrive ha la passione per l'elettronica e, come tanti, conserva i vecchi alimentatori in una scatola: "verranno buoni". Un campione casuale della scatola è risultato nelle seguenti combinazioni: $3.6V =$, $5V =$, $7.2V =$, $9V =$, $12V =$, $12V \approx$, $19V =$, con connettori di diverso tipo e polarità sovente invertite (un quasi-standard prevede il '+' centrale nei connettori coassiali, ma alcuni produttori, e.g. Sony, scelgono il '-').

[70] *http://www.hwupgrade.it/news/telefonia/l-ue-torna-a-parlare-di-connettori-per-gli-smartphone-nuove-misure-al-vaglio_77426.html*

[71] *http://gizmodo.com/heres-the-chip-apple-is-using-to-stop-you-from-buying-c-5945889*

[72] iOS nasce nel 2007, Android nel 2008, . Se nei primi anni gli utenti erano misurati in centinaia di milioni, nel 2019 siamo intorno ai due miliardi di device nel mondo.

mezzi pubblici o in coda alla posta. Questo approccio *inseguitore* che porta i produttori a concentrarsi *in primis* sulla versione *app* di un servizio digitale, se estremizzato (versione *sito web* molto limitata o addirittura inesistente), porta *de facto* all'obbligo di possesso di uno smartphone per accedere al servizio stesso, tagliando fuori fette significative della popolazione[73]. L'ipotesi di mutuare questo approccio anche nel contesto dei servizi digitali della Pubblica Amministrazione implica che un cittadino è tale solo se possiede uno smartphone[74] perfettamente funzionante, carico, connesso... e un *account* sull'*app store* di Google o Apple[75]! Ultimo ma non meno importante, una *app* è spesso un sistema chiuso (è tipicamente *proprietaria*, cfr. sezione "*Software Libero*" - 3.4.1) nel senso che:

- **quasi sempre** non permette l'esportazione di dati[76]
- non permette di capire come interagisce col server, ovvero quali protocolli usa.

Cioè rende molto difficile la realizzazione di software alternativo per la fruizione dello stesso servizio. Per contro un sito web è accessibile con la maggioranza dei *browser*, anche da un PC disponibile pubblicamente, è più facilmente analizzabile per capire quali protocolli e strutture dati usa ed è visualizzabile su schermi grandissimi, facilitando gli ipovedenti, o molto piccoli come quelli degli smartphone.

Esempio nel macro-esempio: **l'accesso online, da PC, al proprio conto corrente**. Da settembre 2019 molte banche stanno introducendo meccanismi di autenticazio-

[73] Una domanda che facciamo sempre al corso di Cittadinanza Digitale e Tecnocivismo è: "perché bisognerebbe prevedere canali diversi oltre allo smartphone per un servizio online?" La reazione di primo acchito è **invariabilmente**: "ma oggi chi è che non ha uno smartphone!?!" Dimenticandosi completamente gli anziani o chi, per scelta, decide di non possederne uno.

[74] Android o Apple, altri sistemi (per ora di nicchia) non sono di fatto supportati.

[75] Sia Android che iOS per funzionare, salvo *giri strani* (usando *ROM* 🕮 alternative e *repository* 🕮 non standard), obbligano a registrare un *account* sul sito del produttore.

[76] Spesso non si riesce nemmeno a capire se, dove e come salva i dati sul telefono stesso.

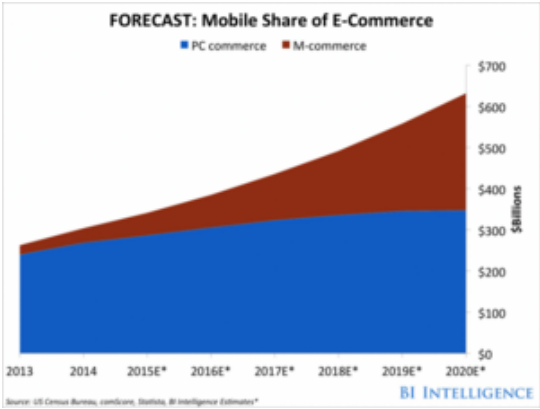


Figura 1.3: Tendenza commercio mobile vs. desktop (jmango360.com)

ne 2FA (*Two Factor Authentication*)[77] poiché la normativa europea di riferimento impone l'implementazione di un doppio canale di autenticazione per elevare i livelli di sicurezza nell'identificazione dell'utente. Purtroppo molte banche hanno interpretato ottusamente questa direttiva attivando una doppia autenticazione via... *app*! Per cui esistono molte banche che **impongono** l'uso di un cellulare *non modificato*[78] per avere accesso online al proprio conto corrente, tra l'altro ignorando completamente l'esistenza di standard internazionali[79] per l'autenticazione 2FA interoperabile, quindi utilizzabile anche utilizzando software libero disponibile sia su smartphone che PC!

[77] *http://en.wikipedia.org/wiki/Multi-factor_authentication*

[78] Quasi tutte le *app* bancarie si rifiutano di girare su sistemi operativi non *stock* o modificati mediante *jailbreak* 🕮

[79] Sono:

- HOTP (*http://tools.ietf.org/html/rfc4226*)
- TOTP (*http://tools.ietf.org/html/rfc6238*)

1.1.6 Scalabilità

Un aspetto importante ai fini della buona realizzazione di un servizio digitale è quello *architetturale*[80] della *scalabilità*:

- Quanto è robusto un sistema nell'espletamento delle sue funzioni all'aumentare degli utenti?
- Se invece gli utenti diminuiscono, il sistema riesce a ridurre le sue richieste di risorse in modo che il suo costo di esercizio si riduca?

Ogni utente che richiede un servizio impegna risorse di calcolo sul server; mentre nell'uso quotidiano gli utenti si distribuiscono in maniera relativamente *uniforme*, in corrispondenza di eventi particolari si possono avere picchi di carico che talvolta diventano insostenibili. Un computer riesce a servire più utenti *contemporaneamente*. In realtà la macchina divide le sue risorse temporalmente occupandosi di ogni utente per un breve istante e passando al successivo in modo così rapido che la percezione è quella di una macchina dedicata. Anche la gestione di questo *round-robin*[81] costa risorse per cui al crescere del numero di utenti le prestazioni globali calano esponenzialmente [TB15].

Un contesto abbastanza frequente in cui si può sperimentare il classico **picco di carico che rende il servizio indisponibile** è quello dei servizi da richiedere entro una scadenza, come la presentazione delle domande di ammissione ai **concorsi pubblici**. Il lettore avrà certamente sentito notizie o letto raccomandazioni come le seguenti:

> - *"Raccomandiamo di non inviare la domanda di partecipazione a ridosso del termine poiché il sito istituzionale potrebbe essere intasato dalle richieste, tenendo anche conto delle tempistiche necessarie a compilare il modulo"*[82]

[80] Cioè del come vengono progettati e combinati i vari componenti di un sistema informatico.

[81] Letteralmente "torneo in cui tutti gareggiano con tutti", ma nel contesto è più significativo il termine *giostra*.

[82] *http://www.money.it/Concorso-IVASS-per-15-esperti-in*

- *"Le cronache raccontano che migliaia di contatti per partecipare al bando per i tirocini hanno intasato il server. Alle 9,30 di stamattina era già tutto bloccato"*[83]
- *"Complice la fretta dei candidati di bruciare sul tempo i concorrenti (i posti sono limitati, e sugli stessi canali di "Mi formo e lavoro" nei giorni scorsi avevano invitato a una certa celerità), sul portale si sono riversati fin dalle prime ore di martedì mattina centinaia di persone interessate, intasando una piattaforma che, probabilmente, non aveva mai fatto registrare prima un traffico web così denso. La situazione è migliorata dopo poche ore"*[84]
- *"Gli aspiranti candidati al concorso per insegnanti e chi ambisce alle supplenze Ata affollano la piattaforma delle Istanze Online. Che quindi si inceppa. Non è la prima volta. Il MIUR ammette i rallentamenti ..."*[85]

Attualmente il problema è molto mitigato dall'esistenza delle *server farm*: edifici in cui vengono installati migliaia di computer che possono essere allocati alla bisogna (anche per pochissimo tempo) per l'espletamento di una funzione. **Se il servizio è progettato in maniera *scalabile* (appunto)** esso allocherà risorse di calcolo man mano che aumenteranno le richieste momentanee per poi liberarle al termine del periodo di picco. In questo modo è come avere un computer la cui potenza (CPU, RAM, disco ecc.) varia in base al carico di lavoro. Nonostante questi accorgimenti

[83] *http://palermo.meridionews.it/articolo/27511/piano-giovani-grande-successo-del-concorso-per-i-gringo-del-mouse-ideato-da-nelli*

[84] *http://www.bisceglieviva.it/notizie/sistema-puglia-intasato-per-alcune-ore*

[85] *http://www.corriere.it/scuola/medie/18_marzo_15/miur-si-blocca-sito-istanze-troppi-accessi-il-concorso-4de7926c-2846-11e8-86ee-403ce21a628a.shtml*

è ancora oggi possibile sperimentare il cosiddetto *slashdot effect*[86].

1.1.7 Sicurezza

Riteniamo doveroso accennare all'aspetto della sicurezza nei servizi, intesa per ora solo come protezione dalle azioni di terzi malintenzionati[87]. Il tema è enorme[88] e non pretendiamo di esaurirlo qui, ci limitiamo a segnalare che nella progettazione di un servizio digitale bisogna preoccuparsi di gestire eventuali tentativi di accesso indesiderato al servizio stesso o ai dati che tratta.

Quindi ad esempio vanno usati canali sicuri per le comunicazioni:

- via web, specie in caso di accessi autenticati, va usato sempre un protocollo crittografato come `https` invece di `http` (per fortuna sempre meno siti web utilizzano quest'ultimo, in chiaro) in modo da evitare la pratica dello *sniffing* 🕮
- via email, andrebbero[89] scambiati messaggi rigorosamente crittografati[90], specie quando contengono informazioni *sensibili*

I dati immagazzinati per l'espletamento del servizio devono essere trattati secondo normativa europea GDPR (*General Data Protection Regulation*)[91] recepita dall'Italia con il Decreto legislativo 10 agosto 2018 n. 101[92].

[86] *http://en.wikipedia.org/wiki/Slashdot_effect*

[87] A breve tratteremo anche l'etica dei fornitori.

[88] Esistono interi corsi universitari dedicati alla sicurezza dei sistemi e delle reti.

[89] Condizionale d'obbligo dato che purtroppo la percentuale di utenti della rete che utilizza sistemi di posta elettronica sicura è veramente bassa.

[90] *http://gnupg.org*

[91] *http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679*

[92] *http://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg*

La regolamentazione degli accessi mediante autenticazione dovrebbe seguire le buone pratiche stabilizzate nel tempo, la già citata 2FA è una soluzione ragionevole[93].

Non è decisamente una buona pratica utilizzare il principio della *security through obscurity*[94] (sicurezza mediante occultamento di informazioni) che ci è capitato di osservare qualche tempo fa analizzando il sistema di comunicazione dello stato di occupazione dei parcheggi in un Comune della Lombardia. L'architettura del servizio che abbiamo analizzato prevedeva che ciascun parcheggio inviasse le informazioni sullo stato di occupazione dei posti auto al sito del Comune che si occupava di visualizzare la situazione globale su una pagina del proprio sito web e su appositi indicatori distribuiti in città. Purtroppo il protocollo usato era molto semplice e totalmente privo di protezione dagli accessi indesiderati: bastava conoscere il formato del pacchetto - documentato in un manuale consegnato a tutti i parcheggi della città - da inviare al sito del Comune per riuscire ad aggiornare i dati di occupazione dei parcheggi, senza necessità di alcuna autenticazione da parte del software del parcheggio. Risulta chiaro che chiunque si impossessi del manuale sopra citato[95] potrebbe generare molto caos inviando informazioni non corrette, potenzialmente causando ingorghi.

1.1.8 Accessibilità

Ogni servizio digitale dovrebbe essere il più **inclusivo**[96] possibile. Quando ci si preoccupa di **non** escludere utenti con abilità fisiche limitate, quali ad esempio i non udenti, ipovedenti o non vedenti, si parla di *accessibilità*.

[93] Quando non viene implementata in maniera *ottusa*, ad esempio vincolando all'uso di *app* proprietarie.

[94] *http://www.schneier.com/essays/archives/2004/10/the_non-security_of.html*

[95] O riesca a fare reverse engineering intercettando il traffico di rete.

[96] Apertura su protocolli e formati, nessun vincolo sull'hardware e sul software per accedervi.

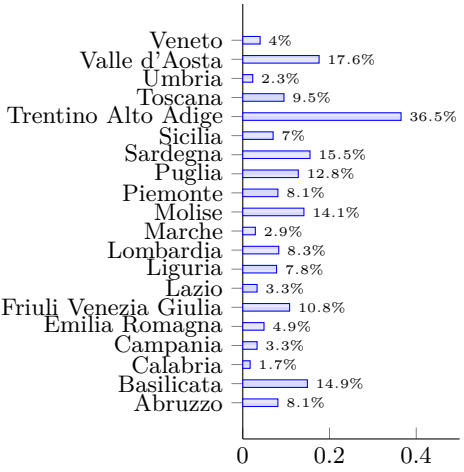


Figura 1.4: Comuni italiani *accessibili*, per regione, situazione al 2014

Il tema accessibilità deriva direttamente, potremmo dire che ne è una *specializzazione*, dal più generico tema della HCI (*Human Computer Interaction*) [Nie00; Nor13], ovvero dell'usabilità degli oggetti, dei meccanismi, del software e dei siti web. Nel progettare l'interfaccia utente di un servizio - sia essa web, desktop o mobile - bisogna fare molta attenzione ai colori, ai *font*, alle dimensioni e comprensibilità delle icone, al tipo di animazioni ecc. Esistono per fortuna alcune normative in merito, la nota direttiva Stanca[97] ha iniziato un filone normativo che poi è giunto fino alle linee guida attuali[98] per la realizzazione dei siti web della P.A. *accessibili* (ad es. ai diversamente abili), che fino al 2014 lo erano ancora poco. Presso il nostro Dipartimento di Informatica implementammo [TS18] uno strumento di analisi automatica per valutare il grado di adeguamento dei comuni italiani: la maggioranza di essi risultò inadempiente (figura 1.4).

[97] *http://www.camera.it/parlam/leggi/04004l.htm*

[98] *http://design-italia.readthedocs.io/it/stable* e *http://developers.italia.it*

Figura 1.5: Un sito web... a orario?

1.2 Etica dei servizi

Finora abbiamo trattato aspetti tecnico-implementativi, ma dobbiamo ancora entrare nel merito di un servizio digitale e di come **dovrebbe comportarsi** nei confronti dell'utente. Dal comportamento più spicciolo come le tempistiche in cui è disponibile (cfr. figura 1.5: un sito web con un orario d'apertura?) fino al trattamento corretto e senza secondi fini, non dichiarati, dei dati personali degli utenti stessi.

Iniziamo col riprendere qualche concetto visto nel capitolo "*Livello 0 [The Net]*" - 0 per declinarlo anche nel contesto dei servizi.

1.2.1 Relatività a livello servizi

Ritroviamo un discreto grado di relatività anche in questo Livello, infatti possiamo affermare quanto segue:

> **I servizi sono relativistici**
>
> Non possono esistere due osservatori che vedono un servizio allo stesso modo.

In questo caso la dimostrazione (e la sperimentazione dell'effetto) è più evanescente e richiede l'utilizzo di qualche strumento software e dell'aiuto di un'altra persona.

Sia chiaro che esiste una quantità fisiologica di relatività che è necessaria e voluta: facciamo l'esempio della

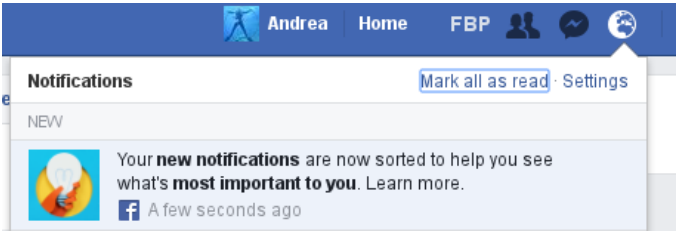


Figura 1.6: Cos'è importante per te... secondo Facebook

richiesta di un certificato anagrafico, è palese che ogni soggetto voglia il proprio[99] e non quello di un altro, idem per una dichiarazione dei redditi o la prenotazione di una stanza in albergo.

Quando facciamo riferimento ai *servizi relativistici* pensiamo a quelli più generalisti come i motori di ricerca, i *social network* o i negozi online di alcuni colossi dell'e-commerce. Sono casi in cui l'informazione a disposizione è quantitativamente difficile da maneggiare per un essere umano, per cui va mostrata attraverso un qualche tipo di filtro, spesso *implicito* e quindi fuori dal controllo dell'utente. In questi casi il filtro mostra ciò che il gestore del servizio ritiene di maggiore interesse per l'utente (cfr. figura 1.6), cioè adatta il filtro al soggetto [Lee17].

L'esperimento che proponiamo passa per Google, ecco le istruzioni:

- bisogna essere almeno in due
- ognuno dotato di un PC o di uno *smartphone* connesso in rete
- tutti i partecipanti devono aprire la pagina iniziale di Google
- tutti i partecipanti devono inserire la stessa frase di ricerca, concordata in precedenza
- alla termine della ricerca ci si confronta sui risultati, quali sono elencati e in che ordine

[99] In questo caso sarebbe addirittura un errore gravissimo fornire lo stesso certificato ad entrambi i soggetti dato che per uno dei due è quello sbagliato.

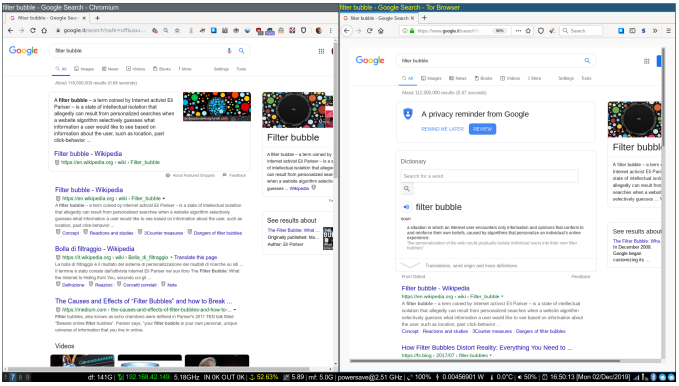


Figura 1.7: Stessa ricerca, diversi risultati (1)

In figura 1.7 vediamo un esempio di ricerca delle parole *filter bubble* usando *Chromium*[100] e *TorBrowser*[101]. Invece in figura 1.8 abbiamo provato con le parole *etica servizi*, sempre attraverso gli stessi due strumenti. Come si può notare i risultati differiscono per contenuto e ordine.

Esperimenti analoghi si possono organizzare sulle piattaforme di acquisti online cercando le stesse parole chiave e confrontandosi sulle liste di prodotti proposti[102]. Fate una prova coi prezzi dei voli[103] cambiando browser o PC... Infatti non giunge sorprendente uno studio[104] che svela un adattamento tariffario molto *relativistico* delle piattaforme tipo Uber, Lyft, ecc. Niente di nuovo sotto il sole, si

[100] Browser di Google, la versione libera.

[101] *http://torproject.org*

[102] Si vocifera che anche i prezzi siano diversi e tarati in funzione dell'acquirente, ma non siamo riusciti a verificarlo. Per certo si sa che Amazon adatta i prezzi dei prodotti anche più volte nell'arco della stessa giornata (*http://www.forbes.com/sites/walterloeb/2014/11/20/amazons-pricing-strategy-makes-life-miserable-for-the-competition*).

[103] *http://millionmilesecrets.com/guides/are-airlines-raising-your-ticket-price-based-on-browser-history*

[104] *http://venturebeat.com/2020/06/12/researchers-find-racial-discrimination-in-dynamic-pricing-algorithms-used-by-uber-lyft-and-others*

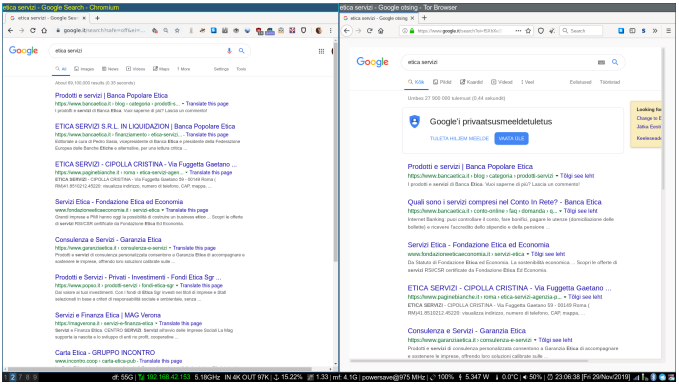


Figura 1.8: Stessa ricerca, diversi risultati (2)

chiama *price discrimination*[105]: una tecnica "antica" che attraverso la tecnologia, che facilita l'introduzione arbitraria di relatività, permette ai venditori di massimizzare il profitto lasciando poche difese agli acquirenti.

Altro esempio è quello offertoci dalle piattaforme di *streaming* internazionali (e.g., Netflix, Prime Video, ecc.) in cui **l'elenco dei media disponibili ai clienti è altamente relativistico**: ogni nazione vede una lista *locale*, cioè adattata al paese da cui proviene la richiesta, al punto che si trovano in rete le spiegazioni sull'uso di strumenti come le *VPN* 🕮 per abbassare l'elevato tasso di relatività[106] ed accedere quindi a liste diverse, più complete.

Se invece focalizziamo il nostro sguardo sul fatto che i *social network* veicolano **pensieri, opinioni e notizie** oltre che pubblicità di prodotti, cosa dovremmo pensare in merito alla relatività?

Ormai quello della *filter bubble* [Lee17] è un concetto noto: motori di ricerca che filtrano grandi quantità di contenuti, non solo merci, per farci vedere solo quelli che ci *interessano*. Il *motore nel cofano* di un *social network*

[105] *http://en.wikipedia.org/wiki/Price_discrimination*

[106] *http://www.howtogeek.com/239616/how-to-watch-netflix-hulu-and-more-through-a-vpn-without-being-blocked*

possiede una *vaga* approssimazione del nostro profilo psicologico personale: siamo noi che gli diciamo cosa *ci piace* con i *like* e le adesioni ai vari gruppi o i *follow* di altri profili, poi un *algoritmo* usa elaborate tecniche per *profilarci* sulla base di quelle *parziali* informazioni. Lo scopo di un *social network* è quello di tenerci il più possibile connessi dato che solo così *consumiamo più pubblicità*, ergo è importante che ci mostri solo informazioni - dal calcio ai *reality*, dalla letteratura antica ai francobolli - che ci invoglino allo *scroll down*, a *scorrere verso il basso* compulsivamente per la voglia di continuare a leggere nel timore di perdere informazioni *fondamentali*. In una spirale *viziosa* ci vengono proposti contenuti ritenuti vicini ai nostri interessi e noi, cliccandoci sopra, rafforziamo la nozione che sono effettivamente interessanti raffinando il profilo che un *social network* ha di noi [GK17; Som14; Man11]. I dati dei profili non sono direttamente a disposizione[107] dei fornitori di contenuti, ma tali fornitori possono impostare una *target audience*, un pubblico tipo, basata su caratteristiche profilabili. Ad esempio è possibile specificare una regione geografica, il sesso o l'età del pubblico a cui si vuol mostrare un contenuto pubblicitario *iniettato* in un *social network*.

Un progetto molto interessante che sta tentando, da qualche anno, il *reverse engineering* 🕮 degli algoritmi di tracciamento e filtraggio è "*Tracking Exposed*"[108].

Sono purtroppo anche molto noti i casi di *pilotaggio politico* via *filter bubble*, cioè il meccanismo con cui alcune organizzazioni hanno comprato dalle varie piattaforme *social* la possibilità di mostrare contenuti *targhettizzati* verso gli elettori, per orientare le opinioni politiche e le successive elezioni, come ad esempio negli USA da Trump[109] e Obama[110], e in UK per il referendum sulla *Brexit*, ben

[107] Salvo scandali come quello di Cambridge Analytica (*http://en.wikipedia.org/wiki/Cambridge_Analytica*).

[108] *http://tracking.exposed/manifesto*

[109] *http://www.wired.com/2016/11/filter-bubble-destroying-democracy*

[110] *http://www.pewresearch.org/internet/2009/04/15/the-internets-role-in-campaign-2008*

raccontato da Carole Cadwalldr in un video al TED[111].

Si ritrova relatività perfino in servizi che riterremmo insospettabili come… le **mappe**, invece proprio Google Maps presenta confini diversi a utenti diversi[112].

A volte è anche utile tenere traccia della variazione cronologica di una *informazione* in Rete, per esempio una pagina web; ovviamente non è banale farlo in proprio, in questo caso ci viene in aiuto "*The Internet Archive*" (cfr. box 1.2.1) che statutariamente si occupa di preservare pagine web *interessanti*, anche su segnalazione degli utenti della Rete.

In sezione "*Relatività*" - 0.2 abbiamo descritto un universo relativistico i cui *osservatori* erano semplici nodi della rete, non necessariamente persone[113]. Qui nel Livello 1 [*services*], purtroppo, stiamo descrivendo gli **effetti relativistici applicati alle persone**, cioè i *soggetti* che *accedono* a un servizio digitale, a volte perfino **autenticandosi**, come ad esempio nel caso dei *social network*.

[111] *http://www.ted.com/talks/carole_cadwalladr_facebook_s_role_in_brexit_and_the_threat_to_democracy?language=en*

[112] *http://www.washingtonpost.com/technology/2020/02/14/google-maps-political-borders*

[113] Ricordiamo che un indirizzo IP corrisponde ad un nodo della rete ma potrebbe essere utilizzato da più persone e una persona potrebbe generare traffico da molteplici indirizzi IP.

TECHBOX: The Internet Archive [1.2.1]

The Internet Archive (*http://archive.org/web*) è un ente non governativo il cui scopo è preservare informazioni che altrimenti andrebbero perse se cancellate dal sito originale. Dato un *URL* 📖 è possibile navigare *indietro nel tempo* andando a consultarne il contenuto ad una data specifica, se presente in archivio.
Purtroppo è abbastanza frequente vedere sparire pagine dal web - a volte perché un sito viene dismesso o ristrutturato, a volte perché ritenute *scomode* - e questo ente cerca, compatibilmente con le risorse disponibili, di fare da *archivista* indipendente, da testimone (viene a volte usato nei tribunali) dell'esistenza di informazioni pubblicate in Rete.

1.2.2 Locard a livello servizi

Con lo stesso criterio usato poco sopra possiamo definire anche a questo livello il:

Principio di Locard *digitale* dei servizi

L'interazione tra un soggetto e un servizio digitale lascia sempre tracce:

- tutt'altro che esigue
- indistruttibili
- spesso **associabili direttamente ad una persona**, invece che semplicemente ad un generico nodo della rete.

In questo caso è facilissimo dimostrare la validità del principio appena enunciato: basti sapere che **ogni** applicativo, sia esso lato *server* (i.e., servizi web), che lato *applicazione* (i.e., *servizi locali*, programmi installati sul proprio PC o *device*), è perfettamente in grado di registrare una traccia di ciò che fa e per chi. L'implementazione più comune del *tener traccia* vive nel meccanismo dei *log file* 🕮, questa funzione di *archiviazione storica* serve *in primis* a scopo di manutenzione: in caso di problemi si può capire cosa ha determinato il malfunzionamento. Ma ovviamente può essere usata anche per sapere cosa fa un particolare utente del servizio in ogni momento della sua interazione: dove clicca, su quali pagine o finestre si sofferma, quali dati compila, in che ordine e in quanto tempo ecc. Si possono perfino tracciare i movimenti del mouse e, in alcuni casi molto specifici, quelli degli occhi, cfr. "*Perception and Effectiveness of Search Advertising on Smartphones*" [DGH16] e "*Eye-Tracking Technologies Are About To Make Advertising Even More Invasive*"[114].

Per rendersi conto della quantità e qualità del tracciamento, se si dispone di account Google e di un device Android è possibile consultare la pagina `http://myactivity`.

[114] `http://www.forbes.com/sites/tarunwadhwa/2013/05/08/with-recent-advances-in-eye-tracking-advertising-set-to-become-even-more-invasive`

google.com, ma anche con un *iPhone* la situazione non è granché differente[115].

L'attenzione che dobbiamo porre noi *cittadini digitali* non è tanto sul *cosa si può o non si può tracciare* (in ogni caso la scelta non è sotto il nostro controllo[116]), ma su che uso viene fatto di questi dati, a quale scopo vengono registrati e per quanto tempo rimarranno a disposizione di chi li ha raccolti: un tema, quello della *data retention* e del GDPR, citato in sezione "*Edmond Locard*" - 0.3.2.

Ci si potrebbe domandare il motivo di tutto questo interesse sulla cattura di dati. Riassumendo con la famosa frase[117] "data is the new oil" (i dati sono il nuovo petrolio), i dati rappresentano la materia prima che rende ricco[118] chi la estrae e la possiede. O anche, citando [Lan17]: "la merce sei tu".

Nel libro "*Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*" [ONe16] l'autrice racconta di come si possa estrarre ricchezza dai dati a spese dei cittadini oggetto della raccolta di informazioni:

- le assicurazioni possono calcolare il vero rischio di eventi negativi e *attualizzare* i premi verso l'alto, annullando il proprio rischio, facendolo quindi ricadere direttamente sull'assicurato, azzerando l'effetto *mutua assistenza*;
- le aziende possono valutare i dipendenti o i candidati per un lavoro in base alla presenza sui *social*;

[115] *http://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears*

[116] Salvo rari casi che tratteremo in sezione "*Software Libero*" - 3.4.1.

[117] *http://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data* (attribuita a Clive Humby)

[118] *Market value* (fonte *http://www.fortune.com/fortune500/2019/search*) delle GAFAM (*http://en.wikipedia.org/wiki/Big_Tech*):

- **G**oogle/Alphabet (816 miliardi di $)
- **A**mazon (874 miliardi di $)
- **F**acebook (475 miliardi di $)
- **A**pple (895 miliardi di $)
- **M**icrosoft (904 miliardi di $)

Si intenda: solo una parte del valore è generato dai dati raccolti.

- gli istituti di credito possono decidere molto *finemente* se concedere e quanto far pagare un prestito, purtroppo con l'introduzione di *disuguaglianze* di genere, censo, razza ecc. poco misurabili se gli algoritmi e i dati di partenza non sono trasparenti;
- i tribunali possono decidere se concedere la libertà su cauzione in base alla probabilità di recidiva calcolata da algoritmi non trasparenti di *crime prediction*;
- i politici possono aumentare le loro *chance* di essere eletti profilando dettagliatamente l'elettorato e preparando quindi programmi *ad hoc*;
- le aziende di commercio online possono stimare la capacità di spesa di ogni utente proponendo quindi prodotti e prezzi *calibrati*[119].

Siamo ormai giunti a quello che Shoshana Zuboff ha definito il *capitalismo della sorveglianza* [Zub19a]:

> *Sur-veil-lance Cap-i-tal-ism, n.*
>
> *1. A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales;*
>
> *2. A parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioral modification;*
>
> *3. A rogue mutation of capitalism marked by concentrations of wealth, knowledge, and power unprecedented in human history;*
>
> *4. The foundational framework of a surveillance economy;*
>
> *5. As significant a threat to human nature in the twenty-first century as industrial capita-*

[119]Sempre verso l'alto, lo scopo di ogni commercio è **giustamente** la massimizzazione del profitto. La calibrazione dei prezzi viene usata normalmente: ad esempio nella grande distribuzione dove lo stesso prodotto viene proposto a prezzi diversi in funzione della posizione del punto vendita. Nel mondo digitale però è molto più facile calcolare istantaneamente il prezzo da proporre ad un singolo utente.

lism was to the natural world in the nineteenth and twentieth;

6. The origin of a new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy;

7. A movement that aims to impose a new collective order based on total certainty;

8. An expropriation of critical human rights that is best understood as a coup from above: an overthrow of the people's sovereignty.

Attenzione che il **capitalismo non è un male**.

Quello *della sorveglianza* però è una degenerazione che conferisce *potere* eccessivo ad un numero limitato di soggetti, aiutato da una architettura di rete debole che non tutela i suoi utenti (cfr. sezione "*Avete rotto Internet*" - 0.5). Quindi ci troviamo di nuovo nella posizione di esortare il cittadino ad una riconquista del controllo sulla Rete che deve tornare al servizio dei suoi utenti: serve consapevolezza e *lobbying* dal basso.

Dopo aver applicato il principio di Locard al mondo digitale, prima a livello di rete e ora dei servizi, non a caso citiamo ora la definizione di *digital footprint*[120]: l'*impronta digitale*[121] che ognuno di noi lascia di sé in rete è l'insieme delle tracce digitali che possono essere raccolte ed esaminate per capire cosa abbiamo fatto, queste tracce si trovano nei vari *log* dei servizi che usiamo. Difficile stimare la dimensione delle nostre impronte, si parla di parecchi gigabyte al giorno.

In sezione "*Il Principio di Locard digitale*" - 0.3 abbiamo descritto un ambiente i cui *soggetti* che lasciano tracce vengono identificati per indirizzo IP. A questo Livello, purtroppo, stiamo descrivendo gli **effetti di Locard digitale applicati alle persone**, cioè i *soggetti* che *accedono* a un

[120] *http://www.Internetsociety.org/tutorials/your-digital-footprint-matters*

[121] Attenzione, stavolta il termine *digitale* non si riferisce al dito! Ma è un ottimo gioco di parole.

servizio digitale, a volte perfino **autenticandosi**, come ad esempio nel caso dei *negozi online*[122].

1.2.3 Orizzonte degli eventi

```
Se un albero cade nella
foresta e non c'è nessuno a
sentire il rumore, di che
colore è l'albero?
```

Parodia della famose frase filosofica sull'osservabilità di un evento, tratta dal gioco "Monkey Island".

La Fisica è affascinante, per questo vogliamo utilizzare un altro concetto interessante come metafora applicabile all'universo digitale. Facciamo qualche breve premessa[123]:

- la *velocità di fuga* è quella necessaria ad un *veicolo*[124] per *sfuggire* definitivamente al campo gravitazionale di un corpo celeste
- la *velocità di fuga* dipende dalla massa del corpo celeste e dalla distanza a cui si trova il veicolo:
  - aumenta al crescere della massa del corpo celeste
  - diminuisce al crescere della distanza dal corpo celeste
- la *velocità della luce* è la massima velocità raggiungibile, circa $300000 km/s$, la nostra Luna dista poco più di un *secondo luce* dalla Terra

Il concetto che vogliamo mutuare qui è quello di **orizzonte degli eventi**. In fisica è il *confine sferico* che si

[122]Se leggendo questa frase avete sperimentato un senso di *deja vu*, non siete in "*The Matrix*": è **quasi** la stessa frase presente in fondo alla sezione "*Relatività a livello servizi*" - 1.2.1… a proposito: pillola blu o pillola rossa?

[123]Il taglio è qui particolarmente divulgativo, ci serve solo per apprezzare il concetto a cui la sezione è dedicata.

[124]In senso ampio: può essere un veicolo vero e proprio, come un razzo o un oggetto sparato da un cannone [Ver19], ma anche un segnale inviato.

crea in corrispondenza della distanza dal corpo celeste all'interno della quale la velocità di fuga supera quella della luce. Se un *veicolo* si trova all'interno di questo confine non avrà alcuna possibilità di raggiungere una velocità di fuga, perché quella della luce è la massima possibile. Più in generale e più pragmaticamente: tutto ciò che si trova dentro il confine rimane dentro, luce compresa; dall'esterno non è possibile osservare o misurare nulla di ciò che accade all'interno dell'orizzonte degli eventi[125].

Tutto ciò che avviene all'interno dell'orizzonte degli eventi *non è accaduto*.

Ogni oggetto crea attorno a sé[126] un orizzonte degli eventi, ma solo quelli di massa enorme espandono il confine a sufficienza per essere apprezzabile, ad esempio tutta la massa della Terra crea un orizzonte del diametro di circa due *centimetri*, quella del Sole circa tre *chilometri*.

Possiamo quindi utilizzare l'orizzonte degli eventi fisico come metafora per definire il nostro:

Orizzonte degli eventi *digitale*

L'*orizzonte degli eventi digitale* è un confine che si crea attorno alla *quantità di privacy* di un soggetto, tutto ciò che avviene all'interno di questo confine non è osservabile *digitalmente* (si dice anche: *non ha eco digitale*) all'esterno[a].

[a] In questo caso ci limitiamo agli eventi *analogici* come lo spostarsi da una stanza all'altra, il parlare con un'altra persona ecc. Abbiamo applicato Locard agli eventi *digitali* come navigare in rete, consultare mail ecc. Nel mondo digitale è molto più difficile crearsi un *orizzonte degli eventi digitale*, negli ambienti della sicurezza informatica si cita sempre la frase: "L'unico vero sistema sicuro è quello spento, gettato in una colata di cemento, sigillato in una stanza rivestita da piombo e protetta da guardie, ma anche in quel caso ho i miei dubbi" (E. Spafford).

[125] Studi recenti aggiungono diverse ipotesi di permeabilità, ma a noi interessa il concetto iniziale per definire poi la nostra versione.

[126] Al suo centro di gravità, considerandone solo la massa.

La *quantità di privacy*[127] di un soggetto purtroppo varia in funzione dell'ambiente in cui ci si trova, ed è misurabile solo indirettamente con la delineazione dell'*orizzonte degli eventi digitale*. Proviamo, per fare qualche esempio, ad analizzare alcuni contesti:

1. un soggetto nella propria abitazione
2. un soggetto per strada in una città
3. un soggetto che cammina nel deserto del Sahara

Nel **primo caso** verrebbe naturale dire che l'*orizzonte degli eventi* coincide con le mura dell'abitazione. Quante volte vado in bagno mentre sono a casa, quanti caffè mi preparo o cosa dico ad altre persone presenti non hanno un *eco digitale*... Sì e no. Non c'è eco digitale se la casa in questione è molto antica (ha un impianto elettrico molto vecchio), non ha un *router WiFi*, non contiene apparecchi connessi a Internet e nessuno dei presenti possiede un telefono cellulare. Infatti man mano che cadono queste condizioni succede che:

- la posizione delle persone all'interno di un appartamento è osservabile tramite il segnale *wifi*[128] o più banalmente dalle telecamere di sorveglianza domestica i cui *stream video* passano per *cloud*[129] esterni alla rete casalinga
- la voce viene captata - e talvolta registrata in *cloud* - dai device presenti, siano essi televisori[130], termostati[131], assistenti domotici[132] e naturalmente telefoni

[127] Abbiamo usato il termine *quantità* invece di *massa*, quella che determina l'orizzonte degli eventi fisico, proprio per esplicitare la natura molto variabile dell'analoga caratteristica che si osserva nel mondo digitale.

[128] *http://hackaday.com/2019/11/28/your-wifi-signals-are-revealing-your-location*

[129] Reti di trasporto che permettono la visione e il controllo della propria casa attraverso *app* per cellulari. Si trovano sovente fuori EU, e.g., Cina.

[130] *http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/index.html*

[131] *http://www.theverge.com/circuitbreaker/2019/2/20/18232960/google-nest-secure-microphone-google-assistant-built-in-security-privacy*

[132] *http://www.bloomberg.com/news/features/2019-12-11/*

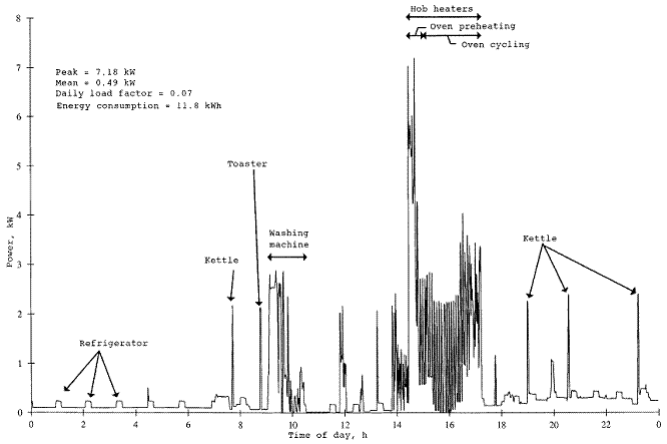


Figura 1.9: Profilazione *elettrica* [Lee10]

cellulari[133]

- l'uso degli elettrodomestici può essere dettagliatamente ricostruito misurando e campionando[134] il consumo istantaneo di corrente dell'appartamento (si veda figura 1.9), dal profilo d'uso si possono evincere la composizione del nucleo familiare e le abitudini dei residenti

Quindi, a meno di un appartamento e di abitanti molto particolari, l'orizzonte si stringe molto, probabilmente al singolo corpo umano… sempre che non si indossi anche qualche *fitness device*[135].

Nel **secondo caso**, del soggetto per strada in una città, ognuno di noi è esposto ad una quantità di *occhi e orecchie* difficile da enumerare:

silicon-valley-got-millions-to-let-siri-and-alexa-listen-in

[133] *http://argomenti.ilsole24ore.com/parolechiave/captatore-informatico.html*

[134] Si può fare da remoto con i nuovi contatori elettronici: inviano al fornitore i dati ogni dieci secondi circa.

[135] Fitbit *et similia*, oggetti che tracciano movimento, battito cardiaco, pressione sanguigna, temperatura ecc. e inviano i dati in rete, *in primis* al produttore dell'apparecchio.

- telecamere di sicurezza visibili pubbliche e private[136], molte delle quali dotate di riconoscimento facciale[137];
- celle telefoniche che triangolano la nostra posizione: si veda il bellissimo lavoro fatto da Malte Spitz che ha chiesto, ottenuto e rappresentato graficamente (figura 1.10) i dati in mano alle compagnie telefoniche (cfr. articolo originale[138] e video al TED[139])
- telecamere più o meno nascoste, come ad esempio quelle presenti in alcuni display pubblicitari[140], Italia compresa[141], o in tutti i bancomat e le colonnine di pagamento ai benzinai self-service.

Nel **terzo caso**, quello di un soggetto che cammina nel deserto del Sahara, se escludiamo il potere visivo dei satelliti di osservazione, forse possiamo affermare che qui l'*orizzonte degli eventi digitale* si allarga a dismisura, ma siamo nel deserto…

In sostanza, si può aumentare la propria *quantità di privacy* eliminando occhi e orecchie digitali dal nostro ambiente, cosa non sempre banale.

Purtroppo siamo persuasi che questo confine si stia restringendo man mano che la tecnologia *fuori controllo*[142] si diffonde. Nella vita di tutti i giorni siamo sempre più

[136] Queste ultime per normativa (*http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/31019*) dovrebbero limitare il campo visivo esterno, normativa purtroppo poco seguita.

[137] *http://www.theguardian.com/technology/facial-recognition*

[138] *http://www.zeit.de/datenschutz/malte-spitz-data-retention*

[139] *http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching*

[140] *http://www.flanderstoday.eu/business/hidden-cameras-be-removed-ad-panels*

[141] *http://www.repubblica.it/economia/diritti-e-consumi/diritti-consumatori/2018/01/30/news/gli_schermi_pubblicitari_in_stazione_ci_osservano_interviene_il_garante-187591395* e *http://www.affaritaliani.it/milano/stazione-centrale-i-totem-pubblicitari-spiano-eta-sesso-dei-passanti-473654.html*

[142] Quando parleremo di Software Libero in "*Software Libero*" - 3.4.1 capiremo cosa intendiamo con *fuori controllo* anziché controllabile e verificabile.

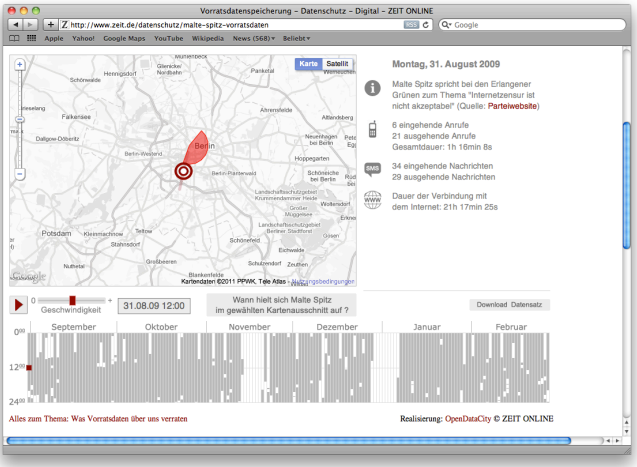


Figura 1.10: Profilazione *geografica* (Malte Spitz)

circondati da così tanti occhi che c'è chi propone abiti e cosmesi mimetici[143] e chi vorrebbe imporre *l'etichettatura dei device*[144], come per i cibi, per obbligare i produttori di hardware e software a dichiarare quali dati, specialmente se audio o video, vengono catturati da un apparecchio e se e dove vengono inviati e immagazzinati.

Quando un evento avviene fuori dall'orizzonte degli eventi digitale, quindi è osservabile, si applica il principio di Locard digitale, ergo l'avvenimento lascia una traccia indelebile: è infatti difficile applicare il cosiddetto *diritto all'oblio*[145], cioè il diritto a far cancellare informazioni pregiudizievoli legate alla persona; un evento *banale* come l'accensione di un elettrodomestico non costituisce informazione pregiudizievole o notizia. Conteremmo invece nell'applicazione del GDPR [GR18; Mar18; But18; Mag18] istituito nel 2016 e che impone regole sulla raccol-

[143] *http://www.theguardian.com/technology/2017/jan/04/anti-surveillance-clothing-facial-recognition-hyperface*
[144] *http://jacquesmattheij.com/et-phone-home*
[145] *http://it.wikipedia.org/wiki/Diritto_all'oblio*

ta, spesso indiscriminata e non dichiarata, e sull'uso dei dati personali.

Il **Cittadino Digitale ideale** che abbiamo in mente è quello che in ogni momento è consapevole del proprio orizzonte degli eventi e capace di ampliarlo o contrarlo secondo quanto desiderato, scegliendo e configurando opportunamente ogni apparato che lo circonda o con cui più in generale interagisce, in modo che sia sotto il proprio controllo.

Capitolo 2

Livello 2 [*access*]

```
Secrecy, censorship,
dishonesty, and blocking of
communication threaten all
the basic needs.
```

Abraham Maslow

Quali dovrebbero essere i *servizi di base* per un cittadino? Una nazione che voglia autoproclamarsi *civile* deve offrire ai suoi cittadini servizi *di base*, *infrastrutturali-analogici* che permettano loro di vivere (proprio fisiologicamente), muoversi, istruirsi, lavorare, socializzare, realizzarsi, ecc. Non deve necessariamente essere lo Stato a fornirli, è sufficiente che il diritto all'accesso sia garantito per tutti i cittadini con pari dignità, cioè senza discriminazioni per censo, luogo di residenza, razza, sesso o religione. Acqua, luce, gas, strade, trasporti, scuole e sanità sono i tradizionali servizi a cui pensiamo quando pensiamo ai servizi di base e sono già regolati in questo modo.

E per il cittadino **digitale**, a quali servizi di base pensiamo nel suo caso? In prima battuta si potrebbe semplicemente rispondere con *accesso alla rete*, inteso come *disponibilità di qualsiasi tipo di connessione a Internet*, ma non è sufficiente. All'inizio della diffusione di Internet, il livello minimo era la disponibilità di una email [And+97], poi divenne l'accesso al web. E non basta nemmeno "un'ora al giorno di WiFi gratuito in alcune zone del centro"[1], abbiamo invece bisogno di reti veloci, in *fibra ottica*, ben distribuite e convenienti per tutti i segmenti della popolazione. Ogni cittadino digitale dovrebbe essere raggiungibile a un indirizzo *di rete*, sia esso un indirizzo di posta elettronica ufficiale, proprio come ogni cittadino ha un indirizzo di residenza fisica, ma ancora meglio sarebbe l'assegnazione di uno spazio *cloud* ufficiale dove archiviare e ricevere ad esempio i documenti della P.A. (Pubblica Amministrazione). Potremmo anche discutere del *diritto all'hardware*:

[1] WiFi gratuito del Comune di Milano nel 2014, qualche anno dopo esteso a *full time* (*http://info.openwifimilano.it*)

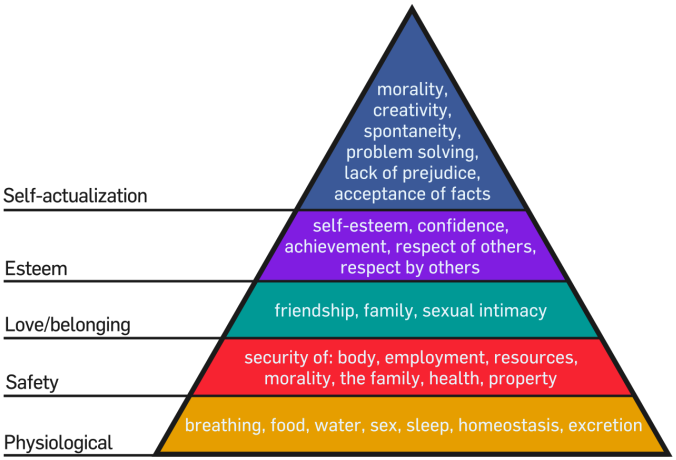


Figura 2.1: La piramide dei bisogni di Maslow (Wikipedia)

dato che per accedere ad un servizio digitale serve un *computing device*, oltre alla connessione, si potrebbe pensare di fornire un computer ad un cittadino in regalo, prestito o comodato d'uso?

Il ragionamento sui servizi essenziali **Livello 2** [***access***] parte da molto lontano nel tempo.

2.1 Bisogni primari dell'uomo

Fu Maslow nel 1943 a proporre la *gerarchia (o piramide, come è stata spesso rappresentata) dei bisogni* [Mas43], della quale in figura 2.1 vi proponiamo una delle sue rappresentazioni: una gerarchia di bisogni umani in cui ogni livello si *appoggia* di fatto sul sottostante, nel senso che se un ipotetico livello N non viene soddisfatto anche i livelli superiori, da N+1 in su, sono del tutto o parzialmente compromessi. Vediamo, partendo dal basso, cioè dal più *impellente* quali sono questi livelli:

1. il livello alla base è quello *fisiologico*: il bisogno di aria, acqua, *cibo*, sonno, etc.; non soddisfare uno di questi bisogni porta alla morte del corpo fisico in tempi brevi, da qualche minuto per la mancanza d'aria a qualche settimana per la mancanza di *cibo*, riprodursi è necessario per la continuità della specie;
2. subito sopra troviamo il livello *sicurezza*: potersi curare, avere un reddito dignitoso, avere dei beni personali[2] e un riparo dalle intemperie;
3. poi troviamo *amore e senso di appartenenza*: amare e essere amati, sentire il calore umano di chi ci circonda, sentirsi voluti, desiderati, sapere che manchiamo a qualcuno che magari attende il nostro ritorno da un lungo viaggio;
4. la *stima*: aver stima di sé, aver sicurezza in sé, essere rispettati e rispettare gli altri, ottenere risultati in ciò che ci soddisfa, essere ascoltati quando esprimiamo pareri;
5. *realizzazione*: poter esprimere la propria creatività e spontaneità, formarsi un'etica, essere liberi da pregiudizi, avere capacità di comprendere la realtà e poter contribuire risolvere i problemi che riscontriamo, poter contribuire all'insieme, alla comunità;

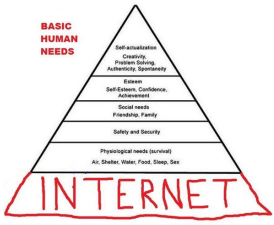
L'implementazione naturale di una piramide completa è quella che parte dal basso e man mano sale fino alla cima. Metaforicamente parlando, come un edificio si costruisce dalle fondamenta, così anche il mondo ideale in cui l'elenco dei bisogni di Maslow è pienamente soddisfatto viene costruito passo passo a partire dalle fondamenta fisiologiche.

Ovviamente esistono casi in cui l'ordine non viene rispettato fedelmente. Sono spesso casi da romanzo o film perché *fanno notizia* o comunque suonano strani o interessanti alle nostre orecchie, esattamente come suonerebbe strana una casa dotata del solo tetto senza mura o delle sole finestre senza porte. Si pensi ad esempio a "*La vi-*

[2]La proprietà privata citata in molte costituzioni, ad es. quella USA [AAV87].

ta è bella" di Benigni, ma anche a molti altri film e libri d'ambientazione in campi di prigionia, in cui l'amore (nel senso più puro del termine) e l'amicizia si compiono anche in contesti di grave privazione fisiologica e di sicurezza [Lev14].

Non si può fare a meno di notare una vicinanza, pur in contesti diversi, fra la piramide di Maslow e i livelli del nostro arcobaleno, in particolare sui livelli alti di entrambi i modelli: Maslow cita l'"Essere ascoltati…" (L6-consultation e L7-democracy) e il "poter contribuire all'insieme, alla comunità…" (L5-participation) che analizzeremo nel secondo volume. Sui livelli bassi, quelli *di sopravvivenza*, per fare una *liaison* basti citare un *meme* 📖 famoso, di fonte ignota purtroppo, riportato qui sotto:



che aggiunge un livello alla piramide di Maslow mettendo il *bisogno di connettività* ancora più in basso dell'aria da respirare!

Molto interessante anche il fatto che nel corso degli anni la stratificazione proposta da Maslow è stata criticata, ad esempio in "*Social Networks: What Maslow Misses*"[3]:

> *I bisogni non sono gerarchici. La vita è più confusa di così. I bisogni sono, come la maggior parte delle altre cose in natura, un sistema interattivo, dinamico, ma è strettamente connesso alla nostra abilità di costruire connessioni sociali.*

[3] *http://www.psychologytoday.com/blog/positively-media/201111/social-networks-what-maslow-misses-0*

Ecco perché l'arcobaleno della Cittadinanza Digitale ha dovuto *piegarsi* ad una applicazione più elastica diventando *spettrografico* (cfr. "Introduzione").

2.2 Cos'è un Servizio Pubblico?

Rubiamo alcune frasi a Wikipedia citando la definizione di *Servizio Pubblico*[4] con qualche grassetto nostro:

> *Un servizio pubblico è un tipo di servizio reso alla collettività, oggettivamente* ***non economico****, ma suscettibile di essere organizzato in forma d'impresa, secondo la disciplina dei vari ordinamenti giuridici. … Il concetto di servizio pubblico è necessariamente connesso ad un riconoscimento giuridico dello stesso: va perciò inteso come servizio tutelabile dall'ordinamento non solo come semplice aspirazione della collettività, ma come* ***bisogno primario*** *da dover necessariamente soddisfare tramite azione legislativa.*

È interessante notare come fin dalla definizione si citino l'aspetto del *bisogno primario* e il lato *economico*. Riferirsi ai bisogni primari ci ricollega a Maslow e ci fa capire come la *ratio* sottostante alla definizione di servizio pubblico sia quella di garantire ad ogni cittadino una piramide dei bisogni *soddisfatti* possibilmente ben costruita. Trattare l'aspetto economico invece ci collega alla nozione che alcuni tipi di servizi sono così onerosi che il loro costo va distribuito sull'intera collettività e non sul singolo che *non deve essere lasciato solo*. Si pensi al tipico caso in cui va garantita l'acqua potabile o la corrente elettrica in un paesino sperduto abitato da poche anime: in tali casi non si può addossare a quei pochi cittadini il costo manutentivo degli impianti che infatti viene ripartito sull'intera regione o nazione.

[4] *http://it.wikipedia.org/wiki/Servizio_pubblico*

Un *servizio* diventa *pubblico* quando viene legislativamente riconosciuto come tale. In Italia sono considerati servizi pubblici, anche se svolti in regime di concessione o mediante convenzione, quelli volti a garantire il godimento dei diritti della persona, costituzionalmente tutelati, alla salute, all'assistenza e previdenza sociale, alla istruzione e alla libertà di comunicazione, alla libertà e alla sicurezza della persona, alla libertà di circolazione e quelli di erogazione di energia elettrica, acqua e gas[5].

Ogni servizio pubblico, secondo la giurisprudenza europea e le autorità di settore, deve essere erogato secondo questi principi[6]:

- *Doverosità*: i pubblici poteri si fanno carico del compito di garantire l'erogazione del servizio;
- *Continuità*: l'erogazione del servizio non può essere arbitrariamente interrotta;
- *Parità di trattamento*: gli utenti hanno tutti pari diritto ad accedere al servizio e ottenere prestazioni di eguale qualità;
- *Universalità*: il servizio va garantito a prescindere dal reddito, dalla localizzazione e dalla fascia sociale (**non discriminazione**);
- *Economicità*: il gestore del servizio deve essere posto in condizione di esercitare l'attività in modo imprenditoriale e conseguire un **margine ragionevole di utile**. Si ricollega indirettamente alla garanzia di usufruire del servizio ad un **prezzo accessibile**;
- *Possibilità di concessione*: è prevista la possibilità di affidare direttamente o indirettamente ad un privato il soddisfacimento del bisogno riconosciuto dall'ente.

Per quanto riguarda gli aspetti economici ci sono casi di servizi così onerosi da obbligare ad una gestione *in perdita*; per questi, definiti *senza rilevanza economica*, è lo Stato a farsene carico. In questi casi si parla di *Servizio Universale*[7], solitamente nei contesti delle comunicazioni,

[5] *http://www.handylex.org/stato/d270194.shtml*
[6] *http://it.wikipedia.org/wiki/Servizio_pubblico*
[7] *http://it.wikipedia.org/wiki/Servizio_universale*

telecomunicazioni, trasporti, energia elettrica e gas.

Indipendentemente da chi sia il fornitore è ovviamente necessario stabilire delle norme che specifichino il livello di *qualità* dei servizi per i cittadini in modo da rispettare i vincoli di cui sopra. Inoltre dovrebbero essere garantiti al cittadino due *meta-diritti* per nulla scontati e non banali da ottenere nel contesto digitale:

- il diritto di misurazione del livello di servizio
- il diritto di contestazione

L'insieme dei principi visti sopra e questi ultimi due meta-diritti dovrebbero prendere concretezza nei cosiddetti SLA (*Service Level Agreement*), i contratti di servizio che ogni utente firma a volte implicitamente o distrattamente, in cui vengono specificati i livelli di servizio, regolamentate le procedure (tempi e modi) per segnalare difformità e le penali per le mancanze.

Ultima considerazione importante: includere un servizio digitale tra quelli definiti *pubblici* significa anche **standardizzarlo** *de iure*, quindi potenzialmente ridurne sensibilmente, se non azzerare, il livello di *lock-in* e favorendo la concorrenza fra possibili concessionari.

2.3 Le infrastrutture non digitali

Prima di affrontare l'analisi dei servizi digitali infrastrutturali concediamoci una breve parentesi elencando e descrivendo alcune infrastrutture non digitali per *allenarci mentalmente* a ragionare in termini di oggetti in gioco, comportamenti, procedure, SLA, scopo, unità e strumenti di misura[8]. Per gli SLA elenchiamo i fattori principali di qualità e solo ove a conoscenza i valori effettivi.

[8]Importante citare gli strumenti di misura perché abbiamo visto (nei capitoli "*Livello 0 [The Net]*" - 0 e "*Livello 1 [services]*" - 1) e vedremo (poco più avanti) che per quelli digitali non sarà sempre facile averne, né saranno affidabili quando li avremo.

2.3.1 Rete elettrica

Veicola corrente elettrica che permette l'effettuazione di lavoro, in senso fisico. I fornitori di corrente si appoggiano ad una rete fisica di distribuzione che attraverso varie trasformazioni, da alta a bassa tensione, portano al contatore di case, uffici e aziende una certa potenza che può essere utilizzata tramite *device* (ad es., elettrodomestici) che trasformano la potenza elettrica in lavoro: fanno girare motori o pompe, accendono lampade, scaldano, ecc.

Le unità di misura principali sono: *Volt*, tensione, misura la forza disponibile; *Ampere*, corrente, misura il flusso di corrente in un conduttore; *Watt*, potenza, misura quanto lavoro si può effettuare nell'unità di tempo; *Wattora*, potenza consumata o lavoro effettuato su un periodo; *Hertz*, frequenza della corrente alternata (la forma d'onda si presume implicita, tipicamente sinusoidale).

Gli strumenti di misura sono prettamente tecnici (voltmetri, wattmetri, ecc.) tranne uno, il *contatore di casa*, strumento che permette all'utente di verificare il proprio consumo istantaneo (Watt) o periodico (Wattora), anche per giudicare grossolanamente il servizio offerto. Il contatore digitale attuale invia i dati di consumo al fornitore tramite *onde convogliate*[9] evitando le procedure di lettura fisica casa per casa.

Gli oggetti in gioco si chiamano *prese*, *spine*, *interruttori*, *contatori*, *apparecchi elettrodomestici*, *cavi*, *scatole di derivazione* e tutto ciò che compone un impianto elettrico e che ad esso può essere connesso.

La procedura per ottenere il servizio è relativamente semplice, anche se non sempre veloce: bisogna rivolgersi ad un fornitore e, fornendo i propri dati, si può chiedere il cosiddetto *allacciamento*. Se l'impianto fisico è già presente fino al contatore dell'utenza, come nel caso di un *subentro*, l'operazione viene effettuata potenzialmente sen-

[9] Meccanismo per inviare segnali informativi usando lo stesso cavo che porta la corrente elettrica all'utente.

za richiedere l'uscita di un *tecnico* perché i nuovi contatori digitali vengono controllati da remoto dalla centrale[10].

SLA: frequenza dell'onda di 50Hz ± 10%, tensione di 220V ± 10%, potenza istantanea espressa in kW erogata in funzione del contratto sottoscritto.

2.3.2 Rete gas

Veicola gas combustibili di vario genere - ad esempio metano o GPL, a seconda dei paesi o delle regioni - che vengono usati per cucinare, scaldare acqua sanitaria o per riscaldamento. In tempi relativamente recenti in Italia è diventato possibile servirsi di fornitori diversi che si appoggiano su una rete fisica di distribuzione gestita da terzi, in modo analogo a quanto avviene per la rete elettrica.

Le unità di misura principali sono: *Metro cubo*, serve a misurare il volume di gas consumato; *Bar* (millesimi), pressione del gas nei tubi.

Gli strumenti di misura tecnici sono ad esempio manometri e flussometri, mentre quello a portata di utente è il *contatore del gas*, una volta puramente meccanico e in Italia in via di sostituzione con strumenti digitali, misura i metri cubi consumati; non fornisce alcuna informazione sulla pressione di fornitura. In era pre-digitale un *letturista* doveva passare periodicamente di casa in casa a prendere le misure indicate sui contatori per dare modo al fornitore di verificare che le stime di consumo calcolate e le autoletture comunicate dagli utenti corrispondessero a quanto effettivamente consumato.

Gli oggetti in gioco si chiamano *rubinetti*, *tubi*, *ugelli* (della cucina a gas, vanno tarati in funzione del tipo di gas usato), *scaldabagni*, *caldaie*, *scarichi*, *comignoli*, *prese d'aria* (obbligatorie nella stanza dove c'è una caldaia) ecc..

La procedura di attivazione è analoga a quella per la rete elettrica.

[10] *Anticamente* i contatori elettromeccanici venivano *piombati* (letteralmente, con un filo metallico chiuso da un sigillo in piombo) per impedirne l'utilizzo senza un'utenza attiva (i.e., pagante).

SLA: pressione minima ($\approx$ 20 mbar), composizione del gas.

2.3.3 Rete idrica

Veicola acqua che viene usata sia per scopi domestici che industriali o agricoli.

Le unità di misura principali sono: *Litro* e *metro cubo*, esprime il volume consumato; *Litro/s* e *metrocubo/s*, volume d'acqua trasportato al secondo, esprime il volume disponibile nel tempo, la cosiddetta *portata*; vari altri fattori di *qualità* come durezza, purezza, residui ecc.

L'unico strumento che conosciamo come semplici utenti è, anche in questo caso, il *contatore dell'acqua*, applicato all'ingresso dell'impianto domestico, misura i metri cubi d'acqua transitati. Attualmente è di tipo meccanico e viene letto da operatori o in auto-lettura (l'utente comunica a lettura per telefono o via web).

Gli oggetti in gioco si chiamano *rubinetti*, *tubi*, *scaldabagni/caldaie*, *braghe*, *lavandini*, *vasche/docce*, *water/bidè* ecc.

La procedura di attivazione è analoga a quella per la rete elettrica.

SLA: flusso minimo, purezza.

2.3.4 Rete telefonica tradizionale

Veicola voce (audio a bassa qualità) che viene usata per comunicare, appunto, *a voce* o ricevere e trasmettere dati via computer o via fax, anche se queste ultime opzioni sono ormai in disuso.

Le unità di misura principali sono: (una volta) lo *scatto*; i secondi o i minuti di conversazione.

Lo strumento di misura attuale lato utente è solo la fattura, dato che il *conta scatti* è un oggetto ormai desueto; volendo si può includere l'orecchio umano, che ci dice se *c'è linea*, se il chiamato è occupato ecc. interpretando i segnali sonori corrispondenti a ciascuna situazione.

Gli oggetti in gioco: *telefono*, *cornetta*, *modem*, *apparecchio fax*, *doppino*, *armadio* (in centrale e in strada), *cabina telefonica* (sempre meno, cfr. box 2.5.3), *gettone* (molto, ma molto, tempo fa).

La procedura di attivazione è analoga a quella per la rete elettrica.

SLA: qualità della voce, vale a dire capacità di trasmettere audio fino a 4kHz.

2.3.5 Altre infrastrutture pubbliche

Si lascia al *divertimento* del lettore la descrizione di altre reti infrastrutturali fisiche e analogiche quali ad esempio: la rete fognaria, quella stradale, il sistema del trasporto pubblico, il servizio postale, il sistema della gestione dei rifiuti ecc.

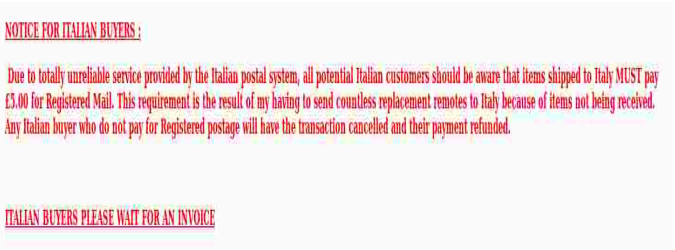
La ratio di questa sezione è ribadire che ognuna di queste infrastrutture **pubbliche** è definita[11] in termini di comportamenti, procedure, SLA, scopo, unità e strumenti di misura e per ognuna vengono stabilite dallo Stato norme che ne regolano l'**accesso** e i termini per la loro **fornitura**, quindi anche per la loro eventuale *commercializzazione*.

2.4 Accesso ai servizi digitali

Nel capitolo "*Livello 1 [services]*" - 1 abbiamo visto gli aspetti tecnico-implementativi dei servizi digitali, in questa sede invece descriveremo quelli relativi all'*accesso*, nel senso del *diritto per un cittadino di avere accesso ad un particolare servizio digitale* senza essere discriminato, a costi accessibili e con una qualità accettabile.

Sarà anche interessante notare come le qualità di un servizio possano influenzare quelle di un altro servizio, come tempi e costi. L'esempio per antonomasia che usiamo spesso, perché di facilissima comprensione ad un pubblico non tecnico, è il caso mostrato nello *screenshot* sottostante:

[11] Sebbene per alcune non sia affatto semplice, come per esempio per il sistema sanitario.


NOTICE FOR ITALIAN BUYERS :

Due to totally unreliable service provided by the Italian postal system, all potential Italian customers should be aware that items shipped to Italy MUST pay £3.00 for Registered Mail. This requirement is the result of my having to send countless replacement remotes to Italy because of items not being received. Any Italian buyer who do not pay for Registered postage will have the transaction cancelled and their payment refunded.

ITALIAN BUYERS PLEASE WAIT FOR AN INVOICE

Un avviso su Ebay **per i soli compratori italiani** che recita (tradotto liberamente): "Nota per i compratori italiani, a causa della totale inaffidabilità del sistema postale italiano, tutti i potenziali compratori italiani dovranno pagare un supplemento per la posta raccomandata di 5 sterline. Questo requisito è il risultato del fatto di aver dovuto gestire in passato innumerevoli richieste di rimpiazzo di prodotti non ricevuti. Ai compratori italiani che non pagheranno il supplemento verrà annullata la transazione e restituito il pagamento.". In questo caso si tratta di (percepita?) inefficienza del servizio *analogico* di consegna delle spedizioni, ma rende bene l'idea dell'**interconnessione** tra diversi livelli infrastrutturali.

Tornando al mondo digitale, dobbiamo esaminare due macro-temi:

- il *digital divide* tecnologico[12], cioè il grado di capillarità dell'infrastruttura di rete che poi deve veicolare i servizi;
- la *net neutrality*, cioè il grado di relatività della rete (cfr. sezioni "*Relatività*" - 0.2 e "*Relatività a livello servizi*" - 1.2.1) che dovrebbe essere il più basso possibile, auspicabilmente esplicitato contrattualmente e misurabile.

[12]Ne esiste anche uno *non tecnologico, cognitivo, sociale, culturale* che esamineremo nel capitolo "*Livello 3 [education]*" - 3.

2.4.1 Digital divide

```
Se io scarico a 100Mbit/s e
tu a 2Mbit/s, in media stiamo
scaricando a 51Mbit/s
(ma tu il film non lo vedi)
```

Il pollo di Trilussa digitale

Il *digital divide*, che in italiano diventa *divario digitale*, misura le disuguaglianze nella disponibilità di accesso alle tecnologie digitali da parte della popolazione. Il fattore tecnico che viene solitamente misurato è quello del livello di connettività infrastrutturale su base territoriale o demografica.

Riteniamo importante lo sforzo di riduzione del *digital divide* **perché non esistano cittadini digitali di serie A e di serie B**, perché tutti possano accedere alla Rete con *potenza* sufficiente per usufruire di - o *erogare* - tutti i servizi *network based*, anche quelli a più alto impatto tecnico come le comunicazioni video e lo *streaming*. I cittadini esclusi dalla connettività sono cittadini svantaggiati.

Normativamente vengono definite due fasce di *digital divide*:

- di primo livello = indisponibilità banda oltre 2 Mbps
- di secondo livello = indisponibilità banda oltre 30 Mbps

L'unità di misura è il *bit/s* 🕮. Un soggetto che disponga di una connessione oltre i 30Mbps si dice *non affetto* da *digital divide*. Quindi la situazione desiderata è una popolazione poco o nulla affetta da *digital divide*: una nazione **sana**.

Tecnicamente vengono inoltre definite e misurate due ulteriori fasce: sopra il secondo livello (velocità in download di almeno 30Mbps) si parla di *banda ultra-larga* NGA (*Next Generation Access*) e quando si arriva a velocità molto superiori ai 100Mbps (tipicamente 1Gbit/s) si parla invece di NGA-VHCN (*Next Generation Access - Very High Capacity Networks*), queste ultime sono di solito implementate con fibra ottica fino in casa.

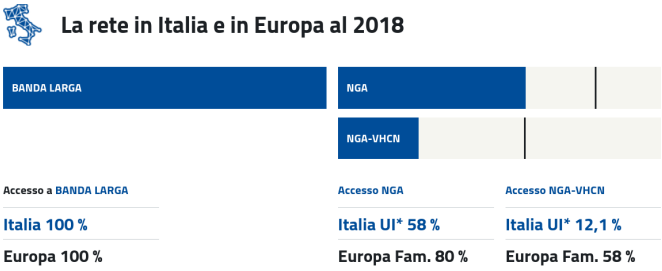


Figura 2.2: Digital divide secondo Infratel (2018)

Per un primo sguardo sulla situazione italiana si può consultare il sito di Infratel[13] (Piano Banda Larga/Ultralarga Italia), di cui mostriamo uno *screenshot* in figura 2.2. Si vede la situazione al 2018 in cui rispetto alla media EU eravamo indietro: 58% contro 80% per l'NGA e un risicato 12% contro 58% per l'NGA-VHCN.

Anche AGCOM[14] tiene sotto controllo lo stato della connettività pubblicando sia rapporti periodici che una bella mappa interattiva[15] di cui proponiamo uno *screenshot* in figura 2.3, mostra la densità delle province raggiunte da connettività superiore a 30Mbit/s (i.e., *non affette da digital divide*) attraverso colori[16]:

- verde scuro = 65%-100%
- verde chiaro = 50%-65%
- arancio = 35%-50%
- rosso = 0%–35%

La Comunità Europea produce ogni anno un rapporto, il DESI[17], che fotografa lo stato della penetrazione di Inter-

[13] `http://www.infratelitalia.it`
[14] `http://www.agcom.it`
[15] `http://maps.agcom.it`
[16] Per la stampa in B/N descriviamo la situazione: rosso in centro Italia nell'interno; arancio ancora in centro Italia, Sardegna e zone montane del nord Italia; verde scuro sud Italia, Emilia Romagna, parte di Lombardia e Veneto; verde nel resto
[17] `http://ec.europa.eu/digital-single-market/desi`

Figura 2.3: Copertura broadband al 29/10/2019 (*screenshot* da AGCOM)

net in Europa, sia dal punto di vista tecnico-infrastrutturale che sociale misurando alcuni indicatori:

- connettività[18]
- capitale umano e abilità digitali[19]
- uso dei servizi Internet da parte dei cittadini[20]
- integrazione di tecnologie digitali nelle aziende[21]
- servizi pubblici digitali[22]
- ricerca e sviluppo in ICT (*Information and Communication Technologies*)[23]

Sfogliando il rapporto 2019[24] sulla connettività si può notare subito come i paesi del nord Europa si posizionino

[18] *http://ec.europa.eu/digital-single-market/en/connectivity*

[19] *http://ec.europa.eu/digital-single-market/en/human-capital*

[20] *http://ec.europa.eu/digital-single-market/en/use-internet*

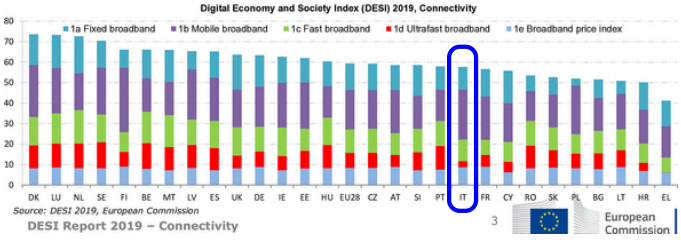
[21] *http://ec.europa.eu/digital-single-market/en/integration-digital-technology*

[22] *http://ec.europa.eu/digital-single-market/en/digital-public-services-scoreboard*

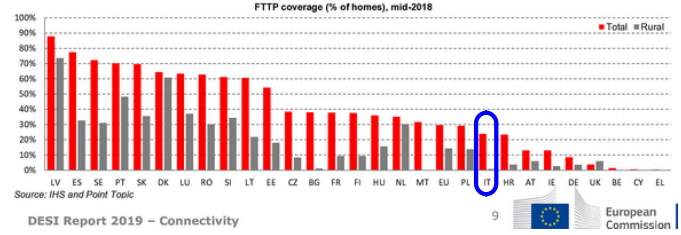
[23] *http://ec.europa.eu/digital-single-market/en/research-development-scoreboard*

[24] *http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60010*

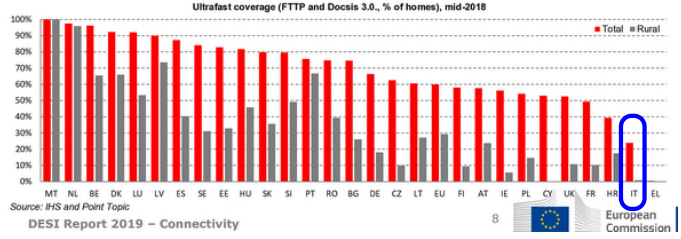
sempre in cima alle classifiche delle varie sotto-categorie mentre purtroppo l'Italia si trovi quasi sempre in coda, ci "salva" solo la telefonia mobile per penetrazione di mercato e bassi costi per gli utenti. Vediamo innanzitutto il nostro posizionamento globale, siamo a 2/3 della classifica:



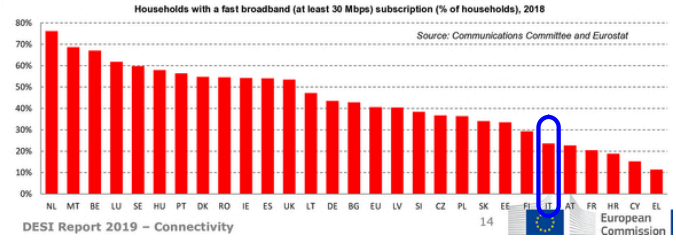
Per quanto riguarda la fibra FTTP (*Fiber To The Premises*), cioè fino *in casa*, ci classifichiamo molto in fondo specie per quanto riguarda le aree rurali:



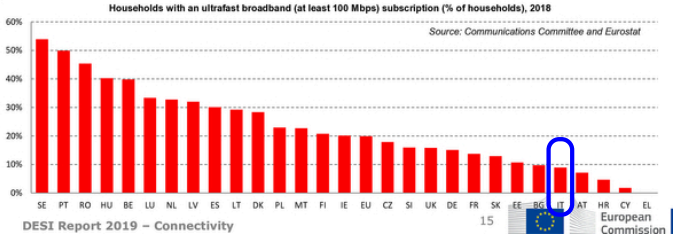
E ancora peggio se guardiamo all'*ultra-fast* (giga bit):



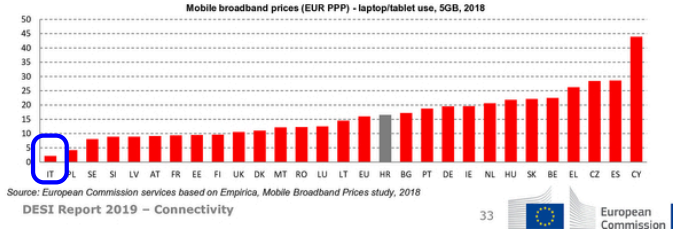
Ancora nel 2019 più del 70% delle utenze è affetto da *digital divide* di secondo livello (ricordiamo: sotto i 30Mbit/s, ma sopra i 2Mbit/s), infatti solo il 25% ha una connessione veloce, siamo sestultimi in EU:



E peggio facciamo, ovviamente, se tagliamo a 100Mbit/s la misurazione, diventiamo quintultimi:



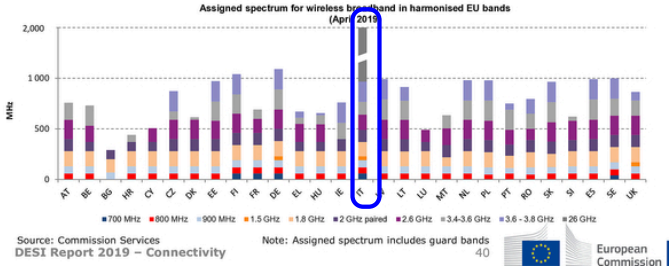
Ma *curiosamente* siamo i meno cari sui *data plan* (piani dati a *forfait*) per cellulari:



L'enfasi sul *curiosamente* è dovuta al fatto che è ormai noto come l'Italia sia un paese *strano*: siamo in cima (terzi) alla classifica del numero di cellulari per abitante[25] pur rimanendo in coda alle classifiche sull'accesso alla Rete. Infatti, sempre il DESI ci mostra come il contesto del 5G (telefonia cellulare di ultima generazione) ci alzi la media, ad esempio dal punto di vista dell'assegnazione delle

[25] *http://www.wired.it/internet/web/2018/01/30/digital-2018-dati*

frequenze, forse dovuta alla fretta di monetizzare a scapito di una visione più strategica.



A **livello mondiale** si può consultare lo studio condotto da M-Lab[26] da cui si evince che l'Europa si posiziona molto bene: tutte le nazioni sono nella prima metà della classifica. Nel 2019 i primi quattro posti sono stati assegnati a Taiwan (primo), Singapore, Jersey (protettorato britannico) e Svezia mentre **l'Italia è al 48° posto su 208 nazioni**; le ultime quattro posizioni sono invece occupate da Mauritania, Guinea Equatoriale, Repubblica Democratica di Timor-Est e Yemen (ultimo).

Saltando al **contesto aziendale**, un rapporto ISTAT[27] del 2019 rileva che il numero di imprese italiane sopra i 10 addetti con connessioni Internet veloci sale:

- **sopra i 30Mbit/s** dal 13% del 2015 al 41%
- **sopra i 100Mbit/s** dal 6,2% del 2015 al 13,8%

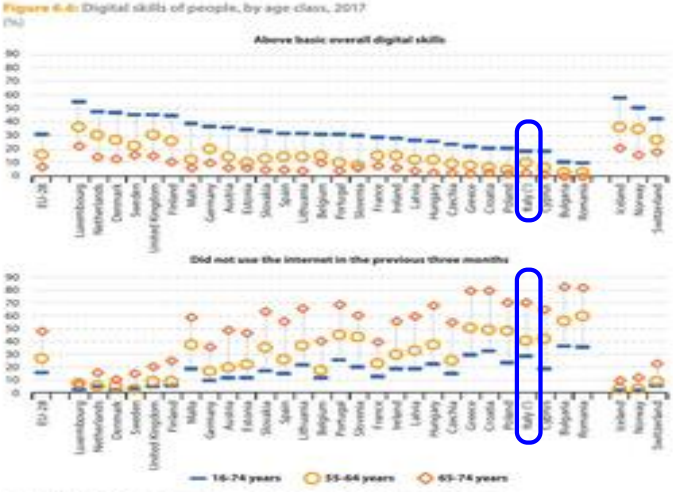
Infine c'è un particolare tipo di *digital divide* non propriamente tecnologico, è quello **cognitivo e culturale** cioè il divario digitale di chi, per *scelta* (non sempre ragionata o conscia, ma spesso per semplice mancanza di conoscenza), non si avvale di connettività e di servizi digitali.

Nel rapporto "Ageing Europe" [SW19], di cui riportiamo qualche grafico qui di seguito, si legge che l'Italia è di

[26] *http://www.cable.co.uk/broadband/speed/worldwide-speed-league*
[27] *http://www.istat.it/it/archivio/236526*

nuovo in coda alle classifiche per utilizzazione dei servizi di *shopping online* per fascia d'età:

Può essere dovuto a nostri deficit? Vediamo: sempre per fascia d'età abbiamo una grossa fetta della popolazione che, in mancanza di abilità digitali, non utilizza Internet o lo fa molto raramente, non solo per acquisti online ma in generale:



2.4.2 *Net Neutrality*

Dopo il *digital divide* il secondo aspetto da considerare è il seguente: una volta ottenuta la connettività *grezza* ad una velocità *teorica* adeguata, non è che poi un alto tasso di *relatività* (cfr. sezioni "*Relatività*" - 0.2 e "*Relatività a livello servizi*" - 1.2.1) mi impedisce comunque di sfruttare tutti i servizi che vorrei?

Come possiamo difenderci e calmierare, se non azzerare completamente, gli effetti relativistici della Rete?

La soluzione più ovvia quanto **impraticabile** sarebbe quella di *tirare*[28] i nostri cavi e connetterli con i nostri *router*, col risultato che la rete risulterebbe pienamente sotto il nostro controllo. Questa soluzione è applicabile solo in contesti molto locali: un singolo edificio da cablare o due edifici a portata di ponte radio. Per collegamenti a grande distanza bisogna affidarsi a *operatori all'ingrosso*, che ammortizzano gli investimenti di cablaggi importanti, sottoterra o transoceanici[29], rivendendo la connettività agli utenti finali attraverso una rete di *ISP* 🕮.

Le domande a questo punto diventano due:

1. Come (se si può) misurare il grado di Relatività della Rete?
2. Come (se si può) modificarlo?

Alcune risposte tecnologiche, purtroppo parziali, sono state citate in sezione "*Provare a difendersi*" - 0.5.2: esistono strumenti di misurazione[30] e soprattutto delle *community* che si sono organizzate per misurare reciprocamente le prestazioni e cercare di *stanare* le sacche di Relatività *artificiosa* nelle varie sotto-reti che compongono Internet.

In questa sezione invece ci interessa presentare la risposta **politica** alla Relatività, la richiesta di un **principio di non discriminazione**: il movimento per la **Net Neutrality** (Neutralità della Rete).

[28] Gergo per *stendere*, *impiantare*.

[29] Questi ultimi si contano, a livello mondiale, sulle dita di poche mani [Eud16].

[30] Più sofisticati di `'ping'` e `'traceroute'` già citati.

Il termine *Net Neutrality* fu coniato da Tim Wu nel 2003 [Man17; Wu03] e molto semplicemente afferma che "qualunque traffico di rete dovrebbe essere trattato in maniera equa", cioè, per riprendere l'epigrafe della sezione "*Mini-esegesi di TCP/IP*" - 0.1.1: "tutti i pacchetti dovrebbero essere uguali" (senza "ma …").

Naturalmente è più facile a dirsi che a farsi, ma attorno al concetto di Net Neutrality si è catalizzato un movimento politico che chiede a gran voce la promulgazione di normative che impongano agli *ISP* 🕮 il rispetto di questi principi [Bil14; Kan14; Eud11a; All+17].

Nel corso degli anni il movimento si è parecchio ampliato[31] fino a contare tra le sue fila perfino alcune grandi aziende, ecco alcuni nomi significativi [Fin17]:

- Vinton Cerf, co-inventore del TCP/IP (cfr. sezione "*Mini-esegesi di TCP/IP*" - 0.1.1)
- Tim Berners-Lee, creatore del World Wide Web
- John Oliver, il famoso (negli USA) presentatore di "*Last Week Tonight*"
- la ACLU (*American Civil Liberties Union*)
- la EFF (*Electronic Frontier Foundation*)[32]
- Greenpeace[33]
- il noto sito di *crowdfunding* 🕮 Kickstarter[34]
- la piattaforma di condivisione video (alternativa a Youtube) Vimeo[35]
- la Mozilla Foundation, nota soprattutto per l'usatissimo *browser* Firefox[36]
- il senatore Bernie Sanders
- la Internet Association[37], associazione mondiale di *imprese Internet* comprendente Amazon, Facebook e Google

[31] *http://www.thebalancesmb.com/the-case-for-net-neutrality-2531681*
[32] *http://eff.org*
[33] *http://greenpeace.org*
[34] *http://kickstarter.com*
[35] *http://vimeo.com*
[36] *http://mozilla.org*
[37] *http://Internetassociation.org*

Dal lato opposto della barricata troviamo ad esempio la già citata Verizon e il Presidente degli Stati Uniti d'America Donald Trump. Quest'ultimo ha nominato Ajit Pai, ex Consigliere Generale di Verizon e strenuo oppositore della Net Neutrality, Presidente del Consiglio di Amministrazione della FCC (*Federal Communication Commission*)[38]. FCC fino al 2017 aveva sempre governato appoggiando la Net Neutrality, ad esempio nel 2010 aveva stabilito tre fondamentali regole [Bil14; Kan14; Eud11a; All+17]:

- **trasparenza**[39]: gli *ISP* 🕮 devono pubblicare le loro *policy* di gestione della rete, le caratteristiche prestazionali e i termini e condizioni di accesso ai loro servizi[40];
- **non blocco**: gli *ISP* 🕮 non devono bloccare alcun contenuto *legale*[41], applicazioni, servizi e device non pericolosi e nemmeno applicazioni e altri servizi in competizione coi propri;
- **non discriminazione**: prescrizione di una generica non discriminazione del traffico.

La nomina di Pai ha ribaltato l'atteggiamento di FCC che nel 2017 ha abrogato le norme protettive nei confronti degli utenti [Giu17]. Per fortuna il movimento a favore della Net Neutrality si è mosso per combattere questa abrogazione [Lic18].

Vediamo contesti più vicini a noi, cosa succede in Europa e Italia? Anche da noi c'è stato dibattito, sebbene, specie in Italia e al di fuori degli ambienti tecnici, i mass media non abbiano dato grandissimo risalto ai processi normativi sul tema. Attualmente sono in vigore delle linee guida[42] emanate dal BEREC (*Body of European Regula-*

[38] L'ente USA (fondato nel 1934) che regolamenta le comunicazioni via satellite, radio, cavo ecc. e che per statuto dovrebbe essere *indipendente* (`http://fcc.gov`).

[39] Quindi misurabilità e verificabilità.

[40] Verificare che le informazioni pubblicate siano effettivamente quelle in vigore è un altro paio di maniche.

[41] Le definizioni di *legale* e *non pericoloso* sono spesso vaghe e facilmente interpretabili.

[42] `http://www.wired.it/attualita/politica/2016/08/30/net-neutrality-europa-linee-guida` e soprattutto `http:`

tors for Electronic Communications), omologo di FCC, che *prescrivono* meccanismi non discriminatori simili ai già citati regolamenti USA. La non obbligatorietà di tali linee guida lascia ai singoli paesi l'effettiva normazione.

Ad esempio il *data cap* 🕮 con esclusioni è perfettamente legale, basta guardare le pubblicità dei vari provider telefonici per rendersene conto: propongono tariffe a *forfait* con **esclusioni** dal cumulo[43]. TIM[44] offre, a settembre 2019, un profilo *Social&Chat* che esclude dal cumulo dati i seguenti servizi: Whatsapp, Facebook, Instagram, Skype, Twitter, Telegram, Linkedin, Viber, Snapchat, WeChat, Tumblr, iMessage, Pinterest, Imo, Tinder, ASKfm; e un profilo *Supergiga Video* che esclude: Youtube, Amazon Prime, Netflix, Rai Play, Mediaset Play, Infinity, Mediaset Premium, CHILI, DAZN, Dailymotion, Fox News, Vimeo e TIMVISION.

Un **produttore di contenuti non *mainstream***, ad esempio chi usa piattaforme libere *self hosted* o piattaforme neutrali come `archive.org` o `wikipedia.org`, sarà svantaggiato nell'attrarre utenti verso la propria piattaforma perché chi vorrà vedere i suoi contenuti dovrà *spendere* traffico consumando il proprio *plafond*.

A tal proposito, dal 2016 in Italia è attivo un gruppo di vigilanza dell'AGCOM (Autorità per le Garanzie nelle Comunicazioni)[45] che pubblica un rapporto [AGC16] periodico sulle sue attività di *moral suasion*, non potendo avvalersi di normative che lo impongano, nei confronti di *ISP* 🕮 non ottemperanti.

Torniamo al contesto mondiale segnalando un interessante caso, quello dell'offerta di Facebook per la fornitura *gratuita* di connettività in India chiamata *FreeBasics*. Essa avrebbe previsto l'accesso gratuito alla rete per molti

`//berec.europa.eu/eng/netneutrality`.

[43] Ci permettiamo di citare di nuovo (lo avevamo fatto nel capitolo "*Livello 0 [The Net]*" - 0) il video tragicomico `http://youtube.com/watch?v=NLKyIhYwyWc` che descrive la distorsione della Rete nell'applicare queste *esclusioni*.

[44] `http://tim.it`

[45] `http://www.agcom.it`

milioni di indiani, **al prezzo di una fortissima relatività**: la lista dei siti accessibili sarebbe stata ridotta a Facebook e pochissimi altri siti o servizi. Una sorta di *keyhole* (buco della serratura) attraverso cui avere uno scorcio *da galeotto*[46] sulla rete. L'offerta è stata rifiutata [Bia16].

Chiudiamo con una piccola nota storica che secondo noi ha anche un *involontario* significato in termini di *relatività* della rete e di accesso alla conoscenza[47]. Nel termine ADSL (*Asymmetrical Digital Subscriber Line*), che identifica una tecnologia di connessione alla Rete, la parola *asymmetrical* descrive la caratteristica tipica di questa tecnologia nel fornire velocità di trasmissione **diverse** a seconda della direzione del flusso dei dati: il flusso *entrante* (*download*) è in genere da 5 a 10 volte più veloce del flusso *uscente* (*upload*). Le origini storiche sono tutto sommato razionali: quando è stata ideata si pensava all'uso *"web 1.0"*[48] e dato che la capacità totale del canale era limitata superiormente si decise di dimensionare *asimmetricamente* i due flussi. Naturalmente questa scelta crea un'enorme **sacca di relatività** proprio all'ingresso della Rete. Ma **l'uso della Rete è cambiato**: oggi è frequente condividere tanta informazione quanta se ne fruisce, per cui sarebbe forse più sensato muoversi verso una allocazione più simmetrica dei flussi. Però anche con le nuove tecnologie basate su fibra ottica osserviamo rapporti, pur migliori, ma sempre intorno al $3.5:1$ (es. 1Gbit/s *down* vs. 300Mbit/s *up*).

[46] Permetteteci il termine, senza offesa per i convitti.

[47] Che tratteremo nel capitolo "*Livello 3 [education]*" - 3.

[48] Pagine web pressoché statiche, il flusso informativo uscente era limitato alla richiesta della pagina da scaricare, mentre il flusso entrante era costituito dalla pagina richiesta che poteva ad esempio contenere immagini anche di dimensioni notevoli.

2.5 Quali servizi digitali di base?

```
You are entitled to food,
clothing, shelter and medical
attention. Anything else
that you get is a privilege.
```

Dal regolamento della prigione di Alcatraz (USA)

Ora che abbiamo un quadro degli aspetti tecnici e qualitativi dei servizi digitali, vogliamo tentare la costruzione di un *elenco di possibilità*, una lista di servizi digitali che potrebbero essere elevati al rango di *servizi di base per la cittadinanza digitale*?

Durante gli anni in cui si è svolto il corso di Cittadinanza Digitale e Tecnocivismo abbiamo sempre proposto agli studenti un breve *compito*: "elenca quali servizi digitali ritieni debbano essere considerati fondamentali, argomentane pro e contro, accessibilità ecc.". Qui di seguito ne riportiamo un condensato, va preso come spunto per ulteriori discussioni e riflessioni, non ha pretesa di proposta formale. Molti dei servizi elencati sono già disponibili sul mercato e accessibili, economicamente parlando.

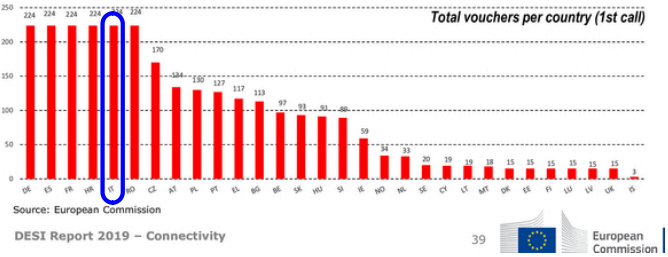
2.5.1 WiFi

A parte l'umorismo del *meme* citato in sezione "*Bisogni primari dell'uomo*" - 2.1 in cui viene dichiarata Internet come bisogno fisiologico fondamentale vediamo quali potrebbero essere i vantaggi, gli svantaggi, i costi ecc.

Garantire copertura *WiFi* sul territorio non è cosa da poco, un router *potente* (tra 100mW e 1000mW) copre un'area di qualche centinaio di metri in assenza di ostacoli quali edifici, colline, monti o di qualche decina all'interno di edifici, specie se in cemento armato. Un Comune piccolo, di qualche chilometro quadrato dovrebbe installa-

re decine di tali router, connetterli mediante cablaggio[49] ad un accentratore che poi realizzi la connessione col resto della Rete. **Molto approssimativamente** il costo di acquisto e installazione **per nodo** è di un migliaio di euro, a cui vanno aggiunti i costi di connettività e di manutenzione dell'infrastruttura: vanno infatti gestiti gli aspetti di autenticazione, sicurezza, monitoraggio del funzionamento ecc.

Per fortuna vengono in aiuto alcuni fondi europei come l'iniziativa *wifi4eu*[50] che l'Italia ha *catturato* con grande efficienza[51]:



Siamo molto curiosi di vedere come verranno spesi quei soldi, se volete consultare la lista di chi è riuscito ad ottenerli potete andare all'elenco percipienti[52].

Un'altra iniziativa nella direzione del *servizio di base/universale*, al momento senza seguito, è stata la proposta di legge[53] del 2014, firmata da più di cento parlamentari che prevedeva l'obbligatorietà per gli esercizi commerciali al di sopra di una certa *dimensione* di fornire accesso WiFi gratuito e senza password. Tale proposta è rimasta senza

[49] Esiste anche la possibilità di creare le cosiddette *reti mesh* che sfruttano la connessione radio tra i router, ma le prestazioni degradano abbastanza rapidamente al crescere del numero di nodi (*http://www.revolutionwifi.net/revolutionwifi/2012/02/mesh-network-performance-impact.html*)

[50] *http://wifi4eu.ec.europa.eu*

[51] Sempre tratto dal rapporto DESI 2019 citato precedentemente.

[52] *http://wifi4eu.ec.europa.eu/#/list-municipalities*

[53] *http://www.businesspeople.it/Business/Media/Proposta-di-legge-per-il-Wi-fi-obbligatorio-nei-negozi-il-si-di-110-parlamentari_70452*

seguito forse anche perché andava contro alla *cultura del terrore* instillata dal *famoso* "*Decreto Pisanu*"[54], rimasto in vigore dal 2005 al 2011 ma i cui effetti nefasti si notano ancora oggi, che prevedeva il controllo dell'identità di ogni persona che accedeva alla rete. Cioè si è passati in pochi anni dal divieto assoluto all'accesso "anonimo" alla Rete alla proposta di renderlo obbligatorio… a spese degli esercenti.

Queste iniziative sono state in realtà superate da innovazioni tecniche, adeguamenti normativi e iniziative commerciali che hanno portato ad una copertura delle connessioni di telefonia mobile[55] superiore al 90% del territorio e con piani tariffari *flat rate* (con traffico dati incluso, decine di GB al mese) intorno ai 10 euro mensili; il servizio di connettività è di fatto garantito e accessibile a tutti i cittadini, pur non essendo formalmente dichiarato come *servizio di base/universale*[56].

Gli unici soggetti *disagiati* sono gli stranieri temporaneamente[57] in Italia, per esempio turisti, che in mancanza di un piano *flat rate* europeo (peraltro disponibile dal 2015[58] per usi *fair* in *roaming*) o mondiale avrebbero bisogno di connettività *pubblica*, in questi casi però basterebbe offrire copertura WiFi nei luoghi maggiormente frequentati.

[54] *http://it.wikipedia.org/wiki/Giuseppe_Pisanu#Il_decreto_Pisanu_antiterrorismo*

[55] *http://www.ripetitore-gsm.it/blog/copertura-mobile-in-italia*

[56] Si veda *http://www.mise.gov.it/index.php/it/comunicazioni/telefonia/servizio-universale* per la definizione di quello telefonico e *http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32015R2120&from=EN* per la direttiva UE a proposito dell'accesso a Internet

[57] Chi resta per un periodo lungo di solito si procura una SIM locale e un telefono *dual-sim* o un secondo telefono.

[58] *http://eur-lex.europa.eu/eli/reg/2015/2120/oj*

2.5.2 Fibra ottica

Molto più interessante, rispetto al WiFi, concentrarsi sulla riduzione del *digital divide* sul territorio nazionale attraverso un adeguato *cablaggio*. Aumentare il grado di connettività globale ha effetti positivi soprattutto sull'economia e sulla produttività: aziende meglio connesse e *smart working*, che anticamente si chiamava *telelavoro*, riducono la *movimentazione degli atomi* preferendo quella *dei bit*. La banda larga porta conoscenza (es. formazione a distanza) oltre che svago (es. *video streaming*) e, contrariamente alla televisione, è uno strumento **bidirezionale**.

Poco sopra abbiamo mostrato come l'Italia sia indietro rispetto al resto d'Europa in questo campo, per recuperare il terreno il Governo ha dato l'avvio, nel 2015, alla "*Strategia Italiana per la Banda Ultra-larga*"[59] con lo stanziamento di fondi verso le regioni per coprire *in primis* le aree cosiddette a *fallimento di mercato*[60]. L'obiettivo è il raggiungimento dei livelli prefissati dall'Agenda Digitale Europea[61] entro il 2020.

Il meccanismo prevede la creazione di una rete di proprietà pubblica[62] che realizza le infrastrutture, principalmente la posa dei cavi, vendendo poi connettività *all'ingrosso* ai vari *ISP* 🕮 sul territorio. In figura 2.4 una mappa della copertura di rete NGA-VHCN (*Next Generation Access - Very High Capacity Networks*) prevista in Lombardia per il 2020.

Il **primo servizio di base/universale** per la Cittadinanza Digitale che ci sentiremmo di proporre è un abbassamento ulteriore del limite stabilito normativamente di *digital divide*, cioè un forte contenimento della *malattia*.

[59] *http://bandaultralarga.italia.it/piano-bul/strategia*

[60] Dove cioè gli operatori commerciali non avrebbero guadagno e quindi rinunciano a investire.

[61] *http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=LEGISSUM%3Asi0016*

[62] Per l'Italia è OpenFiber (*http://openfiber.it/corporate/societa/struttura-societaria*), società partecipata al 50% da Enel e CDP (Cassa Depositi e Prestiti), nata a fine 2015.

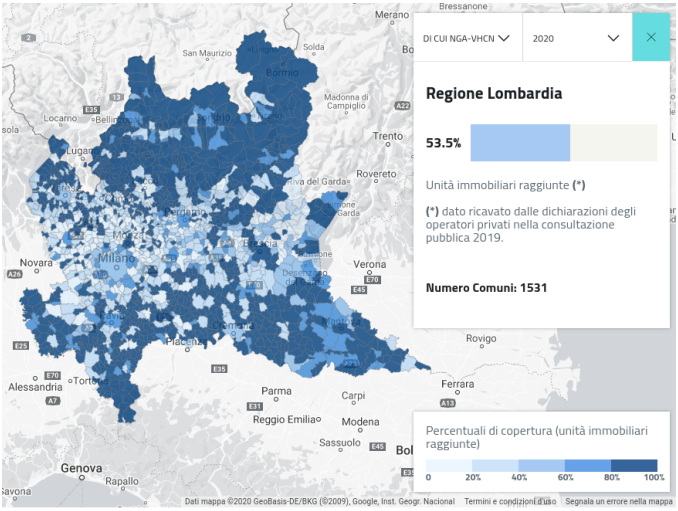


Figura 2.4: Previsione copertura rete alta velocità Lombardia (Italia Digitale 2020)

2.5.3 *Computing device*

Per accedere ad un servizio digitale, tipicamente via Internet, serve una connessione *ragionevole* per quel servizio, ma serve anche un *computer adeguato*, sempre in funzione del servizio: per compilare modulistica *complessa*, come una dichiarazione dei redditi o un bando di gara, non basta un cellulare, invece per seguire un video corso di lingua straniera potrebbe essere sufficiente uno schermo relativamente piccolo e una buona cuffia, se non è necessario interagire con il docente. Difficile definire in anticipo le caratteristiche precise di un ipotetico *device universale*. Per usare una metafora: la Rete (Internet) sta alla rete stradale come un *computing device* sta ad un veicolo. Usi e necessità diverse implicano veicoli diversi.

Pensare di fornire ai singoli cittadini un proprio veicolo **non funziona**, né in termini pragmatici, perché ogni soggetto ha esigenze e capacità diverse, né in termini economici per impegno finanziario che ne deriverebbe. Meglio

a questo punto, sfruttando ancora la metafora della rete stradale, fornire una buona rete di *mezzi pubblici* per i cittadini digitali, che non possono permettersi un *veicolo proprio*. Il *mezzo pubblico digitale* sono le postazioni connesse a Internet messe a disposizione in molti luoghi pubblici come biblioteche, comuni e scuole o privati come in molti alberghi.

Sarebbe importante definire questo tipo di servizio introducendo normative di salvaguardia che garantiscano una presenza capillare sul territorio, ad esempio stabilendo un numero minimo di postazioni pubbliche per abitante.

2.5.4 Domicilio digitale (*storage* e *cloud*)

Invece di un *computing device* fisico potremmo anche pensare a qualcosa di virtuale? Un *personal computer* remoto e virtuale dotato di un *disco* (*storage*) adatto a immagazzinare i nostri dati e documenti, con installati i programmi di uso comune in modo da non aver neppure bisogno di computer fisico, ma di potervi accedere semplicemente da un *web browser* da qualunque postazione[63] pubblica o privata?

Soluzioni come quella appena descritta in realtà esistono già e sono alla portata di chiunque, addirittura la maggior parte delle persone che possiedono un cellulare Android hanno già il servizio gratuitamente abilitato avendo dovuto registrare un account Google per completare la configurazione del proprio telefono.

Stiamo parlando di servizi come Google Drive[64] o Dropbox[65] per quanto riguarda lo *storage*, con alcuni GB di capacità, estendibili a pagamento; di Google Docs[66] o di Office 365[67] per i programmi quali *editor* di documenti, strumento per le presentazioni, foglio elettronico, calenda-

[63] Portando con sé soltanto una login e una password.
[64] *http://drive.google.com*
[65] *http://dropbox.com*
[66] *http://docs.google.com*
[67] *http://office365.com*

rio, agenda ecc.; Gmail[68] per la posta elettronica. Esistono anche alternative libere (nel senso della licenza) e installabili su proprio cloud[69] come NextCloud[70].

Predisponendo un ambiente completo del genere, un cittadino digitale può evitare di avere "il ferro" (il computer) senza perdere traccia del proprio lavoro (quasi) ovunque si trovi.

Non esistono normative di salvaguardia per questo tipo di servizio, in ogni caso è reperibile a costi *contenuti*, addirittura gratis[71] nella maggior parte dei casi. L'unico *caveat* è che i servizi attualmente disponibili sono forniti da aziende extraeuropee che quindi sottostanno a normative molto distanti dalle nostre, si pensi ad esempio al GDPR (*General Data Protection Regulation*) che è normativa europea, ma che in USA non viene applicata.

Per quanto riguarda l'accesso a tale tipo di servizio, non avendo un *device* proprio è chiaro che il cittadino dovrebbe appoggiarsi a postazioni pubbliche dotate di connessione e *browser* quindi valgono le stesse considerazioni fatte in sezione "*Computing device*" - 2.5.3 per la garanzia sul numero di postazioni per abitante.

2.5.5 Posta elettronica e PEC

> `Se non hai una email non esisti`
>
> *(barzelletta, cfr. box 2.5.1)*

Nel mondo analogico il concetto di *indirizzo di un cittadino* ha un ben preciso significato: indica il luogo geografico di residenza o domicilio della persona in questione: tutte le comunicazioni ufficiali e non vengono inviate all'in-

[68] *http://gmail.com*

[69] Se si vuole evitare la *schiavitù* di un servizio ospitato su server fuori dal nostro controllo.

[70] *http://nextcloud.com*

[71] Ma un proverbio dice: "le cose gratuite a volte sono le più costose".

dirizzo conosciuto. Un cittadino sprovvisto di un indirizzo è un *senza fissa dimora*: associamo questa definizione ai criminali latitanti e agli indigenti che vivono per strada.

Potremmo attribuire lo stesso significato al non avere un indirizzo di posta elettronica? Nel mondo digitale in effetti non essere *indirizzabile* vuole davvero dire non esistere, non essere raggiungibile, non contattabile. Se come società ci vogliamo muovere verso una sempre maggiore *dematerializzazione*[72] del paese dobbiamo spingere verso una cultura in cui l'indirizzo *elettronico* diventa persino più importante di quello *fisico*, almeno ai fini della burocrazia e della gestione delle comunicazioni formali. Qualunque servizio digitale richiede la fornitura di un qualche tipo di *indirizzo* per poter contattare (ma anche riconoscere) l'utente durante l'espletamento, l'informazione che **viene richiesta più di frequente è proprio la email**, subito seguita dal numero di telefono (e alcuni servizi specificano che deve essere un cellulare[73]), mentre l'indirizzo fisico è tipicamente opzionale a meno di non dover ricevere consegne di merce.

Oggi ottenere una casella email è semplice e si trovano molte offerte gratuite. Ci sentiamo di proporlo come *servizio di base/universale* solo nell'ottica di evitare, formalizzandone una garanzia normativa, la "mercificazione" delle informazioni personali che molti *provider* operano nell'offrire gratuitamente tale servizio [Lan17].

Il tema importante è inoltre squisitamente culturale, bisogna spingere per una consapevolezza del cittadino nel crearsi il proprio indirizzo digitale e nel *curarlo*: leggere la posta in arrivo e rispondere, possibilmente non con i tempi della posta tradizionale (*snail mail*, mail lumaca).

Ancora più importante il concetto di PEC (Posta Elet-

[72] Eliminazione della carta in tutti i processi della vita quotidiana.

[73] Abbastanza comprensibile: sia perché un cellulare è maggiormente legato ad una singola persona rispetto ad un numero fisso, sia perché tramite cellulare è possibile inviare notifiche SMS, Telegram, Whatsapp ecc.

tronica Certificata)[74], un meccanismo **tutto italiano**[75] che permette l'invio *garantito* di email. L'invio di una PEC genera dei certificati crittografici che attestano l'avvenuto invio e l'avvenuta ricezione, esattamente come una raccomandata con ricevuta di ritorno, con il vantaggio che tali certificati garantiscono anche l'integrità del contenuto.

Dal punto di vista dei *servizi di base* un tentativo maldestro di fornire a ogni cittadino italiano un indirizzo PEC (si chiamava in realtà CEC-PAC ed era uno standard lievemente diverso) fu fatto tra il 2009 e il 2015[76]. La CEC-PAC era una PEC limitata alle comunicazioni tra cittadino e P.A. e impediva la comunicazione tra cittadini come si può vedere nella schermata (in questo caso un tentativo di auto-spedirsi un messaggio) qui sotto:

Fallì principalmente perché molti enti della Pubblica Amministrazione:

- non avevano attivato l'indirizzo PEC oppure...
- lo avevano attivato ma non consultavano mai la casella oppure...
- chiedevano di inviare email agli indirizzi "normali" oppure, ancora peggio...
- chiedevano l'invio di fax o posta cartacea!

[74] *http://it.wikipedia.org/wiki/Posta_elettronica_certificata*

[75] Standard inventato in Italia, incompatibile con standard internazionali: per l'estero un indirizzo PEC italiano viene visto (nel migliore dei casi) come un normale indirizzo email.

[76] *http://www.agid.gov.it/it/search?search_api_fulltext=cec-pac*

Forse i tempi non erano ancora abbastanza maturi per tale rivoluzione, nel 2020 la diffusione della PEC è notevole e si può dire che funzioni: ottenere una PEC è banale quanto una email, unica differenza è che non è un servizio gratuito, però l'ordine di grandezza è della decina di euro annui per l'offerta base.

TECHBOX: La barzelletta della email [2.5.1]

Un disoccupato si presenta ad un colloquio in $GRANDEAZIENDA per un posto come uomo delle pulizie.
Il responsabile del personale, dopo un colloquio e un test gli dice che è assunto e gli chiede l'email per inviargli la documentazione per l'assunzione.
La persona risponde che non ha né computer, né posta elettronica.
Il responsabile allora gli dice che non avere una email significa non esistere e quindi non gli possono dare il lavoro.
L'uomo se ne va, disperato, senza sapere cosa fare e con solo 10 dollari in tasca.
Decide di andare al mercato e comprare una cassa di pomodori. Vendendoli porta a porta in poco tempo riesce a raddoppiare il capitale, e ripetendo l'operazione più volte si ritrova con un discreto capitale.
A quel punto capisce che così può sopravvivere e guadagnare e si organizza: in poco tempo si compra prima un carretto, poi un camion e col tempo arriva ad avere un parco veicoli per le consegne. In pochi anni diventa il proprietario di una grande catena di negozi alimentari.
Ad un certo punto decide di stipulare una polizza sulla vita per lui e la sua famiglia, contatta un assicuratore e sceglie un piano previdenziale, ma, quando l'assicuratore gli chiede l'email per mandargli la proposta, lui risponde che non ha né computer né posta elettronica.
"Singolare", dice l'assicuratore "lei ha costruito un impero, ma non ha una email! Immagini che cosa sarebbe se avesse avuto un computer!"
L'uomo ci pensa un momento e risponde: "Sarei l'uomo delle pulizie di $GRANDEAZIENDA!"

2.5.6 Identità digitale e SPID

```
``Altolàchivalà! Amici o
nemici?'' - ``Semplici
conoscenti!''
```

Sturmtruppen (Bonvi)

Salvo casi molto semplici, per usufruire di un servizio bisogna *accedere*, nel senso di *autenticarsi*. Per *avere un account*, cioè essere riconoscibili, tipicamente ci si deve preventivamente registrare: vanno fornite alcune informazioni anagrafiche, si deve creare una password[77] e da quel momento in poi si potrà utilizzare il servizio ogni volta che si vorrà.

Il difetto di questa procedura è che si deve effettuare **per ogni servizio a cui si vuole accedere**, inventando e ricordandosi login e password di ognuno. Un primo modo di ovviare al problema di doversi annotare su carta, o peggio sulla rubrica del telefono[78], quelle informazioni è l'adozione di un *password manager* (cfr. box 2.5.2). Ma dover ripetere la procedura di registrazione ogni volta resta un sistema macchinoso.

Sarebbe ideale avere a disposizione un meccanismo cosiddetto di SSO (*Single Sign On*), cioè un gestore centralizzato di identità che permetta di accedere a tutti i servizi compatibili registrandosi una volta sola ed utilizzando un unico *account*.

Naturalmente questo tipo di funzionalità è disponibile da tempo immemore in molti sistemi informatici di grandi dimensioni[79], ma in questa sede ci interessa citare un servizio di autenticazione tutto sommato recente e ad og-

[77] Tipicamente con alcuni vincoli minimi sulla forma, ad esempio lunghezza minima, presenza di maiuscole, minuscole e segni di punteggiatura o caratteri speciali, non una parola di senso compiuto ecc. in modo che non risulti facilmente indovinabile dai *bot* 🕮.

[78] Ricordiamo che quei dati vengono salvati **tipicamente in chiaro** in cloud (Android su Google, iPhone su Apple)!

[79] *NIS/YP* e *LDAP* risalgono ai primi anni '90 del XX secolo.

gi utilizzabile principalmente per i servizi della Pubblica Amministrazione, stiamo parlando di *SPID* 🕮:

> *SPID è il Sistema Pubblico di Identità Digitale che garantisce a tutti i cittadini e le imprese un accesso unico, sicuro e protetto ai servizi digitali della Pubblica Amministrazione e dei soggetti privati aderenti*[80]

SPID 🕮 si ottiene facilmente[81] e una volta ottenuto si può utilizzare per autenticarsi e richiedere servizi su praticamente ogni sito web della P.A. italiana. La lista dei siti che accettano *SPID* 🕮 è nutrita[82], conta (febbraio 2020) più di 4000 amministrazioni nazionali, mentre le utenze finora (idem) attivate sono poco meno di sei milioni[83]. Esempi notevoli di P.A. compatibili con *SPID* 🕮:

- INPS
- INAIL
- Agenzia Entrate
- Fascicolo Sanitario Elettronico e Servizi Sanitari
- moltissimi Comuni
- Regioni
- Bollo auto e servizi di pagamento tributi
- SUAP

[80] *http://www.agid.gov.it/it/piattaforme/spid*

[81] Su *http://www.spid.gov.it* c'è l'elenco dei provider, l'unica procedura non gratuita è l'identificazione (di persona o via webcam), ma il costo è molto contenuto, dell'ordine della ventina di euro.

[82] *http://www.spid.gov.it/servizi*

[83] *http://avanzamentodigitale.italia.it/it*

TECHBOX: I *password manager* [2.5.2]

Sono programmi utilissimi e ne consigliamo caldamente l'utilizzo: salvano i dati su file in formato standard criptato, l'unica password da ricordare sarà quindi quella di decrittazione del file stesso.
Permettono la gestione delle password per categorie, generano password *random* seguendo un *template* configurabile ed esistono anche sotto forma di app per smartphone, potendo così condividere il file delle password tra PC e cellulare attraverso un servizio di sincronia cloud (e.g., Dropbox, Google Drive, ecc.).
Il più noto è *keepass* (*http://keepass.info*).

2.5.7 Altri servizi

Lasciamo in forma di lista commentata alcuni servizi su cui si dibatte ma per i quali non abbiamo ancora una proposta articolata:

- **Firma digitale**, meccanismo di firma crittografica dei documenti: attualmente esistono standard internazionali e locali[84], un documento firmato digitalmente è di provenienza certa (autenticità), non ripudiabile e integro; la verifica di queste proprietà è molto più facile rispetto alla controparte cartacea, è sufficiente un software per computer, tablet o cellulare. A seconda del fornitore, prevede l'uso di chiavette hardware, i cosiddetti *token OTP (One Time Password)*, o di carte elettroniche digitali come la CIE (Carta Identità Elettronica) con l'utilizzo di un lettore apposito; costa qualche decina di euro l'anno.
- **Marca temporale**, meccanismo di *timestamping*, ovvero timbratura con data e ora: permette di garantire data e ora di un certo *evento* (tipicamente l'emissione di un documento, un file), ad esempio a fini di notifica, notarili, di tutela del copyright ecc. Può essere combinata con la firma digitale. Viene tariffata *a timestamp generato*, qualche centesimo l'uno.
- **Conservatoria digitale**[85], meccanismo di archiviazione sicura e garantita per documenti digitali: molti procedimenti burocratici prescrivono la conservazione dei documenti anche per molti anni (es. documentazione fiscale), in versione cartacea esistono strutture fisiche preposte e (lascamente) certificate[86]; in versione digitale attualmente esistono parecchi forni-

[84] *http://www.agendadigitale.eu/documenti/firme-elettroniche-tutte-le-tipologie-alla-luce-del-regolamento-eidas*

[85] *http://www.agid.gov.it/it/piattaforme/conservazione*

[86] Ad esempio i commercialisti, era prassi offrire il servizio (a pagamento) di *conservazione archivi cartacei* ai propri clienti, ma non sempre il servizio era *garantito* nel senso di protetto da eventi atmosferici, incendi ecc.

tori[87].

- **Fatturazione elettronica**[88], versione digitale della fatturazione tradizionale, basata sull'interscambio (attraverso server governativo) di file in formato XML (*eXtensible Markup Language*) di facile compilazione[89].
- **VoIP (*Voice over Internet Protocol*)**, telefonia via rete, lo standard internazionale più diffuso è libero e si chiama SIP (*Session Initiation Protocol*)[90] (da non confondere con l'antico nome della compagnia dei telefoni nazionale italiana) anche se molti utenti usano programmi proprietari (Whatsapp, Skype ecc.) senza conoscere la tecnologia su cui poggiano. Curioso anche il fatto che la telefonia tradizionale sia stata per molti anni (si veda box 2.5.3) considerata *de iure* un *servizio universale*, ma mai si sia accennato ad un discorso analogo per la telefonia via rete, anche se, a onor del vero, lo si fa per il servizio di rete in quanto tale (cfr. sezione "*Digital divide*" - 2.4.1).

[87] *http://www.agid.gov.it/it/piattaforme/conservazione/conservatori-accreditati*

[88] *http://www.agenziaentrate.gov.it/portale/aree-tematiche/fatturazione-elettronica*

[89] *http://www.agenziaentrate.gov.it/portale/web/guest/aree-tematiche/fatturazione-elettronica/guida-fatturazione-elettronica/come-predisporre-inviare-ricevere-fe/come-si-predispone-fe*

[90] *http://www.ietf.org/rfc/rfc3261*

TECHBOX: Le cabine telefoniche [2.5.3]

In tema di *servizi di base* non possiamo non citare il caso delle cabine telefoniche, fino a tempi recenti considerate formalmente un *servizio universale* sottoposto a rigidi vincoli di presenza sul territorio e procedure garantiste per la dismissione: se il gestore voleva dismetterne una doveva prima affiggere una comunicazione sulla cabina stessa e attendere un periodo di transizione in cui i cittadini della zona potevano motivare la richiesta di mantenimento in funzione.
Dal 2019[a] invece la cabina telefonica perde il suo status:

> *Nel 2019 si parlerà di cabine telefoniche perché un paio di mesi fa è stato approvato il nuovo Codice europeo per le comunicazioni elettroniche. Tra le comunicazioni elettroniche ci sono anche quelle fatte per strada con una cornetta in mano e, come sempre, l'Italia dovrà 'recepire quel testo nel proprio ordinamento'. In poche parole, l'Unione Europea dice nel Codice che gli Stati possono smettere di considerare i telefoni pubblici un 'servizio universale', cioè che ogni Stato deve impegnarsi a offrire ai propri cittadini. TIM, la società che gestisce tutti i telefoni pubblici d'Italia, è infatti ancora obbligata a garantire un certo numero di cabine telefoniche funzionanti. Dai prossimi mesi potrebbe iniziare a smantellarle, ma per farlo avrà bisogno di permessi che dipendono dal parere dell'AGCOM, l'Autorità per le garanzie nelle comunicazioni.*

Una mappa delle cabine e dei posti telefonici pubblici era consultabile su *http://www.tim.it/telefono-pubblico*, pagina ora sparita dal web e raggiungibile solo attraverso *archive.org* (cfr. box 1.2.1).

[a] *http://www.ilpost.it/2019/02/03/cabine-telefoniche*

Capitolo 3

Livello 3 [*education*]

"Il sonno della ragione genera mostri" (F. Goya)

Molte tecnologie sono più difficili da usare rispetto al rubinetto dell'acqua. E non è solo l'uso ad essere complesso: diventa tema tutt'altro che banale[1] anche e soprattutto quello della conoscenza *whitebox* 🕮 e delle implicazioni e ramificazioni della tecnologia, specie quella digitale. Citando un'intervista a Douglas Rushkoff[2]:

> *Le nostre tecnologie diventano più complesse mentre noi diventiamo più semplici. Esse imparano su di noi mentre noi impariamo sempre meno su di loro. Nessuno può capire tutto quello che succede in un iPhone, tanto meno nei sistemi pervasivi.*

[1] Senza offesa per il sistema idrico che è tutto fuorché banale.
[2] `http://www.wired.com/2011/07/douglas-rushkoff`

Il progresso tecnologico in questo caso non aiuta, anzi peggiora la situazione: col tempo aumenta infatti il numero delle funzionalità e degli oggetti da gestire e conoscere (si pensi ad esempio a tutto l'universo *Internet of Things*); tutto questo non è adeguatamente accompagnato - **attualmente** - da una maggiore consapevolezza degli utenti. L'intento degli autori è quello di contribuire a invertire la tendenza in modo che in un futuro vicino l'universo tecnologico sia **completamente conoscibile**.

La scienza dell'informatica ha prestato e presta tuttora molta attenzione nei confronti dell'usabilità del software [Nie00; Nor13] - si tratti di programmi, *app*, siti web o altro - ma sono stati fatti sforzi insufficienti per diffondere la consapevolezza di massa sui cosiddetti *internals*: i meccanismi di funzionamento, le architetture, il trattamento dei dati e altri dettagli che restano appannaggio di pochi addetti ai lavori.

Anche sul fronte politico è tutt'altro che facile seguire[3] le purtroppo innumerevoli iniziative negativamente impattanti sulla vita del cittadino digitale. Siamo certi che se nominassimo ad esempio: ACTA (*Anti Counterfeiting Trade Agreement*), SOPA (*Stop Online Piracy Act*), PIPA (*PROTECT IP Act*), HADOPI (*Haute Autorité pour la Diffusion des Œuvres et la Protection des droits d'auteur sur Internet*), DRM (*Digital Rights Management*)[4], UEFI (*Unified Extensible Firmware Interface*) o le varie proposte di legge (alcune purtroppo in vigore[5]) per *azzoppare la crittografia*, la maggior parte dei lettori confesserebbe di aver forse letto o sentito citare l'acronimo, ma senza associarlo ad un particolare *attacco alla Cittadinanza Digitale*. Questi *attacchi* sono quasi ignorati nelle notizie quotidiane e la battaglia è spesso silenziosamente combattuta da movimenti tecno-politici come le già citate Free Software Foundation, Electronic Frontier Foundation ecc. Però an-

[3] E men che meno influenzare!

[4] Meglio noto nel *nostro* ambiente (quello del Software Libero) come "*Digital Restriction Management*"

[5] *http://theverge.com/2018/12/7/18130391/encryption-law-australia-global-impact*

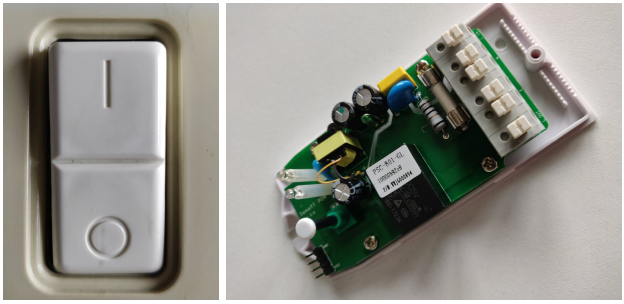


Figura 3.1: Interruttore semplice (sx) vs. interruttore *Internet of Things* (dx)

che il singolo cittadino digitale può acquisire consapevolezza e arruolarsi in questa *lotta* per la presa di possesso della propria *computing agency* (si veda più avanti in sezione "*La computing agency rubata*" - 3.1.4). Servono quindi strumenti cognitivi[6], approccio critico, curiosità e voglia di imparare.

Il **Livello 3** [***education***] è dove analizziamo proprio questi temi:

- partendo dai problemi (*minacce* tecnologiche, *digital divide cognitivo*, legislazione);
- esaminando poi le risposte dall'alto, quelle *istituzionali* promosse dalle politiche per la diffusione della conoscenza informatica;
- illustrando le risposte dal basso, dei gruppi di interesse e le comunità *grassroots*, il *crowdsourcing* 📖;
- infine aggiungendo le nostre proposte ad integrazione e completamento del quadro generale delle necessità del cittadino digitale: Software Libero, *Right to repair* e *Learn to code*.

3.1 Un mondo minaccioso?

Cosa c'è di più semplice di un interruttore della luce (figura 3.1 a sx)? Premendo su "1" la luce si accende mentre premendo su "0" si spegne. E un termostato da riscaldamento autonomo? Ruoto la ghiera della temperatura in senso orario e ad un certo punto la caldaia parte, la ruoto in senso opposto e ad un certo punto si spegne. O ancora un'automobile *vecchio stampo*? Giro la chiave e il motore tenta di avviarsi. Infine un telefono PSTN (la "vecchia" linea telefonica): alzo la cornetta, attendo il segnale di linea, compongo il numero desiderato e attendo l'attivazione della conversazione.

Però man mano che la tecnologia avanza ogni *strumento* tende ad essere sostituito da alternative *con capacità decisionali proprie (intelligenti?).*

Il semplice interruttore da puramente elettromeccanico diventa *elettronico* (figura 3.1 a dx) e lo si comanda da una *app* per cellulare o da un sistema di controllo domotico: il comando di accensione della luce viene digitato sull'interfaccia utente del cellulare (o del tablet o del proprio computer) e l'*intenzione* viene comunicata ad un server probabilmente in Cina[7] che **a sua volta attiva** l'attivazione del *relè*, l'utente quindi si trova a dipendere da un servizio **gestito da altri** per il funzionamento degli oggetti (luci, ecc.) di casa sua.

Vediamo ora il caso del termostato, prendiamo ad esempio il *Nest*[8], un termostato *intelligente* che impara dalle nostre abitudini: quando giorno per giorno impostiamo la ghiera per comunicare i nostri *desiderata* sulla temperatura ambientale **lui** aggiunge informazione ad un modello che si costruisce internamente ed è sulla base di quel modello che decide come e quando attivare la caldaia di casa, **non** c'è

[6] Alcuni strumenti tecnici sono stati citati nei capitoli precedenti.

[7] Nel caso del Sonoff di figura 3.1 l'azienda produttrice risiede a Shenzen mentre D-Link, altro vendor molto diffuso, a Taiwan. Non possiamo sapere dove tengano i server.

[8] *http://nest.com*

connessione causale diretta tra la ghiera e la fiamma della caldaia.

Ancora, le automobili moderne si avviano solo in determinate condizioni (freno e cambio in posizione *park* oppure frizione premuta) e si preannunciano frequentemente *innovazioni* come l'avvio del veicolo solo se si è sobri o solo se l'assicurazione e il bollo sono stati pagati.

In ultimo, la telefonia *voce* è ormai relegata ad una piccola frazione delle attività effettuate mediante un telefono cellulare.

Tutto questo in un contesto dove il numero di oggetti *Internet of Things*, non solo smartphone e PC, con cui dobbiamo *relazionarci*[9] è in continuo aumento: se nel 2010 il rapporto *devices per person* (oggetti digitali a persona) era di *1.83*, nel 2015 era aumentato a *2.09*, nel 2020 si prevede raggiungerà il *3.96* mentre nel 2025 la previsione diventa *9.27* [Saf+17]. Più in là, nel 2030, potremmo arrivare anche a 15 *device*[10] o più.

Attenzione però: per noi **"relazionarci" vuol dire conoscere, configurare, manutenere, controllare**, non lasciare che sia il contrario.

Inoltre ogni singolo *oggetto digitale* diventa sempre più *complesso* (sia nel senso di *denso di funzionalità* che di *difficile comprensione*) col tempo.

Si pensi ad esempio al solo *kernel* di Linux[11]: nato nei primi anni '90, inizialmente contava poche centinaia di migliaia di LOC (*Lines Of Code*)[12], ma già nel 2004 arrivava a cinque milioni di LOC mentre alla fine del 2019 ha raggiunto quasi trenta milioni[13] di LOC. Discorso analogo per il software applicativo: i più noti pacchetti di produtti-

[9] *http://ncta.com/whats-new/iot-has-quietly-and-quickly-changed-our-lives*

[10] *http://martechadvisor.com/articles/iot/by-2030-each-person-will-own-15-connected-devices-heres-what-that-means-for-your-business-and-content*

[11] Che ricordiamo essere alla base di Android, nonché di moltissimi *device Internet of Things*.

[12] Righe di codice.

[13] *http://phoronix.com/scan.php?page=news_item&px=Linux-Git-Stats-EOY2019*

vità personale (Microsoft Office, LibreOffice) raggiungono parecchie decine di milioni di LOC ciascuno e migliaia di funzioni. Dal punto di vista del numero di pacchetti disponibili per una *installazione*[14] di GNU/Linux siamo sull'ordine di grandezza delle centomila unità[15]. Mentre su un cellulare Android è comune vedere oltre cento applicazioni installate[16].

Questa *complessità* va gestita? Certamente **andrebbe** gestita, ma temiamo che le scelte progettuali dei vari produttori di hardware e software vadano invece nella direzione del **mascheramento**.

3.1.1 Tecnologia mascherante

> `Una tecnologia sufficientemente avanzata è indistinguibile dalla magia`
>
> *Terza legge di Arthur C. Clarke.*

Il senso della frase di Clarke[17], per come lo leggiamo noi, è che **non comprendere** una tecnologia ce la fa vedere come misteriosa e magica e come tale può incutere paura e quindi rifiuto oppure affascinare e quindi essere accettata incondizionatamente, in modo *fideistico*. E spesso, purtroppo, è chi crea e vende la tecnologia a renderla opaca, proprio per impedire a chi la usa di percepirla come qualcosa di razionale e gestibile. Il produttore di tecnologia non vuole utenti consapevoli, vuole clienti paganti, nel migliore dei casi.

Partiamo da un esempio banale ma significativo, una deprimente situazione che chi scrive sperimenta ancora og-

[14] La cosiddetta *distribuzione*, ad esempio Debian *http://debian.org*

[15] Poco meno di settemila installate sul computer di chi scrive.

[16] Esattamente 278 sul cellulare di chi scrive questa nota.

[17] Famosissimo scrittore di fantascienza, l'autore di "*2001: odissea nello spazio*".

gi durante gli esami del corso di Programmazione[18]: per valutare gli allievi, all'esame ci si fa consegnare il *sorgente*[19] dei programmi creati dagli studenti durante l'esame, perché gli *eseguibili* non sono "parlanti". Molti sistemi operativi, purtroppo, nel visualizzare il contenuto delle cartelle del *filesystem* omettono una parte del nome del file (la cosiddetta *estensione*, e.g., '.txt', '.doc' ecc.) per cui quando si ha ad esempio una cartella contenente i seguenti file:

```
ContaVocali.class
ContaVocali.java
CostoAbbonamento.class
CostoAbbonamento.java
Triangolo.class
Triangolo.java
TrovaParole.class
TrovaParole.java
```

Una volta aperta la finestra relativa a tale cartella si vedrebbero delle icone con le seguenti etichette:

```
ContaVocali
ContaVocali
CostoAbbonamento
CostoAbbonamento
Triangolo
Triangolo
TrovaParole
TrovaParole
```

Certo, con icone lievemente diverse, ma di non sempre immediata interpretazione.

L'effetto di questo *mascheramento di informazione* è che ad ogni sessione d'esame c'è sempre qualche studente

[18] Dipartimento di Informatica, Università degli Studi di Milano, corso di Programmazione (usiamo Java e Go) del primo anno.

[19] Scrivere un programma vuol dire produrre almeno un file *sorgente* (che sostanzialmente è un file di testo) che deve essere *compilato* da un altro programma (*compilatore* appunto) per produrre un file *eseguibile*. Il file eseguibile è compreso dalla macchina, il file sorgente dall'umano.

che consegna gli eseguibili invece dei sorgenti perché clicca sull'icona sbagliata nel fare il caricamento dei file.

Usando la terminologia della Cittadinanza Digitale e Tecnocivismo si potrebbe dire che ad un *cittadino* (lo studente) è stato negato un diritto (la valutazione del proprio elaborato da parte di un docente) a causa di una informazione *mascherata* (l'estensione del file) da uno strumento informatico. O anche che una **mancata conoscenza** tecnica (non sapere che l'opzione di mascheramento è disabilitabile o non saper usare altri strumenti non mascheranti, ad esempio a linea di comando) ha impedito al cittadino il superamento dell'**ostacolo** introdotto, *in modo del tutto arbitrario*, dal software.

Molte interfacce utente grafiche, le cosiddette WYSIWYG (*What You See Is What You Get*)[20], nella foga della semplificazione "per rendere accessibile la complessità" spesso tendono a *mascherare* informazioni e funzioni che diventano visibili solo effettuando operazioni esplicite. Come ad esempio l'interfaccia web di Wordpress[21] che maschera le azioni effettuabili sugli oggetti (pagine e *post*) a meno di non passarci sopra col mouse[22]: la figura 3.2 mostra due *post* in Wordpress, quello più in basso visualizza le azioni (*Edit | Quick Edit | Trash | View*) perché il mouse (non visibile nello *screenshot*) era sopra quella zona dello schermo.

Ci permettiamo un ultimo esempio riferendoci ad un oggetto familiare ai più: un telefono Android[23]. Android è un sistema operativo, lanciato nel 2008, basato su un *kernel* Linux a cui si aggiungono varie *app* (programmi applicativi) che permettono ad esempio l'effettuazione delle chiamate, la consultazione di siti Internet, la comunicazione via mail, chat ecc. Una parte delle *app* viene installata dal produttore del telefono, altre possono invece essere in-

[20] Ciò che vedi è ciò che hai/ottieni.

[21] `http://wordpress.org`

[22] Il cosiddetto *hovering*.

[23] Nessuno degli autori *possiede* oggetti Apple... anche se in effetti solo Apple possiede i suoi oggetti, il resto del mondo al massimo può usarli.

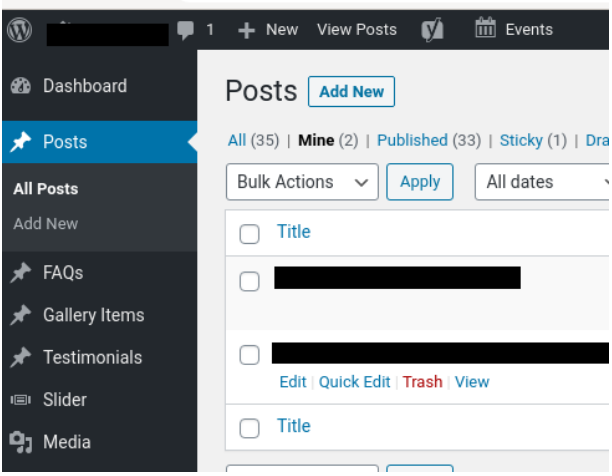


Figura 3.2: Interfaccia web Wordpress

stallate dall'utente consultando degli *store* digitali in cui trovare un'ampia scelta di software gratuito e a pagamento. Il numero esatto di *app* disponibili non è dato sapere[24], ma ciò che vogliamo sottolineare è che una volta installata una *app* questa ha accesso a informazioni e funzionalità del telefono (posizione geografica, contatti, *storage* ecc.) secondo una serie di *permessi* che il proprietario del telefono può, più o meno, controllare. Questo meccanismo di gestione dei permessi[25] è stato introdotto per poter *ingabbiare* software estraneo in modo da impedirgli di *fare cose* diverse da quelle dichiarate[26]. I permessi hanno nomi *parlanti* (per un tecnico) come *ACCESS_FINE_LOCATION* (accesso alla posizione GPS precisa) e ogni applicazione di-

[24] Altro bell'esempio di **relatività a livello servizi**: non è nemmeno certo che venga proposta la medesima scelta di *app* a diversi utenti a fronte delle stesse parole chiave di ricerca.

[25] *http://developer.android.com/guide/topics/permissions/overview*

[26] Famoso il caso delle *torch apps*: applicazioni apparentemente semplici (e inutili in questo caso) che però nascondevano funzioni di raccolta indiscriminata di dati dell'utente (un esempio *http://snopes.com/fact-check/flash-and-grab*).

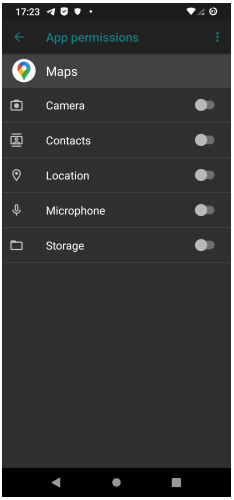


Figura 3.3: Modificare i permessi di una *app* Android

chiara (in un file di configurazione) quali permessi necessita che le vengano concessi per poter funzionare. La lista dei permessi conta poco meno di duecento elementi, ciò vuol dire che **ogni** *app* chiederà tipicamente la concessione di alcune decine di permessi per poter funzionare. Purtroppo il comportamento di *default* 🕮 in Android è quello di concedere tutti i permessi richiesti dall'applicazione. Per selezionare *finemente* la lista dei permessi bisogna:

- aver effettuato il *rooting/jailbreaking* 🕮 del telefono
- aver attivato qualche impostazione, purtroppo non sempre disponibile, per non concedere automaticamente i permessi alle applicazioni
- aver voglia di gestire **migliaia**[27] di permessi **a mano**, usando la goffa interfaccia utente del telefono stesso (figura 3.3, impostazione dei permessi *per singola app* da ripetere per ogni *app* installata).

[27] Sul telefono di chi scrive la lista dei permessi effettivamente attivati conta più di **quindicimila** elementi, vuol dire che ognuna delle 278 applicazioni installate ha chiesto in media una cinquantina di permessi.

L'impresa è così improba che anche chi, come l'autore di questa sezione, vorrebbe limitare i danni è comunque molto sconfortato e spesso "lascia perdere" accettando qualche rischio[28]. In questo caso più che di *mascheramento* si potrebbe parlare eufemisticamente di *disincentivo*, mediante complicazione introdotta arbitrariamente, alla fruizione di funzioni (in questo caso le gestione sensata dei permessi).

Sia chiaro che nonostante questi *problemi della tecnologia* la nostra risposta non sarà **mai** il *neo-luddismo* 🕮 ma bensì una lotta, per lo più politica e culturale, per rendere trasparente, perfettamente conoscibile e gestibile ogni tecnologia, un approccio in *stile Software Libero* (cfr. più avanti sezione "*Software Libero*" - 3.4.1) applicato ad ogni aspetto della vita quotidiana.

3.1.2 L'ignoranza della legge...

...non è una scusante, recita l'articolo 5 del C.P.[29]. Cioè il fatto di commettere un illecito senza saperlo non assolve dalle proprie responsabilità.

Ma pare che soprattutto in Italia il legislatore si sia fatto *prendere un po' troppo la mano*, sia per numero di leggi[30], la cosiddetta **iper-normazione** (e iper-ramificazione[31]), sia per comprensibilità dei testi, al punto da sollecitare una

[28] Si vedano:

- *http://threatpost.com/googles-war-on-android-app-permissions-60-percent-successful/153311*
- *http://cnet.com/news/your-phone-talks-about-you-behind-your-back-these-researchers-are-listening-in*
- *http://forbes.com/sites/zakdoffman/2020/03/06/android-security-horror-show-new-report-warns-40-of-you-face-this-dangerous-malware-risk*

[29] *http://brocardi.it/codice-penale/libro-primo/titolo-i/art5.html*

[30] *http://phastidio.net/2019/07/21/la-sconfitta-di-borrelli-la-tragedia-di-un-popolo*

[31] "Visti articoli X, Y e Z si rimanda alle disposizioni dell'articolo B comma 7 sostituendo il termine 'e il' al posto di 'o il'."

sentenza (nr. 364 del 24/03/1988[32]) della Corte Costituzionale che delegittima parzialmente l'articolo 5 del C.P. rilevando che si deve tenere conto dell'*ignoranza inevitabile* dovuta ad esempio ad analfabetismo, ma anche a **oscurità del testo**:

> *27. - Da quanto innanzi osservato discende, in via generale, che l'inevitabilità dell'errore sul divieto (e, conseguentemente, l'esclusione della colpevolezza) non va misurata alla stregua di criteri c.d. soggettivi puri (ossia di parametri che valutino i dati influenti sulla conoscenza del precetto esclusivamente alla luce delle specifiche caratteristiche personali dell'agente) bensì secondo criteri oggettivi: ed anzitutto in base a criteri (c.d. oggettivi puri) secondo i quali l'errore sul precetto è inevitabile nei casi d'impossibilità di conoscenza della legge penale da parte d'ogni consociato. Tali casi attengono, per lo più, alla (oggettiva) mancanza di riconoscibilità della disposizione normativa (**ad es. assoluta oscurità del testo legislativo**) oppure ad un gravemente caotico (la misura di tale gravità va apprezzata anche in relazione ai diversi tipi di reato) atteggiamento interpretativo degli organi giudiziari ecc.*

Un esempio, molto noto in campo fiscale, di questa modalità molto italiana di iper-normare astrusamente è dimostrata dall'esistenza e dalla grande diffusione della collana di guide Frizzera[33]: un insieme di testi di **interpretazione** delle normative fiscali per aiutare commercialisti e fiscalisti a districarsi nella pletora di leggi, norme e perfino circolari dell'Agenzia delle Entrate che si sovrappongono le une alle altre dando filo da torcere al contribuente e ai suoi

[32] *http://cortecostituzionale.it/actionSchedaPronuncia.do?anno=1988&numero=364*

[33] *http://24oreprofessionale.ilsole24ore.com/prodotti/guida-pratica-sistema-frizzera*

consulenti. In un paese civile, in cui la legislazione fosse cioè chiara e di facile interpretazione, tali guide dovrebbero risultare inutili a priori e a nessuno dovrebbe venire in mente di costruirci sopra un florido commercio[34].

Quindi come **Cittadini** (prima ancora che Digitali) dovremmo chiedere al nostro legislatore come minimo chiarezza dei testi e semplificazione[35], anche per risalire classifiche che ci vedono molto indietro nei sistemi legislativi (es. in figura 3.4, siamo al 28esimo posto secondo WJP).

Invece come **Cittadini Digitali** dovremmo rivolgere la nostra attenzione a una serie di normative, in vigore o proposte, che riguardano la **sfera digitale**. Norme spesso internazionali o a volte applicabili solo in legislazioni estere ma che influenzano, purtroppo in **senso negativo**, anche il nostro universo digitale perché molti servizi su cui ci appoggiamo sono erogati da aziende straniere che applicano le leggi del proprio stato. Tali normative (o *proposte*, comunque *potenzialmente* pericolose) sono doppiamente minacciose poiché, oltre a indirizzarsi verso la sfera digitale, il loro *iter* è frequentemente meno noto rispetto a quello della legislazione tradizionale, salvo forse negli ambienti legati al mondo della cultura libera (cfr. sezione "*Software Libero*" - 3.4.1).

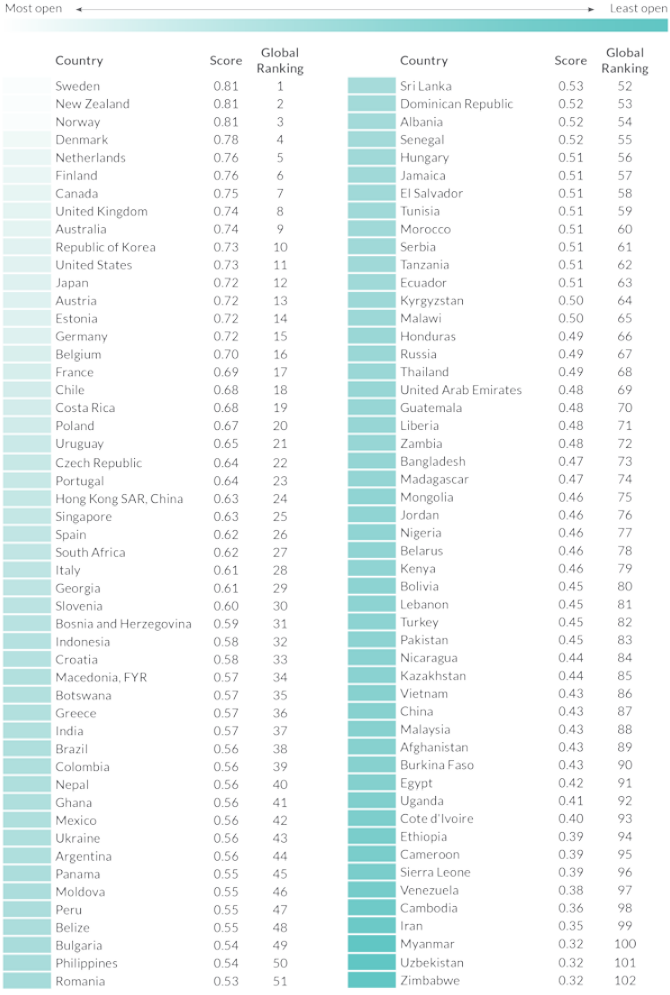
Vediamo qualche esempio concreto di minaccia o attacco legislativo alla Cittadinanza Digitale, la lista è ben lungi dall'essere onnicomprensiva:

- **Brevetti** [BL10][36] in generale e sul software [PCA18] in particolare. La loro efficacia sul progresso della scienza è molto discussa e discutibile, attualmente i brevetti in generale sono diventati semplicemente

[34] Si intenda: nulla contro l'editore Frizzera che fa un egregio lavoro, ci stiamo solo riferendo al fatto che tale mercato non avrebbe ragione di essere.

[35] In relazione alla lunghezza dei testi e soprattutto al **numero di leggi**, in Italia non è nemmeno dato sapere la dimensione esatta del corpus legislativo (*http://ilfattoquotidiano.it/2014/08/28/riforme-il-paese-soffoca-in-un-labirinto-di-leggi/1101193*)

[36] Un riassunto sui "miti" dei brevetti si può leggere qui: *http://hitstartup.com/myths-about-patents-and-trademarks-in-startups*.



Country	Score	Global Ranking
Sweden	0.81	1
New Zealand	0.81	2
Norway	0.81	3
Denmark	0.78	4
Netherlands	0.76	5
Finland	0.76	6
Canada	0.75	7
United Kingdom	0.74	8
Australia	0.74	9
Republic of Korea	0.73	10
United States	0.73	11
Japan	0.72	12
Austria	0.72	13
Estonia	0.72	14
Germany	0.72	15
Belgium	0.70	16
France	0.69	17
Chile	0.68	18
Costa Rica	0.68	19
Poland	0.67	20
Uruguay	0.65	21
Czech Republic	0.64	22
Portugal	0.64	23
Hong Kong SAR, China	0.63	24
Singapore	0.63	25
Spain	0.62	26
South Africa	0.62	27
Italy	0.61	28
Georgia	0.61	29
Slovenia	0.60	30
Bosnia and Herzegovina	0.59	31
Indonesia	0.58	32
Croatia	0.58	33
Macedonia, FYR	0.57	34
Botswana	0.57	35
Greece	0.57	36
India	0.57	37
Brazil	0.56	38
Colombia	0.56	39
Nepal	0.56	40
Ghana	0.56	41
Mexico	0.56	42
Ukraine	0.56	43
Argentina	0.56	44
Panama	0.55	45
Moldova	0.55	46
Peru	0.55	47
Belize	0.55	48
Bulgaria	0.54	49
Philippines	0.54	50
Romania	0.53	51
Sri Lanka	0.53	52
Dominican Republic	0.52	53
Albania	0.52	54
Senegal	0.52	55
Hungary	0.51	56
Jamaica	0.51	57
El Salvador	0.51	58
Tunisia	0.51	59
Morocco	0.51	60
Serbia	0.51	61
Tanzania	0.51	62
Ecuador	0.51	63
Kyrgyzstan	0.50	64
Malawi	0.50	65
Honduras	0.49	66
Russia	0.49	67
Thailand	0.49	68
United Arab Emirates	0.48	69
Guatemala	0.48	70
Liberia	0.48	71
Zambia	0.48	72
Bangladesh	0.47	73
Madagascar	0.47	74
Mongolia	0.46	75
Jordan	0.46	76
Nigeria	0.46	77
Belarus	0.46	78
Kenya	0.46	79
Bolivia	0.45	80
Lebanon	0.45	81
Turkey	0.45	82
Pakistan	0.45	83
Nicaragua	0.44	84
Kazakhstan	0.44	85
Vietnam	0.43	86
China	0.43	87
Malaysia	0.43	88
Afghanistan	0.43	89
Burkina Faso	0.43	90
Egypt	0.42	91
Uganda	0.41	92
Cote d'Ivoire	0.40	93
Ethiopia	0.39	94
Cameroon	0.39	95
Sierra Leone	0.39	96
Venezuela	0.38	97
Cambodia	0.36	98
Iran	0.35	99
Myanmar	0.32	100
Uzbekistan	0.32	101
Zimbabwe	0.32	102

Figura 3.4: Open Government Around the World (World Justice Project)

delle armi per togliere dal mercato la (nuova) concorrenza e per consolidare posizioni semi-monopolistiche a scapito del cliente; in campo software non sono riconosciuti dappertutto e in ogni caso limitatamente a determinati contesti (invenzioni non puramente software), ma c'è molto *lobbying* per estenderne l'applicazione. Qualora questa spinta lobbistica dovesse avere successo probabilmente assisteremmo alla morte del mondo dello sviluppo software molto fervente e variegato[37] come lo conosciamo oggi... per assistere alla nascita di oligopoli del software controllati da enormi aziende.

- **Copyright** [Ali12] **sempre più lungo** vs. "pirateria"; un po' come succede per i brevetti, il copyright nasce con intento positivo e degenera nel corso della storia diventando per lo più un ostacolo all'accesso alla conoscenza e alla ricerca, in particolar modo quando viene esteso ed utilizzato massivamente per: *paywall* (su notizie e pubblicazioni scientifiche), DRM (si veda in sezione "*La computing agency rubata*" - 3.1.4), proposte di estensione temporale esagerate (e.g., 100 anni dalla morte dell'autore) o tecnicamente assurde (vedi sotto, direttiva EU 2019-2020).
- **La nuova direttiva EU**[38] che: 1) imporrà tasse sui *link con citazione* che impatteranno sui clienti finali; 2) costringerà le piattaforme di gestione dei media (es. youtube, vimeo ecc.) a dotarsi di filtri sui contenuti pressoché impossibili da realizzare. Ciò potrebbe elevare a dismisura il tasso di relatività a livello servizi perché molte piattaforme potrebbero semplicemente decidere di negare agli utenti EU contenuti altrimenti disponibili al resto del mondo.

[37] Solo GitHub conta più di 100 milioni di progetti software.

[38] Si veda *http://eff.org/deeplinks/2019/03/european-copyright-directive-what-it-and-why-has-it-drawn-more-controversy-any* e *http://cnbc.com/2019/05/10/youtube-faces-existential-threat-from-the-eus-new-copyright-directive.html*

- la recentissima[39] proposta inserita nel decreto-legge 30 aprile 2020, n. 28 che vorrebbe imporre agli ISP (e/o ai produttori di device connessi in rete) un **filtro anti-porno attivo di default** (salvo richiesta di disabilitazione da parte dell'utente); normativa assurda e inapplicabile su vari piani concettuali e tecnici:
  - Chi decide quali sono i contenuti non appropriati?
  - Come viene implementata tecnicamente?
  - Il blocco è per sito (filtro DNS aggirabile?) o per singolo media? Se viene filtrato il contenuto si degenera in **censura**[40].
  - Con la crittografia[41] come si relaziona? (vogliamo abolire la crittografia per poter esaminare i possibili contenuti pornografici?!? cfr. poco sotto)
  - Quasi certamente inoltre viola le normative europee sulla *Net Neutrality* (cfr. sezione "*Net Neutrality*" - 2.4.2).
- **HADOPI (*Haute Autorité pour la Diffusion des Œuvres et la Protection des droits d'auteur sur Internet*)**[42], una norma tuttora in vigo-

[39] Si vedano le notizie:
- *http://repubblica.it/economia/2020/06/19/news/filtro_automatico_al_porno_su_internet_ecco_la_norma_firmata_lega-259545443*
- *http://ilgiornale.it/news/cronache/filtro-automatico-porno-su-internet-lega-firma-norma-1871547.html*

E si sappia che tentativi analoghi a livello internazionale sono ampiamente falliti (*http://techdirt.com/articles/20190331/14283541915/uk-government-misses-another-ship-date-porn-filter.shtml*).

[40] Si veda il recentissimo blocco del sito del progetto Gutenberg *http://www.repubblica.it/tecnologia/2020/06/09/news/oscurata_la_piu_antica_libreria_digitale_wikimedia_inaccettabile_-258783839*

[41] Pregasi notare che ormai quasi tutto il traffico web (e probabilmente anche quello non-web) viaggia su *HTTPS* dove la "S" sta per "*secure*", crittografato, non leggibile salvo che dall'interessato.

[42] *http://en.wikipedia.org/wiki/HADOPI_law*

re (sebbene modificata in senso depenalizzante) in Francia: quando fu introdotta prevedeva la disconnessione automatica, a cura dell'*ISP* 🕮, di un utente che fosse stato *scoperto*[43] a condividere materiali protetti da copyright, senza possibilità per l'utente stesso di difesa presso alcun tipo di ente giudiziario o arbitrale.

- **TPP (*Trans Pacific Partnership*)**[44], trattato internazionale proposto da 11 stati (tra cui USA), ma per fortuna poi non ratificato: composto da 5600 pagine, già questo rappresentava un ostacolo alla conoscibilità, era stato tenuto segreto fino agli ultimissimi stadi di negoziazione e prevedeva, tra l'altro, modifiche molto pesanti del copyright allungandone la durata e imponendo agli stati firmatari una forte penalizzazione degli illeciti nonché l'obbligo di implementare meccanismi di DRM (*Digital Restriction Management*).
- **ACTA (*Anti Counterfeiting Trade Agreement*)**[45], trattato internazionale proposto ma non ratificato: anche in questo caso segretato durante il processo di stesura, toccava in particolare il tema della protezione del copyright a scapito della libertà di parola e della privacy delle comunicazioni.
- **TTIP (*Transatlantic Trade and Investment Partnership*)**[46], ancora un trattato in discussione[47], sempre a processo segretato, con impatto su vaste aree del commercio ma soprattutto nel contesto del *copyright enforcement*, tanto da essere definito una *resurrezione dell'ACTA*).

[43] Si intende, mediante monitoraggio continuo e pervasivo del traffico di rete.

[44] *http://eff.org/issues/tpp*

[45] *http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement*

[46] *http://en.wikipedia.org/wiki/Transatlantic_Trade_and_Investment_Partnership#Criticism_and_opposition*

[47] Pare lasciato decadere nel 2019, nel senso che probabilmente non riprenderanno i negoziati.

- **SOPA (*Stop Online Piracy Act*)**[48], una proposta di legge USA per imbavagliare qualunque sito fosse stato *colto* a diffondere materiale senza licenza materiale protetto da copyright. Se fosse stata approvata le sanzioni per violazione del diritto d'autore sarebbero state esacerbate a dismisura, prevedendo perfino l'oscuramento di un intero sito[49] colto a diffondere illecitamente anche un singolo artefatto. Per nostra fortuna, ma anche in virtù della mobilitazione mondiale[50] che vide perfino l'organizzazione di uno *sciopero dei siti web* (fra i *big* aderì Wikipedia), la legge non fu approvata.
- **CISPA (*Cyber Intelligence Sharing and Protection Act*)**[51], proposta di legge USA volta a legalizzare il monitoraggio pervasivo (mediante "accordi" con i *big player*) del traffico Internet per scovare e sgominare gli "attacchi *cyber*" violando nel contempo privacy e libertà civili degli utenti. Dopo discussi passaggi parlamentari è stata in lasciata decadere a favore di **CISA (*Cybersecurity Information Sharing Act*)**[52], purtroppo altrettanto liberticida.
- **PIPA (*PROTECT IP Act*)**[53], acronimo contenente un acrostico[54], ennesima proposta di legge USA per *combattere* il *copyright infringement* mediante oscuramento generalizzato[55] di siti e piattaforme.

[48] *http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act*

[49] Pensiamo a storage eterogenei come youtube o vimeo, non al "sitarello del ragazzino".

[50] La legge sarebbe stata applicata a qualunque piattaforma situata (*hosted*) nel territorio USA, ma gli effetti nefasti di oscuramento si sarebbero propagati in tutta Internet.

[51] *http://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act*

[52] *http://en.wikipedia.org/wiki/Cybersecurity_Information_Sharing_Act#Civil_liberties_groups*

[53] *http://en.wikipedia.org/wiki/PROTECT_IP_Act*

[54] PROTECT sta per "*Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act*".

[55] Non chirurgico: un singolo contenuto in violazione avrebbe permesso l'oscuramento di tutta la piattaforma.

- **DMCA (*Digital Millennium Copyright Act*)**[56]: legislazione USA adottata con principi analoghi anche in Europa come EUCD. Si tratta di norme negativamente impattanti sul mondo della tecnologia, prevedono una forte criminalizzazione di chi studi, realizzi e divulghi tecniche di aggiramento delle tecnologie di protezione del copyright, anche se queste non vengono effettivamente utilizzate per *copyright infringement* (violazione). Sul "divulgare", metaforicamente parlando sarebbe come rendere illegali le voci enciclopediche dei funghi velenosi o dell'acido muriatico.
- periodicamente vengono proposte un po' in tutto il mondo varie leggi **anti-anonimato in rete**... una per tutti il nostro primato italiano: la proposta Carlucci che nel 2009 stravinse il Big Brother Award[57] "Bocca a stivale" e "Minaccia da una vita". Al di là dell'impossibilità tecnica di realizzare tale tipo di tecnologia - identificare l'autore di ogni singolo bit che circola in rete - non si capisce quale sia l'utilità pratica se non il raggiungimento di quel controllo totale dei contenuti, quindi quasi dei pensieri, che qualche politico talvolta auspica.
- con la stessa frequenza del punto precedente vengono proposte a livello internazionale (in questo caso la fanno da padrone USA e UK) varie **leggi anti-crittografia** - lo scopo è quello di rendere trasparenti, almeno allo Stato, tutte le comunicazioni in rete, allo scopo **dichiarato** di *prevenzione del crimine* - in varie forme:
  1. rendere illegale crittografia con chiavi *troppo lunghe*[58].
  2. rendere illegale ogni tipo di crittografia che non preveda una *super-chiave* (in possesso dello Sta-

[56] *http://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act*

[57] *http://bba.winstonsmith.org/bbai2009.html*

[58] Una chiave lunga rende più difficile e lungo il lavoro di decrittazione a *forza bruta*.

to) per la decrittazione *alla bisogna* (*on demand*). Al di là del tipo di tecnologia alla quale ci si rivolge l'idea stessa di indebolire i meccanismi crittografici è sbagliata a vari livelli[59] perché non impedisce ai veri criminali di usare tecnologie illegali (quindi ad alta protezione della segretezza) e **contemporaneamente** espone i *law abiding citizens* (cittadini rispettosi della legge) ad eventuali abusi da parte di funzionari poco scrupolosi o di criminali che dovessero riuscire venire indebitamente in possesso di una eventuale *super-chiave*.

- per ultima citiamo una normativa **in vigore** molto meno dannosa[60] delle precedenti, ma che ha un sapore veramente amaro per come viene *venduta* da parte del mondo politico, parliamo del cosiddetto "**equo compenso**"[61]: un balzello di sapore *medievale* da pagare sui supporti di memorizzazione (*un tanto al mega*). Ideato per compensare i titolari dei diritti di copyright che, secondo i proponenti della normativa, altrimenti non verrebbero retribuiti qualora tali supporti venissero usati per "copiare illecitamente materiale coperto da diritti d'autore". Cioè si decide di punire *a pioggia* un po' tutti gli utenti per eventuali illeciti commessi da una piccola percentuale degli utenti stessi, preventivamente! Un po' come il famoso[62] proverbio cinese "Quando torni a casa picchia tua moglie, tu non sai perché ma lei sì"; l'*equo* compenso di *equo* non ha nulla, è solo l'ennesima follia, purtroppo non solo italiana, per estrarre denaro dalle tasche dei contribuenti[63].

[59] *http://eff.org/deeplinks/2014/09/nine-epic-failures-regulating-cryptography*

[60] Colpisce le nostre tasche, non le nostre libertà.

[61] *http://it.wikipedia.org/wiki/Equo_compenso_in_Italia*

[62] Ma anacronistico e assurdo, sia chiaro.

[63] Si veda qualche articolo di Scorza dell'epoca:

- *http://ilfattoquotidiano.it/2014/07/23/copia-privata-caro-franceschini-ci-ripensi-anche-apple-la-smentisce*
- *http://ilfattoquotidiano.it/2014/07/05/copia-privata-ecco-le-nuove-tasse-su-pc-e-smartphone-fino-a-20-*

3.1.3 *Code is law!*

Lawrence Lessig[64] nel 1999 scrisse un libro (qui[65] un articolo che lo riassume) che consideriamo pietra miliare di un ragionamento che proponiamo e ampliamo qui. Iniziamo con la dichiarazione di apertura di Lessig:

> *Every age has its potential regulator, its threat to liberty. Our founders feared a newly empowered federal government; the Constitution is written against that fear.*

Traduciamo liberamente: "Ogni era ha i suoi 'regolatori'[66] e le sue minacce alla libertà. I nostri fondatori temevano un governo troppo potente e la nostra Costituzione è scritta in modo da impedirlo."

Poi prosegue con:

> *Ours is the age of cyberspace. It, too, has a regulator. This regulator, too, threatens liberty. But so obsessed are we with the idea that liberty means 'freedom from government' that we don't even see the regulation in this new space. We therefore don't see the threat to liberty that this regulation presents.*

Traduciamo ancora: "La nostra è l'era del cyberspazio. Anch'esso ha un regolatore che minaccia la libertà. Ma siamo così ossessionati dall'idea che la libertà significhi 'libertà dal governo' che non vediamo nemmeno le regole di questo nuovo spazio e non ne vediamo la minaccia alla libertà che rappresenta."

Ed ecco il nucleo del suo *caveat*:

euro-per-un-hard-disk

[64] Probabilmente noto ai più come l'inventore delle licenze Creative Commons, ma anche esimio accademico e attivista politico, è un fervente propugnatore dell'alleggerimento delle leggi sul copyright.

[65] *http://harvardmagazine.com/2000/01/code-is-law-html*

[66] I poteri di uno stato di diritto: amministrativo, legislativo e giudiziario.

> *This regulator is code: the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned. It affects who sees what, or what is monitored. In a host of ways that one cannot begin to see unless one begins to understand the nature of this code, the code of cyberspace regulates.*

Ultima traduzione: "Questo 'regolatore' è il **codice**: il software e l'hardware che rendono il cyberspazio così com'è. Questo codice, o architettura, stabilisce i termini in cui si vive la vita nel cyberspazio. Determina quanto sia fattibile proteggere la privacy o quanto sia fattibile censurare il diritto di espressione del pensiero. Determina se l'accesso alle informazioni è generale o se le informazioni sono suddivise in zone[67]. Influenza il 'chi vede cosa' e cosa viene monitorato. In una moltitudine di modi che non si può iniziare a vedere se non si inizia a capire la natura di questo codice, il codice del cyberspazio stabilisce le regole."

Lessig ci sta avvertendo: il software e l'hardware regolano il cyberspazio, ma noi aggiungiamo che ormai **il software regola il mondo intero**[68]! Cioè il cyberspazio non è più qualcosa di *relegato* alla Rete, molto distante e ininfluente sulla nostra vita di tutti i giorni. Cyberspazio e mondo reale sono ormai così strettamente interdipendenti che nessuno dei due può *regolarsi* come se l'altro non esistesse. Ormai ogni attività umana è supportata e spesso addirittura *regolata* da **artefatti** software. Al punto che la nostra stessa vita dipende da come viene scritto il software: un primo esempio famoso risale agli anni '80 del ventesimo secolo, coinvolse un macchinario per la cura contro il can-

[67] Non usa esplicitamente il termine *Relatività della Rete*, ma noi ora possiamo farlo.

[68] Molti, noi compresi, dicono: "everything is code".

cro, a causa di errata programmazione somministrò dosi eccessive di radiazioni ai pazienti *in cura*[69]. Allo stato attuale gli esempi di software che *regola* la vita umana sono diventati molteplici [ONe16]: dai sistemi per le decisioni sulle concessioni di mutui ai programmi che valutano la probabilità di recidiva per i criminali o "prevedono" i crimini fino ad arrivare ai meccanismi di *reputation* cinesi che attribuiscono **punteggi di cittadinanza**[70] attraverso cui *guadagnare* o **perdere** diritti.

Poi aggiunge che le regole del cyberspazio *stanno*[71] cambiando, in peggio. Da un luogo protettivo del *free speech* e delle libertà individuali si va verso una *prigione*[72] iper-controllata e normata dall'alto da governi e grandi aziende, spesso in accordo tra loro. In questa "prigione virtuale" ogni bit che fluisce è associato a chi lo trasmette in modo, quando va bene, da poterlo condizionare in ogni scelta che effettua - dal prodotto che acquista al partito che vota - oppure, quando va male, da imputargli eventuali illeciti[73] per comminargli sanzioni e *isolamento sociale*, o peggio rinchiuderlo in **carcere reale**, a seconda del grado di repressione vigente in ciascun regime.

Infine Lessig attribuisce all'architettura del TCP/IP una natura *protettiva* dell'anonimato e della libertà di parola e stampa, sancita dal Primo Emendamento della costituzione USA, ma ci avverte che l'architettura può cambiare, in meglio o in peggio, **basta riscrivere il software**. E per riscriverlo, o almeno per poter dire la propria su come andrebbe riscritto, va **compreso**.

A distanza di vent'anni, dall'alto - no, dal basso - del nostro "senno di poi", dopo Snowden e WikiLeaks, ci troviamo a dover dissentire a proposito della *presunta* caratte-

[69] *http://en.wikipedia.org/wiki/Therac-25*

[70] *http://espresso.repubblica.it/attualita/2019/01/15/news/il-rating-del-buon-cittadino-cosi-si-relizza-l-incubo-di-orwell-1.330495*

[71] Sempre nel 2000, ricordiamocelo.

[72] Nostro termine, pensando al Panopticon già citato in sezione "*Il Principio di Locard digitale*" - 0.3.

[73] Sempre più probabili viste le spinte legislative di cui sopra.

ristica protettrice del TCP/IP. Lessig scriveva che in principio le comunicazioni in rete erano anonime e non sottoposte ad alcun tipo di censura: in questo sposava una concezione *romantica* della storia di Internet, purtroppo oggi dimostratasi falsa. Come abbiamo visto nel capitolo "*Livello 0 [The Net]*" - 0 i meccanismi che consentono la de-anonimizzazione delle comunicazioni con il relativo tracciamento dei comportamenti in rete, la censura attraverso l'interruzione della trasmissione o alterazione del contenuto e il controllo del tipo di comunicazioni in corso per mezzo del *deep packet inspection* sono parte integrante dell'architettura di Internet fin dal suo concepimento e implementazione iniziali; anonimato e libertà di espressione - che sono due facce della stessa medaglia - non sono mai stati considerati importanti dai progettisti di Internet. Per correggere questi difetti *inglobati* nell'architettura, come abbiamo visto in sezione "*Riprogettare Internet*" - 0.5.3, occorre modificare opportunamente il software che la determina, correggendone gli errori **di fondo** a seguito di una approfondita analisi che tenga conto che anonimato e libertà di espressione devono essere protetti in modo robusto dall'architettura... questo richiede una discreta conoscenza *sufficientemente diffusa* e *trasversale*, quindi una adeguata cultura informatica... è qui che torniamo ad essere in accordo con Lessig: **la necessità di comprendere** che l'architettura digitale *ingloba norme* che ne determinano il funzionamento, attraverso *il codice*.

Il software, il codice, non decide da solo come gestire l'informazione, sono le persone, in particolare gli sviluppatori, a deciderlo. Chi scrive il codice decide l'architettura. Lessig[74] ci esorta a prendere parte allo sviluppo, ad avere un ruolo nelle scelte architetturali, a non lasciarle solo agli sviluppatori che altrimenti, dice, "sceglieranno i valori fondamentali per noi". Non lasciamo che il divario tecnologico tagli fuori noi cittadini dal controllo e dalle scelte.

Noi naturalmente ci sentiamo di prendere posizione a

[74]Che in questo articolo *non* prende una posizione esplicita tra *more regulation* e *less regulation*.

favore di una Rete *neutra*, decentralizzata, che garantisca l'anonimato e la segretezza delle comunicazioni, implementata con algoritmi totalmente trasparenti[75] e meno controllabile possibile da *altri*.

Ma la lezione utile per questo capitolo è l'esortazione di Lessig a non delegare le scelte politiche in merito alla tecnologia, perché la Rete e il software che la regola sono una parte fondamentale della nostra Cittadinanza Digitale, sono l'ossigeno di una parte molto importante delle nostre relazioni sociali: quelle *digitalizzate*.

Dobbiamo quindi comprendere, "conoscere per deliberare" [Ein55], "programmare o essere programmati" [Rus10].

3.1.4 La *computing agency* rubata

Per l'ultima minaccia esterna, la più pesante e impattante, torniamo alla tecnologia parlando di come non solo ci vengano mascherate le sue funzionalità (sezione "*Tecnologia mascherante*" - 3.1.1), ma ci venga proprio impedito di controllare ciò che *possediamo* (o che crediamo di possedere).

Cosa intendiamo con *CA (Computing Agency)*? La CA è l'insieme dei *device* che **esegue computazioni e azioni**:

- in nostra vece e su nostra richiesta (a volte implicita, ma comunque sotto la nostra responsabilità);
- su richiesta di altri ma con impatti su di noi.

Facciamo il nostro solito esempio banale: quando mettiamo una pietanza in un forno e lo accendiamo impostando un timer di spegnimento, gli stiamo delegando la funzione di contare il tempo correttamente. Se però si brucia la cena la responsabilità è nostra. Certo, possiamo fare causa al produttore se riteniamo si tratti di un malfunzionamento, ma è solo una rivalsa, gli ospiti potranno forse comprendere, ma rimarranno comunque delusi.

Il forno è un oggetto semplice, ma non tutti gli oggetti lo sono, non al giorno d'oggi.

[75] Si veda sezione "*Software Libero*" - 3.4.1 più avanti.

Come già detto all'inizio di questo capitolo, stiamo assistendo da anni alla corsa a "mettere Internet in tutte le cose" [Man18]. Mettere Internet non vuol dire solo *connettere*, è più un eufemismo giornalistico per indicare l'implementazione di un qualche tipo di "intelligenza" e **autonomia** negli oggetti che ci circondano.

Un'auto che decide per conto suo di frenare improvvisamente[76], un termostato intelligente[77] che ascolta le conversazioni in appartamento e ne invia il contenuto al cloud del costruttore (Google), un *ebook reader* che cancella dal device dell'utente, su ordine del venditore, un libro assieme alle note aggiunte durante la lettura[78], una bambola Barbie che registra e invia al produttore tutto ciò che i bambini dicono[79].

Ogni oggetto dotato di un processore specie se connesso alla rete, è una minaccia potenziale **se, beninteso, non siamo noi a conoscerlo, configurarlo e controllarlo completamente**.

E purtroppo la tendenza è nella direzione sbagliata, verso una progressiva **perdita di controllo** sull'insieme dei device, sulla nostra *Computing Agency*. In "*The internet of things we don't own?*" [Sch16] (*Internet of Things* che **non** possediamo) viene delineato un quadro negativo: una pletora crescente di oggetti autonomi di cui noi siamo solo

[76] Honda HRV del 2019 di uno degli autori, frena da sola improvvisamente entrando in una rotonda se rileva un altro veicolo che "taglia la strada" (in realtà è lontano e non si avrebbe collisione o, peggio, è semplicemente di fianco - ad es. un motorino - ma viene rilevato dai sensori come "davanti"), in più di un'occasione è stato sfiorato l'incidente (tamponamento da dietro, perfino con un autobus). La concessionaria è a conoscenza del problema (segnalato da molti utenti), ma **nemmeno i tecnici ufficiali possono disabilitare** quel pericoloso comportamento automatico.

[77] Il già citato Nest, oltre a imparare le nostre abitudini, è stato scoperto a **origliare** tramite un microfono non dichiarato dal produttore (*http://edition.cnn.com/2019/02/20/tech/google-nest-microphone-secret/index.html*).

[78] *http://io9.gizmodo.com/amazon-secretly-removes-1984-from-the-kindle-5317703*

[79] *http://theguardian.com/technology/2015/mar/13/smart-barbie-that-can-listen-to-your-kids-privacy-fears-mattel*

utenti nel migliore dei casi, mentre nel peggiore diventiamo noi stessi il bersaglio da osservare per carpire informazioni "utili" a fini commerciali e di monitoraggio degli "illeciti" già citati nei capitoli precedenti.

Il tutto implementato attraverso *software proprietario* (si veda sezione "*Software Libero*" - 3.4.1) che implementa la cosiddetta "filiera del DRM (*Digital Rights Management*)"[80]: un insieme di meccanismi tecnologici che impediscono ad un computer di far funzionare software o hardware (con a bordo meccanismi software) che non sia stato approvato dal produttore o di utilizzare i propri contenuti multimediali in modi differenti rispetto a quanto *approvato* dal produttore, ad esempio impedendo la stampa[81] di un testo o porzioni di esso. Il DRM impedisce al "possessore"[82] di sostituire il software di un device con un altro di suo gradimento o di usufruire pienamente dei contenuti legalmente acquistati: l'oggetto diventa una scatola chiusa, le cui chiavi sono in mano al produttore e non all'acquirente.

L'estremo è rappresentato perfettamente nella contrapposizione "John Deere vs. resto del mondo"[83], tutt'ora in corso, che ha dato enorme spunto al movimento *right to repair*[84]. John Deere produce macchine agricole, è stata una delle prime case produttrici a sfruttare a fondo il *Digital Restriction Management* rendendo impossibile il *servicing* (manutenzione, riparazione) in proprio dei suoi prodotti. Gli agricoltori infatti, e con sgomento, si sono man mano accorti dell'impossibilità di effettuare le riparazioni sul campo perché i "loro" veicoli, pesantemente controllati da centraline completamente opache, vere e proprie *black box*, impediscono ogni tipo di misurazione e configurazione a "estranei" - ovvero a chi non possiede i certificati critto-

[80] Meglio noto come DRM (*Digital Restriction Management*).

[81] Si pensi anche alla stampa in Braille per i ciechi.

[82] Tra virgolette proprio a enfatizzare lo svuotamento del ruolo legato al verbo *possedere*.

[83] *http://foxnews.com/tech/tractor-hack-farmers-are-harnessing-hacked-software-for-john-deere-repairs*

[84] *http://repair.org*

grafici per accedere a quei device - non esplicitamente autorizzati, ovviamente i "proprietari" dei veicoli **non sono autorizzati**. Riprenderemo questo tema in sezione "*Right to repair*" - 3.4.2.

Discorso analogo per la quasi totalità degli smartphone: essi non sono "nostri" se non possiamo gestirli a nostro piacimento… e non possiamo farlo finché non ci appropriamo dei *diritti di root* (potere di amministrare il device)[85], facoltà che è negata salvo *arzigogoli* tecnici non alla portata di tutti i "proprietari" e che nella maggior parte dei casi fa decadere la garanzia sull'apparecchio[86]. L'impedimento viene *venduto* ***formalmente*** *nell'interesse dell'utilizzatore*, ma in realtà ha il malcelato scopo di impedire che il telefono venga effettivamente controllato appieno da chi ha comprato l'oggetto e lo vorrebbe gestire a suo piacimento. E cosa mai non si potrà fare senza questi fantomatici *diritti di root*? Guarda caso **non** si può:

- impedire ad una *app* di connettersi alla rete;
- impedire ad una *app* di raccogliere informazioni arbitrarie;
- bloccare la pubblicità;
- in generale diventa molto complicato verificare e tenere sotto controllo il comportamento delle varie *app* che si installano sul device e di cui quindi bisogna fidarsi ciecamente.

Molti produttori di telefoni e di *app* arrivano all'assurda demonizzazione della procedura di *rooting* tanto da avvisare l'utente quando rilevano che una simile operazione è stata effettuata: viene considerato *pericoloso* (per chi?) possedere il proprio device, cfr. figura 3.5 che mostra il messaggio visualizzato dalle *app* **Ufficio Postale** (a SX) e **Zoom** (a DX) quando rilevano che l'apparato è *rooted*. E in questo caso siamo fortunati che poi l'*app* funziona normalmente, molte altre *app*, ad esempio quelle di moltissime banche, si **rifiutano** di funzionare nelle medesime condizioni[87].

[85] *http://en.wikipedia.org/wiki/Rooting_(Android)*

[86] Anche se la validità legale di queste clausole contrattuali è decisamente dubbia e fortemente contestata.

[87] Tanto che esistono software appositi (e.g., Magisk - *http://*

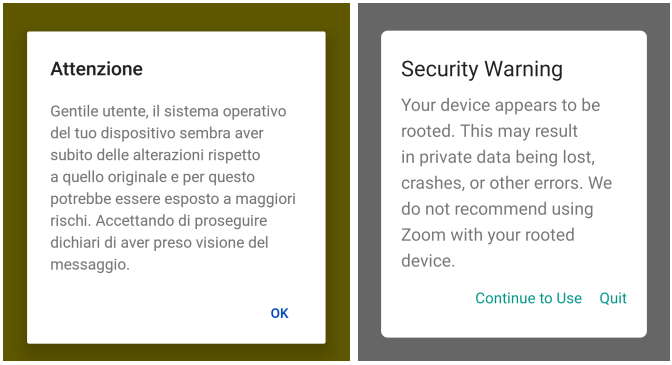


Figura 3.5: È pericoloso possedere il proprio device...

In sostanza stiamo assistendo ad un progressivo *shift* (spostamento) dell'*agency* dal possessore del device verso *altri*, determinando in questo modo un **limitato permesso d'uso**, dove non è nemmeno sempre chiaro il "chi usa chi": si passa da *to own agency* (poter agire) a *to be owned by agency* (essere soggetti a agire altrui). Esempio dell'estremismo verso cui sta andando il mondo è il recente annuncio di una "tecnologia" BMW[88] per attivare o disattivare (a pagamento, ovviamente) vari servizi sulla *propria* autovettura: i sedili si riscalderanno solo se avrete pagato l'abbonamento al servizio, il sistema di guida avanzato idem. Una nuova definizione di *proprietà*[89] e un **futuro distopico che noi non vogliamo**.

Quello che abbiamo raccontato fin qui descrive appunto "*Un mondo minaccioso?*" - 3.1, a cui ora possiamo togliere il punto di domanda, che sta pian piano[90] **rubando la nostra *Computing Agency*** e, se la colleghiamo al concetto del "*Code is law!*" - 3.1.3, si potrebbe dire che con essa ci viene "rubata" anche la possibilità di partecipazione ad

magisk.me) che implementano una sorta di *gabbia* che impedisce ad alcune *app* di rilevare la condizione *rooted*.

[88] *http://cnet.com/roadshow/news/bmw-vehicle-as-a-platform*

[89] Ogni volta che leggete dei termini di *marketing* "As a Service" o "As a Platform" dovreste alzare il sopracciglio.

[90] Ma nemmeno tanto lentamente...

una piena cittadinanza. Si fa credere al cittadino che deve prendere le *cose* (oggetti, device, servizi, architetture ecc.) così come *date*, senza discuterle o tentare di sottoporle ad *hacking*[91]; nella maggior parte dei casi il cittadino subisce, per difetto di conoscenza, per "pigrizia"[92] o per mancanza di *coraggio critico*. Ma il nostro **vero Cittadino Digitale** è colui il quale ha piena coscienza e possibilmente, nei limiti delle sue forze[93], controllo della propria *Computing Agency*.

3.2 Il cittadino inconsapevole

Il Cittadino **è pronto**? È Digitale? Purtroppo temiamo di **no** e ci sentiamo di affermare che la strada da fare è ancora molto lunga e tortuosa, infatti il cittadino:

- ritiene poco importante l'accesso alla connettività e ancor di più risulta poco sensibile ai temi citati finora quali *relatività* e *monitoraggio invasivo*;
- non possiede o non ritiene fondamentale la conoscenza in merito alle tecnologie, specie quelle legate al mondo ICT (*Information and Communication Technologies*);
- anche quando acquisisce conoscenza lo fa superficialmente pur ritenendosi spesso un *esperto*.

Prima di analizzare questi temi, permettete un *primo acchito* esemplificativo di impatto, una notizia[94] (con rela-

[91] *http://en.wikipedia.org/wiki/Hacker_culture*

[92] Non in senso spregiativo, ci rendiamo perfettamente conto che fronteggiare tutte le minacce che abbiamo descritto non è banale, costa fatica mentale e fisica. Perfino gli autori di questo testo a volte alzano bandiera bianca.

[93] O in quelle delle varie *community* che ruotano intorno a questi temi: la forza del *crowd* (della massa).

[94] Si vedano i seguenti:

- *http://corrierecomunicazioni.it/pa-digitale/il-giudice-si-appella-alle-orecchiette-e-blocca-il-processo-digitale*
- *http://www.anailatina.it/2016/04/non-si-trattava-di-bufala-perche-al-giudice-piacciono-proprio-le-orecchiette-a-rettifica-di-quanto-prima-detto-sulla-*

tiva immagine, figura 3.6) che, come si suol dire: "ha fatto il giro del web". Un giudice italiano, nel 2016, motiva la sua *necessità* di avere copie **stampate su carta** dei documenti relativi ad una causa con l'impossibilità di "apporre orecchiette allo schermo o sottolinearlo"! Con buona pace dei migliori propositi di arrivare al vero e proprio "processo telematico" e ignorando totalmente l'esistenza di fior di tecnologie per l'annotazione di documenti digitali. E i giudici sono persone che rivestono ruoli importanti, devono appunto giudicare, ma purtroppo sono spesso poco aggiornati e legati ad un mondo molto *analogico-cartaceo* in perenne ritardo sulla digitalizzazione. Se ne accorgono anche all'estero [Kir14] osservando che, soprattutto quando si dibatte di temi ad alta tecnologia (e.g., nelle *litigation* tra imprese), spesso il giudice non capisce nemmeno lontanamente l'argomento su cui deve deliberare, al punto estremo da non riuscire ad interloquire con i periti.

Veniamo ora ai tre temi fondamentali.

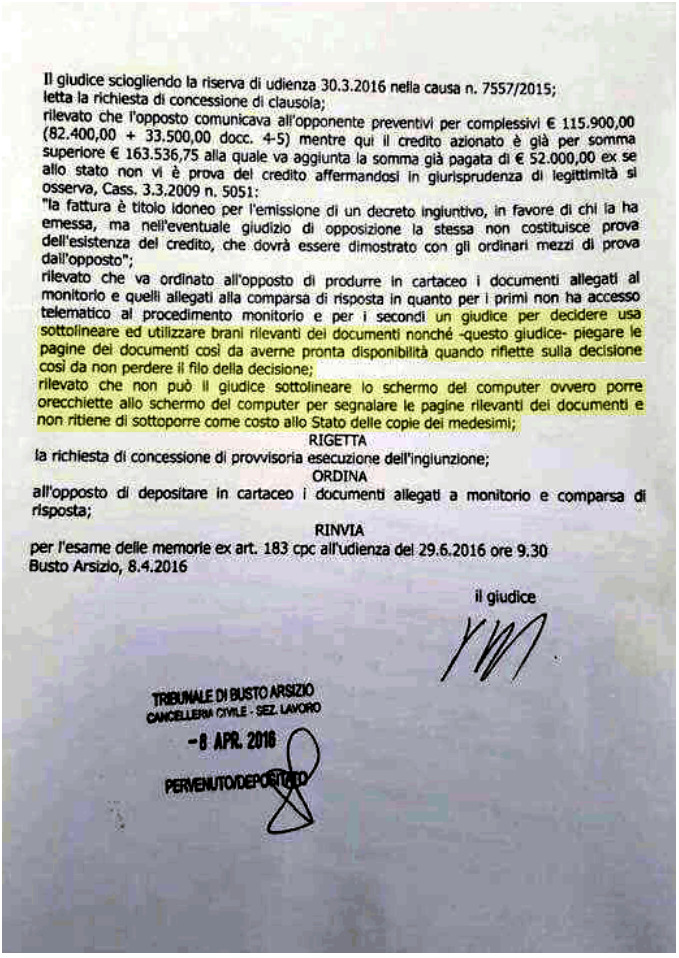
3.2.1 Il *digital divide* non tecnologico

```
- ``Ma da te arriva la rete a
banda larga?'' - ``Sì, ma
non mi importa.''
```

Ispirato a una scena di "Kentucky Fried Movie" (John Landis, 1977 - http://youtube.com/watch?v=IqDKOibnGbE)

In sezione "*Digital divide*" - 2.4.1 abbiamo trattato il c.d. *digital divide* inteso come *tecnologico*, che divide il territorio nazionale in chi è raggiunto da cablaggio ad alta velocità (fibra, VDSL e copertura telefonica di ultima generazione) e chi invece ha a sua disposizione solo connessioni più lente (ADSL o peggio ISDN).

ordinanza-del-tribunale-di-busto-arsizio-in-tema-di-processo-telecart



Il giudice sciogliendo la riserva di udienza 30.3.2016 nella causa n. 7557/2015;
letta la richiesta di concessione di clausola;
rilevato che l'opposto comunicava all'opponente preventivi per complessivi € 115.900,00 (82.400,00 + 33.500,00 docc. 4-5) mentre qui il credito azionato è già per somma superiore € 163.536,75 alla quale va aggiunta la somma già pagata di € 52.000,00 ex se allo stato non vi è prova del credito affermandosi in giurisprudenza di legittimità si osserva, Cass. 3.3.2009 n. 5051:
"la fattura è titolo idoneo per l'emissione di un decreto ingiuntivo, in favore di chi la ha emessa, ma nell'eventuale giudizio di opposizione la stessa non costituisce prova dell'esistenza del credito, che dovrà essere dimostrato con gli ordinari mezzi di prova dall'opposto";
rilevato che va ordinato all'opposto di produrre in cartaceo i documenti allegati al monitorio e quelli allegati alla comparsa di risposta in quanto per i primi non ha accesso telematico al procedimento monitorio e per i secondi un giudice per decidere usa sottolineare ed utilizzare brani rilevanti dei documenti nonché -questo giudice- piegare le pagine dei documenti così da averne pronta disponibilità quando riflette sulla decisione così da non perdere il filo della decisione;
rilevato che non può il giudice sottolineare lo schermo del computer ovvero porre orecchiette allo schermo del computer per segnalare le pagine rilevanti dei documenti e non ritiene di sottoporre come costo allo Stato delle copie dei medesimi;

RIGETTA

la richiesta di concessione di provvisoria esecuzione dell'ingiunzione;

ORDINA

all'opposto di depositare in cartaceo i documenti allegati a monitorio e comparsa di risposta;

RINVIA

per l'esame delle memorie ex art. 183 cpc all'udienza del 29.6.2016 ore 9.30
Busto Arsizio, 8.4.2016

il giudice

TRIBUNALE DI BUSTO ARSIZIO
CANCELLERIA CIVILE - SEZ. LAVORO
-8 APR. 2016
PERVENUTO/DEPOSITATO

Figura 3.6: Orecchiette allo schermo?!?

Il fatto, su cui si ha ben poco controllo, di essere o meno raggiunti dall'alta velocità si deve però sposare con la **volontà** di connettersi.

Purtroppo, recenti analisi[95] mostrano che una gran parte della popolazione italiana, si parla di milioni di famiglie, pur raggiunta dalla banda larga, si *accontenta*[96] di velocità minori di 10 Mbps o addirittura decide di non abbonarsi proprio ad un servizio di connettività *landline*, indipendentemente dalla velocità disponibile, adducendo mancanza di utilità o dichiarando più che sufficiente la connettività a disposizione attraverso la rete dati 3G o 4G (cellulare).

Il già citato (nel capitolo "*Livello 2 [access]*" - 2) DESI[97] conferma questa situazione di **rinuncia digitale** soprattutto per l'Italia, indietro di parecchi punti percentuali (69% contro 81%) rispetto alla media europea della popolazione connessa.

Anche in tema di *differenze di genere* ITU ha riscontrato[98] a livello mondiale una distanza importante tra uomini e donne nell'accesso alla connettività e nella scelta di materie tecnologico-informatiche. Parliamo di circa dieci punti percentuali, in larga misura nelle aree meno sviluppate del pianeta.

Per essere molto chiari: non riteniamo **affatto** che questo tipo di *digital divide sociale* sia *connaturato* nelle categorie di persone che lo **subiscono**, le ragioni di queste differenze derivano senza dubbio da una complessa serie di *condizioni ambientali* e *rapporti di potere* in atto nelle diverse culture e nei diversi sistemi economici. Si tratta di argomenti molto ampi e che esulano da quello che tratteremo in questo volume.

[95] *http://agendadigitale.eu/cultura-digitale/il-digital-divide-culturale-e-una-nuova-discriminazione-sociale*

[96] Potrebbe essere una scelta dettata dalla disponibilità economica (*http://corrierecomunicazioni.it/digital-economy/si-allarga-il-digital-divide-meta-della-popolazione-mondiale-e-ancora-offline*), ma per fortuna il rapporto velocità/prezzo diventerà man mano meno dirimente, a tendere si osserverà sempre meno differenziazione di prezzo in funzione della velocità di navigazione.

[97] *http://ec.europa.eu/digital-single-market/en/desi*

[98] *http://itu.int/en/mediacentre/Pages/2019-PR19.aspx*

3.2.2 Deficit di conoscenza

Ci stiamo domandando se il nostro cittadino è digitale o meno… iniziamo con l'impietoso (per l'Italia) quadro descritto dal DESI 2020[99] di cui mostriamo un'immagine significativa in figura 3.7[100] e di cui riportiamo il seguente:

> *L'anno scorso si è registrato un miglioramento sia delle competenze degli utenti di Internet (almeno delle competenze digitali di base) sia delle competenze avanzate (laureati e specialisti in Information and Communication Technologies). Nel 2019, la percentuale di persone che hanno almeno competenze digitali di base ha raggiunto il 58% (rispetto al 55% nel 2015). Gran parte della popolazione dell'UE, tuttavia, manca ancora di competenze digitali di base, anche se la maggior parte dei lavori richiede tali competenze. Nel 2018, circa 9,1 milioni di persone hanno lavorato come specialisti ICT in tutta l'UE, 1,6 milioni più di 4 anni prima. Tuttavia, permane una carenza di specialisti ICT sul mercato del lavoro: il 64% delle grandi imprese e il 56% delle PMI che hanno assunto specialisti ICT nel 2018 hanno riferito che i posti vacanti per gli specialisti ICT sono difficili da colmare. Il problema è ancora più diffuso in Romania e in Repubblica Ceca, dove almeno l'80% delle imprese che hanno reclutato o cercato di assumere specialisti ICT ha riferito di tali difficoltà. Esiste anche un problema di equilibrio di genere in quanto solo uno su sei specialisti ICT sono donne. Nel complesso, nella dimensione del capitale umano del DESI, Finlandia, Svezia ed Estonia sono le più avanzate.*

[99] *http://ec.europa.eu/digital-single-market/en/human-capital*

[100] Capitale umano digitale, il rettangolo indica media EU mentre quello con gli spigoli arrotondati evidenzia l'Italia.

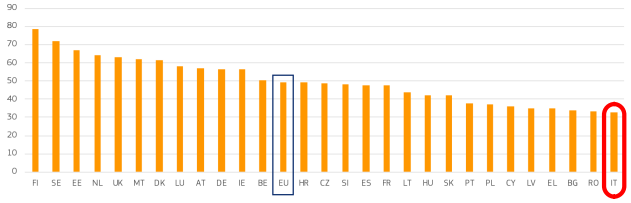


Figura 3.7: DESI 2020, capitale umano (digitale)

Il DESI ci comunica quindi una tendenza positiva generale, ma, come si può notare in figura, l'Italia è all'**ultimo posto** in Europa.

Negativamente interessante anche la nostra posizione per quanto riguarda i servizi digitali[101]: **siamo terzultimi nell'uso** a fronte di avere a disposizione tutto sommato una discreta offerta di servizi digitali[102] dato che siamo a dieci posizioni dal fondo classifica per disponibilità degli stessi.

Scontiamo una notevole arretratezza culturale storica che dobbiamo colmare e i fievoli segnali che si vedono non bastano a stare al passo coi tempi. Nel 2013[103] ancora il 40% delle famiglie (soprattutto al sud Italia) non disponevano di una connessione a Internet. Nel 2015[104] una percentuale *elevata* (11%) di giovani tra gli undici e i diciassette anni non aveva mai mai usato Internet, specie al sud[105], mentre il 17% di loro credeva che Internet fosse di Bill Gates[106], tanto per fare qualche esempio.

[101] *http://ec.europa.eu/digital-single-market/en/use-internet*

[102] *http://ec.europa.eu/digital-single-market/en/digital-public-services-scoreboard*

[103] Rapporto "Cittadini e nuove tecnologie" (ISTAT 2013) *http://www.istat.it/it/archivio/108009*.

[104] Rapporto IPSOS (Save The Children) 2015 *http://repubblica.it/solidarieta/cooperazione/2015/02/06/news/save_the_children-106682455*.

[105] L'Italia è molto divisa anche dal punto di vista tecnologico.

[106] Anche se non ci sono andati molto lontano in effetti, Internet resta sotto il controllo di pochi enti.

Anche fuori dal contesto tecnologico siamo carenti. Ad esempio nella *lettura dei libri*: il rapporto[107] stato editoria Italia 2017 (Ufficio studi AIE) su dati del 2016, ci dice che il 58% degli italiani legge meno di un libro annuo, nella classe dirigente la quota si situa sul 38.6% e tra i laureati sul 25%.

Un ente che viene citato spesso è OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico)[108] che periodicamente pubblica statistiche in ambito *misurazione della conoscenza*, ad esempio attraverso il "Programma per la valutazione internazionale dello studente", i risultati del programma ci collocano intorno a metà classifica[109].

Ne "Le cause dell'analfabetismo digitale italiano"[110] del 2014, partendo dal rapporto "Noi-Italia"[111] che ISTAT compila ogni anno, veniva descritto un quadro disastroso per l'Italia patologicamente arretrata sul piano della cultura[112] tecnologica. *In primis* troviamo una definizione interessante di alfabetizzazione (grassetto nostro):

> *Il focus … è sul versante dell'alfabetizzazione digitale, intesa come* ***acquisizione delle competenze digitali di base, necessarie per una piena cittadinanza (digitale)****. Questa è esattamente la stessa definizione che ritroviamo per l'alfabetismo funzionale. Non a caso.*

Successivamente nell'articolo vengono definiti due tipi di **(an)alfabetismo tecnologico**[113]:

[107] *http://www.aie.it/Cosafacciamo/Pubblicazioni/Scoprilapubblicazione.aspx?IDUNI=1ef0zdli0hl4lgbnabou2psj68026&MDId=10655&Skeda=MODIF306-53-2017.10.11*

[108] *http://oecd.org*

[109] *http://www.roars.it/online/le-fake-news-di-presa-diretta-sulla-scuola-italiana*

[110] *http://agendadigitale.eu/infrastrutture/le-cause-dell-analfabetismo-digitale-italiano*

[111] *http://noi-italia.istat.it*

[112] Dal punto di vista delle infrastrutture e investimenti relativi invece ci posizioniamo di solito un po' meglio degli ultimi.

[113] Usiamo però i nostri termini dato che non amiamo *analfabeti-*

- quello **operativo**, cioè del "saper usare", del "saper cliccare sulle icone" (senza capire cosa c'è sotto);
- e quello **meta-operativo** che ci fa conoscere e capire cosa c'è "sotto al cofano"[114] e ci stimola a comprendere i processi, anche i nostri stessi processi di apprendimento.

Infine, sempre in "Le cause dell'analfabetismo digitale italiano", viene utilizzato come *proxy* dell'alfabetismo l'uso sistematico della rete, delineando la situazione seguente:

- chi non ha mai utilizzato Internet = 37% nella popolazione 6-75 anni;
- chi utilizza Internet sporadicamente = 13% sulla popolazione 6-75 anni;
- chi ha utilizzato Internet recentemente ma non è in grado di utilizzare i servizi più comuni (interazione con PA, home banking, pagamenti elettronici) = 24% della popolazione 6-75 anni;
- chi utilizza Internet anche per i servizi più comuni = 26% della popolazione 6-75 anni.

L'Italia è purtroppo sistematicamente e storicamente arretrata [DG11; Eur15] su entrambi i fronti dell'alfabetismo (informatico e digitale), scontiamo (rispetto agli altri paesi UE):

- mancanza di competenze e abilità in generale (**analfabetismo funzionale**, precursore di quello *operativo* e del *meta-operativo*);
- mancanza di interesse per la cultura scientifica e tecnologica [For18]
- infrastrutture carenti (cfr. sezione "*Digital divide*" - 2.4.1);
- mancanza ecosistemi tecnologici (simil Silicon Valley, MIT/Harvard, LSE) [For18];
- interessi economici contrari che *remano contro* gli investimenti sull'innovazione della rete[115];

smo informatico e *analfabetismo digitale*, non veicolano la corretta semantica.

[114] Letteralmente dall'inglese "under the hood".

[115] Ma dal 2011 di "*I nemici della rete*" [DG11] a oggi forse gli atteggiamenti, anche sulla scorta di qualche spinta dal basso, stanno

- una classe dirigente mediamente analfabeta digitale, che frena per non sentirsi sorpassata;

Anche i fin troppo mitizzati *nativi digitali*[116] descritti da Prensky, cioè i nati *assieme alle tecnologie* (circa dopo il 1985), sono spesso meno *savvy* [Bau09] (cioè **comprendono meno**) e pure "lost in navigation", citiamo da "*Studenti, computer e apprendimento: dati e riflessioni*" [Toz+15]:

> *Negli ipertesti gli studenti italiani sono "lost in navigation". Altro dato riferito all'Italia da valutare con attenzione è che quando gli studenti usano Internet per svolgere compiti scolastici dimostrano di non saper pianificare bene ed eseguire una ricerca, né dimostrano di saper valutare l'utilità di una informazione o l'attendibilità delle fonti.*

Come conferma anche Fuggetta in "*Cittadini ai tempi di Internet: Per una cittadinanza consapevole nell'era digitale*" [Fug18]: "i nativi digitali sono in realtà molto meno 'maturi digitali' di quanto immaginiamo", bisogna **superare l'uso, l'addestramento**, serve un salto di qualità nei modelli cognitivi e comportamentali.

L'AICA (Associazione Italiana per l'Informatica e il Calcolo Automatico) ci descrive infatti un paradosso[117]: "Il termine 'nativo digitale' suggerisce **falsamente** come i giovani intuitivamente sappiano usare le tecnologie digitali. Questo termine perpetua una percezione sostenuta da alcuni genitori, insegnanti e politici e porta all'omissione dai programmi scolastici di materie volte a sviluppare competenze digitali."

Infine, forse un po' meno paradossalmente, perché in effetti era la categoria peggio messa, dall'altro estremo ri-

lentamente cambiando.

[116] *http://it.wikipedia.org/wiki/Nativo_digitale*

[117] *http://www.aicanet.it/-/nativi-digitali-analfabetismo-che-non-ti-aspetti*

spetto ai *nativi digitali*, troviamo gli **anziani**, coloro che più si sono evoluti[118] nel corso degli ultimi dieci anni.

3.2.3 La conoscenza acritica

> `Non credete a tutto ciò che leggete su Internet.`
>
> *Abraham Lincoln (1809-1865)*

Nel bellissimo libro di Nichols "*La conoscenza e i suoi nemici. L'era dell'incompetenza e i rischi per la democrazia*" [NV18] viene ben descritta la crisi della competenza nell'era di Internet: l'enorme disponibilità di informazione praticamente in tempo reale che abbiamo, letteralmente, nelle nostre mani - il cellulare - sta demolendo il concetto di *esperto*: "perché affidarvi a persone con istruzione e esperienza superiori alle vostre quando potete ottenere da soli quell'informazione?". Il problema è che anche oggi è perfettamente attuale la:

Legge di Sturgeon

Il 90% di ogni cosa è spazzatura.

Sturgeon la coniò negli anni cinquanta per giudicare la produzione letteraria cartacea, ma secondo Nichols quando questa legge viene applicata al materiale disponibile in Internet quel *90%* è addirittura **molto ottimistico**. Questo perché è molto facile per **chiunque** "buttar fuori qualcosa in Internet": pubblicare un sito web è un'operazione semplice ed economica[119] ergo ad oggi si incontrano *miliardi* di siti dei quali solo alcuni *milioni* contengono effettivamente informazioni sensate e veritiere, il resto è *fake* (falso) o semplicemente opinione *da bar*. Purtroppo, inoltre, a volte certe "informazioni", le c.d. *fake news*, vengono costruite

[118] *http://avvenire.it/agora/pagine/internet-anziani-connessi*

[119] Qualche decina di euro annui.

e messe lì a bella posta per influenzare le scelte, politiche e non, dei cittadini, si veda ad esempio il caso "Cambridge Analytica" [Kai19]: dati personali di milioni di utenti Facebook rivenduti e utilizzati per fare *micro-targeting politico*, cioè informazione costruita su misura per piccoli gruppi ben identificati di potenziali elettori.

Se a questo aggiungete che, complice la *relatività a livello servizi* (cfr. sezione "*Relatività a livello servizi*" - 1.2.1), quando consultate un *motore di ricerca* vi viene restituito un *set* di pagine che si adatta al vostro *bias culturale* [SL16] e che lo stesso motore di ricerca non ha alcun interesse a valutare la veridicità dei risultati che vi fornisce[120], ecco che avete perso molte possibilità di scremare i milioni dai miliardi.

L'effetto finale che otteniamo è una sorta di pandemia di *effetto Dunning-Kruger*[121]: condizione che si applica a chiunque[122] e fa credere al soggetto in questione di conoscere un argomento molto più di quanto ne sappia realmente, in particolare la relazione è prevalentemente *inversa*, meno so più credo di sapere.

Questa pandemia porta parecchie persone a credere *fino alla morte* alle "cure alternative" per le malattie, a ritenere pericolosi i vaccini o il 5G, a non credere agli allunaggi delle missioni Apollo ecc.

L'unica medicina contro il *Dunning-Kruger* è il **pensiero critico**: l'abilità di affrontare le affermazioni sia analizzandole per come sono formulate sia confrontandole con proprie conoscenze (che ci devono essere) per valutarne la veridicità senza prendere tutto ciò che si legge per *oro colato* ("Certo che è sicuro, l'ho letto su Google!"). Se, come è vero, per l'editoria *non-fiction* tradizionale esiste la "fuffa" (i.e., materiale non verificato) a maggior ragione il discorso vale su Internet, proprio per la facilità con cui si possono creare contenuti e divulgarli.

[120] Basta che clicchiate sulla pubblicità.

[121] *http://it.wikipedia.org/wiki/Effetto_Dunning-Kruger*

[122] Autori di questo testo inclusi.

Quindi ci servirebbe, in rete, ancora più attenzione che nel cartaceo, ma purtroppo si osserva una tendenza contraria, frutto forse della voglia di combattere il bombardamento informativo cui siamo sottoposti. Purtroppo in "*Does the internet make us stupid?*" [Mau14] e in "*The Dumbest Generation: How the Digital Age Stupefies Young Americans and Jeopardizes Our Future (or, Don't Trust Anyone Under 30)*" [Bau09] viene fornito un quadro desolante:

- lettura superficiale (c.d. *skimming*), cioè quella pratica per cui si legge solo qualche parola ogni tanto credendo di poter carpire comunque il significato del testo;
- riduzione delle abilità cognitive: incapacità di comprendere un testo, di cogliere la struttura ecc.;
- contenuto frammentato (es. ipertesti) che non aiuta a concentrarsi;
- ecosistema di c.d. *interruption technologies*: fare più cose[123] in parallelo credendo di riuscire a seguirle tutte;
- copia e incolla che assopisce il pensiero creativo e che conferisce poca consapevolezza su ciò che si sta producendo;
- basso livello di attenzione;
- perdita della capacità di concentrazione;
- *esternalizzazione* della conoscenza verso il *cloud*: "perché devo ricordarmelo se posso cercarlo in rete?".

Ultima ma non meno importante esortazione: fate vostra e cercate di comprendere il significato recondito della frase in epigrafe di questa sezione.

3.3 Difese istituzionali

Per affrontare un mondo digitale che può rappresentare una minaccia se non ben gestito, quali strumenti ci offrono le istituzioni? Quali misure vengono proposte e attuate "dall'alto"? Di che qualità sono tali iniziative?

[123] Es. gestire più chat contemporanee mentre si segue una lezione e si sta leggendo un testo a video su un argomento diverso.

Iniziamo col dire che per fortuna il problema è *istituzionalmente* sentito e in qualche modo affrontato. A supporto utilizzeremo alcuni estratti della "*Raccomandazione del Consiglio relativa alle competenze chiave per l'apprendimento permanente*" [EU18] che descrivono gli intendimenti dell'UE (Unione Europea).

> *Il pilastro europeo dei diritti sociali sancisce come suo primo principio che ogni persona ha* ***diritto a un'istruzione****, a una formazione e a un apprendimento permanente di qualità e inclusivi, al fine di mantenere e acquisire competenze che consentono di* ***partecipare pienamente alla società*** *e di gestire con successo le transizioni nel mercato del lavoro.*

↗ Si riconosce il diritto all'istruzione, che deve essere continua e di livello elevato e adeguato[124] al mantenimento del grado di partecipazione nella società.

> *Le competenze richieste oggi sono cambiate: più posti di lavoro sono automatizzati, le* ***tecnologie svolgono un ruolo maggiore in tutti gli ambiti del lavoro e della vita quotidiana*** *e le competenze imprenditoriali, sociali e civiche diventano più importanti per assicurare resilienza e capacità di adattarsi ai cambiamenti.*

↗ Concordiamo col testo UE nel riconoscere il grande impatto che le tecnologie, soprattutto - aggiungiamo noi - digitali, hanno su ogni aspetto della vita.

> *Nel contempo, indagini internazionali quali il Programme for International Student Assessment (PISA) dell'Organizzazione per la cooperazione e lo sviluppo economici (OCSE) o*

[124] Almeno, meglio se si può migliorare.

> *il programma per la valutazione internazionale delle competenze degli adulti (PIAAC) dell'OCSE indicano che una quota costantemente elevata di adolescenti e adulti dispone di* ***competenze di base insufficienti****. Nel 2015 uno studente su cinque aveva gravi difficoltà nello sviluppo di competenze sufficienti in lettura, matematica e scienze. In alcuni paesi fino a un terzo degli adulti possiedono competenze alfabetiche e aritmetico-matematiche solo ai livelli più bassi. Il 44% della popolazione dell'Unione possiede competenze digitali scarse, e il 19% nulle.*

↗ Come detto in sezione "*Il digital divide non tecnologico*" - 3.2.1, misuriamo tuttora un certo *distanziamento* fra conoscenze possedute e complessità del mondo che ci circonda, qui sopra evidenziato nei contesti tradizionali, ma ancor più evidente nel campo delle tecnologie, digitali in particolare.

> *Nell'economia della conoscenza, la memorizzazione di fatti e procedure è importante, ma non sufficiente per conseguire progressi e successi. Abilità quali la* ***capacità di risoluzione di problemi, il pensiero critico, la capacità di cooperare, la creatività, il pensiero computazionale, l'autoregolamentazione*** *sono più importanti che mai nella nostra società in rapida evoluzione. Sono gli strumenti che consentono di sfruttare in tempo reale ciò che si è appreso, al fine di sviluppare nuove idee, nuove teorie, nuovi prodotti e nuove conoscenze.*

↗ Abbiamo descritto analogamente il problema della conoscenza *meta-operativa* in sezione "*Deficit di conoscenza*" - 3.2.2, mentre sul pensiero critico forniamo la nostra posizione concorde in sezione "*La conoscenza acritica*" - 3.2.3.

Inoltre preghiamo il lettore di ricordare il paragrafo citato qui sopra quando leggerà la sezione "*Learn to code*" - 3.4.3.

> *Innalzare il livello di padronanza delle competenze di base (alfabetiche, matematiche e **digitali**) e sostenere lo sviluppo della capacità di **imparare a imparare** quale presupposto costantemente migliore per apprendere e partecipare alla società in una prospettiva di apprendimento permanente;*

↗ Qui ci si concentra sul tema delle competenze *digitali* in particolare e, di nuovo, su quello delle competenze meta-operative.

> *Promuovere l'acquisizione di competenze in **scienza, tecnologia, ingegneria e matematica (STEM)**, tenendo conto dei collegamenti con le arti, la creatività e l'innovazione, e motivare di più i giovani, **soprattutto ragazze e giovani donne**, a intraprendere carriere STEM;*

↗ Oltre a rimarcare l'importanza delle STEM vediamo per la prima volta il tema *gender* che abbiamo citato in sezione "*Il digital divide non tecnologico*" - 3.2.1.

> *Promuovere lo sviluppo di competenze in materia di **cittadinanza** al fine di rafforzare la consapevolezza dei valori comuni enunciati nell'articolo 2 del trattato sull'Unione europea e nella Carta dei diritti fondamentali dell'Unione europea.*

↗ Viene citata la "cittadinanza", senza però associarla mai a "digitale", cosa che invece noi proponiamo.

> *Promuovendo molteplici approcci e contesti di apprendimento, anche **con l'uso opportuno delle tecnologie digitali**, nell'istruzione, nella formazione e nell'apprendimento;*

↗ E infine interessante questo punto in cui si propongono competenze digitali *da raggiungere attraverso* le stesse, una sorta di *circolo virtuoso* che si autoalimenta.

Tra gli **allegati** del "*Raccomandazione del Consiglio relativa alle competenze chiave per l'apprendimento permanente*" [EU18], ne troviamo in particolare uno che definisce quali sono le **competenze chiave** necessarie al cittadino, di cui evidenziamo quelle che ci interessano particolarmente:

- competenza alfabetica funzionale
- competenza multi-linguistica
- competenza matematica e competenza in **scienze, tecnologie e ingegneria**
- **competenza digitale**
- competenza personale, sociale e **capacità di imparare a imparare**
- competenza in materia di **cittadinanza**
- competenza imprenditoriale
- competenza in materia di consapevolezza ed espressione culturali

Vediamo e commentiamo ora, sempre tramite estratti, corredati di grassetti nostri, qualche dettaglio su quelle da noi evidenziate come importanti.

> *Le persone dovrebbero saper applicare i principi e i processi matematici di base nel contesto quotidiano, nella sfera domestica e lavorativa (ad esempio in ambito finanziario) nonché seguire e vagliare concatenazioni di argomenti. Le persone dovrebbero essere in grado di svolgere un ragionamento matematico, di comprendere le prove matematiche e di comunicare in linguaggio matematico, oltre a saper usare i sussidi appropriati, tra i quali i dati statistici e i grafici, nonché di* ***comprendere gli aspetti matematici della digitalizzazione****.*

↗ Non nascondiamo il nostro entusiasmo nel leggere quel "aspetti matematici della digitalizzazione" perché, pur in

maniera molto sintetica, esprime lo stesso intento che permea il nostro testo.

> *Per quanto concerne scienze, tecnologie e ingegneria, la conoscenza essenziale comprende* ***i principi di base del mondo naturale, i concetti, le teorie, i principi e i metodi scientifici fondamentali, le tecnologie e i prodotti e processi tecnologici****, nonché la comprensione dell'impatto delle scienze, delle tecnologie e dell'ingegneria, così come dell'attività umana in genere, sull'ambiente naturale. Queste competenze dovrebbero consentire alle persone di* ***comprendere meglio i progressi, i limiti e i rischi delle teorie, applicazioni e tecnologie scientifiche nella società*** *in senso lato (in relazione alla presa di decisione, ai valori, alle questioni morali, alla cultura ecc.).*

↗ Qui ritroviamo quello che noi abbiamo identificato nella voglia di vedere "*under the hood*", inoltre si cita il comprendere le conseguenze delle tecnologie sulla società che è alla base della *Cittadinanza Digitale e Tecnocivismo.*

> *Tra le abilità rientra la* ***comprensione della scienza in quanto processo di investigazione mediante metodologie specifiche, tra cui osservazioni ed esperimenti controllati, la capacità di utilizzare il pensiero logico e razionale per verificare un'ipotesi, nonché la disponibilità a rinunciare alle proprie convinzioni se esse sono smentite da nuovi risultati empirici****. Le abilità comprendono inoltre la* ***capacità di utilizzare e maneggiare strumenti e macchinari tecnologici nonché dati scientifici per raggiungere un obiettivo o per formulare una decisione o conclusione sulla base di dati probanti****. Le persone*

> *dovrebbero essere anche in grado di riconoscere gli aspetti essenziali dell'indagine scientifica ed essere capaci di comunicare le conclusioni e i ragionamenti afferenti.*

↗ Molto interessanti questi passaggi perché implicano, pur senza indicare esplicitamente, la lotta contro il pensiero a-critico e le *fake news* e, ancora più importante, l'uso di tecnologia e dati scientifici[125] per migliorare la nostra conoscenza del mondo.

> *La competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali* ***(inclusa la programmazione)****, la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cibersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il* ***pensiero critico****.*

↗ Di nuovo il "*Learn to code*" - 3.4.3 e il pensiero critico come *presupposti* alle competenze digitali.

> *Le persone dovrebbero essere in grado di utilizzare le tecnologie digitali come* ***ausilio per la cittadinanza attiva e l'inclusione sociale, la collaborazione con gli altri e la creatività nel raggiungimento di obiettivi personali, sociali o commerciali****. Le abilità comprendono la capacità di utilizzare, accedere a, filtrare, valutare, creare, programmare e condividere contenuti digitali. Le persone dovrebbero*

[125] Approfondiremo gli *opendata* 🕮 quando tratteremo il Livello 4 [*transparency*].

> *essere in grado di gestire e proteggere informazioni, contenuti, dati e identità digitali, oltre a riconoscere software, dispositivi, intelligenza artificiale o robot e interagire efficacemente con essi.*

↗ E qui un *mix* di CDT con la parte superiore della piramide di Maslow.

> *Per la competenza in materia di* ***cittadinanza*** *è indispensabile la capacità di impegnarsi efficacemente con gli altri per conseguire un interesse comune o pubblico, come lo sviluppo sostenibile della società. Ciò presuppone la capacità di pensiero critico e abilità integrate di risoluzione dei problemi, nonché la capacità di sviluppare argomenti e di partecipare in modo costruttivo alle attività della comunità, oltre che al processo decisionale a tutti i livelli, da quello locale e nazionale al livello europeo e internazionale. Presuppone anche la capacità di* ***accedere ai mezzi di comunicazione sia tradizionali sia nuovi, di interpretarli criticamente e di interagire con essi, nonché di comprendere il ruolo e le funzioni dei media nelle società democratiche****.*

↗ Infine, in questo paragrafo ci piace leggere finalmente un embrione di pensiero verso la *Cittadinanza Digitale* e *Tecnocivismo*.

Abbiamo preso da "*Raccomandazione del Consiglio relativa alle competenze chiave per l'apprendimento permanente*" [EU18] perché è una dichiarazione di intenti interessante e molto condivisibile, ma nel corso degli anni molte sono state le iniziative, sia a livello nazionale che internazionale.

Ad esempio in "*Introduzione dell'insegnamento scolastico dell'educazione civica*" [Dep19] troviamo l'articolo 5

dedicato alla "Educazione alla cittadinanza digitale" che dal titolo poteva far sperare bene, ma andando ad analizzare[126] i temi trattati dal testo in oggetto secondo l'Arcobaleno della CDT vediamo che lo spettrogramma risultante (figura 3.8) è carente su alcuni livelli:

- Livello 0 [*The Net*]: **assente**, non vengono trattate le distorsioni della Rete
- Livello 1 [*services*]: **molto trattato**, i servizi digitali sono ritenuti importanti
- Livello 2 [*access*]: **appena sfiorato**, non interessano digital divide, inclusività delle infrastrutture e più in generale i diritti di base della CDT
- Livello 3 [*education*]: **molto trattato**, questo picco era atteso, essendo un piano dedicato alla formazione
- Livello 4 [*transparency*], Livello 5 [*participation*] e Livello 6 [*consultation*]: **qualche accenno**, quindi si ritengono accettabili trasparenza e partecipazione, ma senza troppi obblighi[127]
- Livello 7 [*democracy*]: **assente**, non si discute del livello più alto della partecipazione civica

Vediamo spesso spettrogrammi analoghi, con i livelli partecipativi *deboli*, e non è un caso: i livelli alti **fanno paura**, l'ascolto è *pericoloso* perché poi bisogna dare seguito alle richieste della cittadinanza.

A livello internazionale è famoso il piano di investimenti USA "Computer Science for All" descritto in "*A Decade of ACM Efforts Contribute to Computer Science for All*" [Fis16]. Un piano ambizioso, alcuni miliardi di dollari, che dichiara come le *abilità digitali* non possano più essere considerate opzionali e prevede l'insegnamento dell'*informatica*[128] fin dalle elementari[129] e medie con laboratori *hands-on* ("mettici sopra le mani"), quindi non solo teoria. Inoltre prevede molta formazione degli insegnan-

[126] Il lavoro è stato fatto da un nostro tesista, Luca Messina, che ringraziamo.
[127] Siamo a livello di "contentino".
[128] Qui declinata in termini *meta-operativi*.
[129] Ovviamente con le dovute cautele e modelli formativi adeguati.

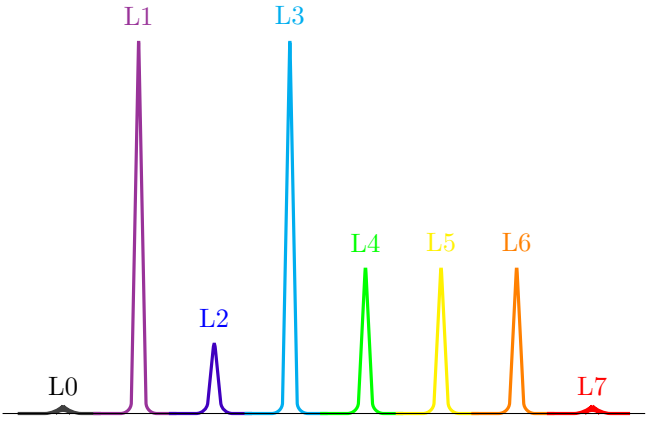


Figura 3.8: Spettrogramma abilità art.5

ti, cosa che qui in Italia ad esempio, proprio nel campo digitale, è stata introdotta molto tardi.

Cosa è stato fatto in Italia?

3.3.1 Le politiche per l'informatica a scuola dal 1985 ad oggi

Sono ormai quarant'anni che le "Tecnologie dell'Informazione e della Comunicazione" (TIC, come vengono chiamate nel mondo della scuola) condizionano ogni aspetto della società e ne influenzano lo sviluppo, rendendo più efficienti i processi e favorendo la creazione di nuovi prodotti e servizi. Mentre nelle attività economiche, nella pubblica amministrazione, Forze Armate, Ricerca ecc. l'approccio fisiologico è quello utilitaristico su come utilizzare al meglio l'informatica per il conseguimento dei propri fini (nuovi prodotti, maggiore efficienza, più sicurezza, progresso scientifico ecc.) l'obbiettivo che la Scuola dovrebbe porsi è quello peculiare alla sua missione istituzionale: "lo sviluppo di un approccio critico al mondo digitale" [Gui19].

Vedremo invece che i programmi di investimento e le iniziative di diffusione che si sono susseguite hanno riguar-

dato soprattutto l'*education technology*, anziché la *media education*, e che l'approccio tecno-centrico ha condizionato gli investimenti orientandoli - soprattutto all'inizio - verso l'acquisizione delle dotazioni strumentali (hardware e software) piuttosto che verso la formazione informatica degli insegnanti.

Infine si è perseguita la competenza digitale a scapito della consapevolezza, ma i confronti internazionali (vedi sezione "*Il digital divide non tecnologico*" - 3.2.1) sulla *information literacy* certificano un fallimento a cui solo l'ultimo PNSD (Piano Nazionale Scuola Digitale) sembra voler porre rimedio.

Il quadro normativo per le politiche sul digitale a scuola attualmente è costituito proprio dal PNSD (si veda prossima sezione "*Il Piano Nazionale Scuola Digitale*" - 3.3.2), l'ultima incarnazione di un'attenzione che la politica ha da sempre riservato al tema dell'utilizzo delle tecnologie informatiche nella scuola, elaborando strategie che riflettevano lo spirito dei tempi sia riguardo alle opportunità offerte dalla tecnologia, sia riguardo alle spinte culturali e ai condizionamenti ideologici.

La storia italiana è densa di iniziative, qui di seguito le principali[130]:

- **1985 - PNI - Piano Nazionale Informatica**
  Questa prima fase di introduzione delle tecnologie informatiche nella scuola si dà come obbiettivo l'utilizzo di strumenti informatici nell'insegnamento della matematica e della fisica anche attraverso la programmazione e l'implementazione di algoritmi. Le classi coinvolte sono quelle del primo biennio delle superiori. Vengono anche attivate sperimentazioni nei licei classici e scientifici e negli istituti tecnici commerciali, che si spingono fino alla programmazione (spesso utilizzando l'ambiente Turbo Pascal[131]).

[130] Per una trattazione esaustiva si rimanda a [Gui19] che dedica l'intero capitolo 2 al tema delle politiche per il digitale a scuola.
[131] *http://it.wikipedia.org/wiki/Turbo_Pascal*

- **1990 - PNI2**
  La prima metà degli anni '90 vede il diffondersi degli ipertesti, dei contenuti multimediali e delle reti (anche se in modalità pre-web rispetto a come lo conosciamo oggi). Nuovi modelli didattici come il *costruzionismo* influenzano la politica scolastica, e di conseguenza il ruolo del computer nel contesto educativo. Il secondo Piano Nazionale Informatica promuove l'utilizzo di ipertesti e la sperimentazione di connessioni telematiche ed estende l'ambito di applicazione alle discipline dell'area linguistico-letteraria delle superiori.
- **1997 - PSTD - Programma di Sviluppo delle Tecnologie Didattiche**
  Nel 1995, mentre il Web esce dal perimetro accademico e inizia la sua diffusione nella società, il Ministero della Pubblica Istruzione avvia i progetti pilota che condurranno al Programma di Sviluppo delle Tecnologie Didattiche 1997-2000. I contenuti del programma riflettono le opportunità tecnologiche (multimedialità, uso della Rete) e le suggestioni culturali del periodo: l'approccio costruttivista vede il computer come uno strumento per la costruzione di conoscenza e la condivisione di contenuti. L'ambito di applicazione viene esteso alle scuole elementari e medie.
- **2002 - For TIC - Piano Nazionale di Formazione degli Insegnanti sulle Tecnologie dell'Informazione e della Comunicazione**
  Il successivo intervento nasce in un contesto caratterizzato dal diffondersi di Internet nella società italiana, dalla elaborazione in sede europea della Strategia di Lisbona[132] che riconosce il ruolo fondamentale di istruzione e formazione per la crescita e lo sviluppo economico e dal nuovo ruolo assunto dai dirigenti scolastici per effetto della riforma sull'autonomia (i

[132] *http://archivio.pubblica.istruzione.it/buongiorno_europa/lisbona.shtml*

presidi *manager*). In questo clima culturale vengono coinvolti circa 180.000 docenti su un programma di formazione che finalmente affianca all'obbiettivo di garantire alle giovani generazioni le competenze informatiche anche quello di farne degli utenti consapevoli MIUR 2002, pag. 4[133]. Purtroppo a fronte di tanto slancio quel che resta è soprattutto la **ECDL (*European Computer Driving License*)**, la patente europea del computer presa a riferimento per la certificazione delle competenze digitali. Si tratta di una famiglia di certificazioni (in Italia amministrate da AICA[134] che dal 1995 ha soprattutto alimentato un'offerta formativa a livello poco più che *operativo*. Finché riguardano solo gli aspetti di "utilizzo", iniziative come l'ECDL (European Computer Driving License) e ECDL e-Citizen restano del tutto insufficienti a sostenere il processo di digitalizzazione di una nazione moderna.

- **2007 - PSD - Piano Scuola Digitale**
  Se negli anni '80 e '90 l'ambito delle TIC era soprattutto quello delle materie tecnico scientifiche (matematica, fisica, informatica) nel tempo c'è la tendenza a estenderlo alle altre materie, e questo approccio viene formalizzato nel Piano Scuola Digitale che introduce il concetto di *ambienti per la didattica* e finanzia l'adozione dello strumento in voga nel periodo: le LIM (Lavagna Interattiva Multimediale). Vengono inoltre avviati 3 progetti pilota: Cl@ssi 2.0, Scuole 2.0 e l'azione Editoria Digitale Scolastica. Il piano, per quanto utile per la diffusione delle attrezzature (soprattutto per il Mezzogiorno, che godrà anche del Piano Operativo Nazionale - PON 2007-13) si rivelerà tuttavia fragile sul piano degli obbiettivi pedagogici, come stigmatizzato dallo studio OECD 2013[135]

[133] *http://archivio.pubblica.istruzione.it/news/2002/allegati/linee_guida.pdf*
[134] *http://www.ecdl.it*
[135] *http://read.oecd-ilibrary.org/education/review-of-the-italian-strategy-for-digital-schools_5k487ntdbr44-en#page97*

che si conclude con le seguenti considerazioni:

> *L'introduzione di massa di apparecchiature TIC senza cambiamenti curricolari, pedagogici e, in definitiva, di valutazione che ristrutturano il lavoro di insegnamento, aggiunge semplicemente le TIC in cima a quello che attualmente è il lavoro "reale" degli insegnanti e crea resistenza. Come ha affermato un insegnante durante le interviste sul campo: "Inizia cambiando l'insegnamento, quindi l'attrezzatura necessaria".*

E per ultimo appare il PNSD (Piano Nazionale Scuola Digitale) che andiamo ad analizzare.

3.3.2 Il Piano Nazionale Scuola Digitale

Il PNSD (Piano Nazionale Scuola Digitale) è l'attuale risposta *dall'alto*, istituzionale, nazionale al problema descritto sopra nelle sezioni "*Un mondo minaccioso?*" - 3.1 e "*Il cittadino inconsapevole*" - 3.2.

Venne istituito nel 2015[136] nell'ambito dell'iniziativa "La Buona Scuola" dell'allora Primo Ministro Matteo Renzi. Oggi si possono trovare informazioni sulla pagina dedicata[137] al PNSD nel sito del Ministero dell'Istruzione. Il documento di progetto è disponibile in vari formati (PDF, ebook) e anche in inglese, qui faremo riferimento (anche per gli estratti) alla versione italiana[138].

Il PNSD è strutturato in *azioni* volte a risolvere i problemi strutturali e culturali della scuola italiana: viene complessivamente definito come "un'azione culturale e di sistema".

Queste *azioni* sono idealmente raggruppate nelle macroaree (tra virgolette gli estratti dal documento di progetto):

[136] *http://www.miur.gov.it/web/guest/scuola-digitale*
[137] *http://www.istruzione.it/scuola_digitale*
[138] *http://www.istruzione.it/scuola_digitale/allegati/Materiali/pnsd-layout-30.10-WEB.pdf*

- Strumenti = "condizioni di accesso, la qualità degli spazi e degli ambienti, l'identità digitale e l'amministrazione digitale"
- Competenze e contenuti = "serve identificare nuove traiettorie, guardando alle pressanti richieste del presente in termini di competenze, ma soprattutto interpretando quelle del futuro"
- Formazione = "formazione del personale, orientata all'innovazione didattica e aperta a quella organizzativa, sarà cruciale per fare uno scatto in avanti"
- Accompagnare nella sfida dell'innovazione = collegamento col territorio, monitoraggio del piano stesso, *steering* (governo)

Nell'introduzione viene descritta onestamente la situazione di partenza della scuola italiana come sub-ottimale, anche nel confronto con gli altri paesi della Unione Europea attraverso i dati OCSE. Inoltre viene presentata la storia delle iniziative precedenti facendone tesoro e impostando quindi il PNSD come **costitutivamente digitale**.

Il PNSD si occupa di molti aspetti della scuola, da quelli infrastrutturali a quelli contenutistici e vengono previsti anche meccanismi di monitoraggio e di governo *in itinere*, non è cioè un piano statico, ma dovrebbe adattarsi alla situazione contingente nel corso del tempo.

Per i contenuti e le competenze l'ispirazione è quella del *lifelong learning* (formazione continua) simboleggiata dalla figura 3.9 (a pagina 72 del documento di progetto, a sua volta proveniente da fonte *World Economic Forum* del 2013) che si basa su tre pilastri:

- nozioni di base, conoscenze
- competenze, pensiero critico, *problem solving*
- aspetti personali e sociali, interazione con altri e con situazioni fuori *confort zone*

Con gli studenti del corso di Cittadinanza Digitale e Tecnocivismo abbiamo "letto" la proposta del PNSD mediante una analisi *spettrografica CDT* per studiare quali livelli dell'Arcobaleno vengono affrontati dalle varie *azioni*.

Il processo è quello che utilizziamo solitamente per crea-

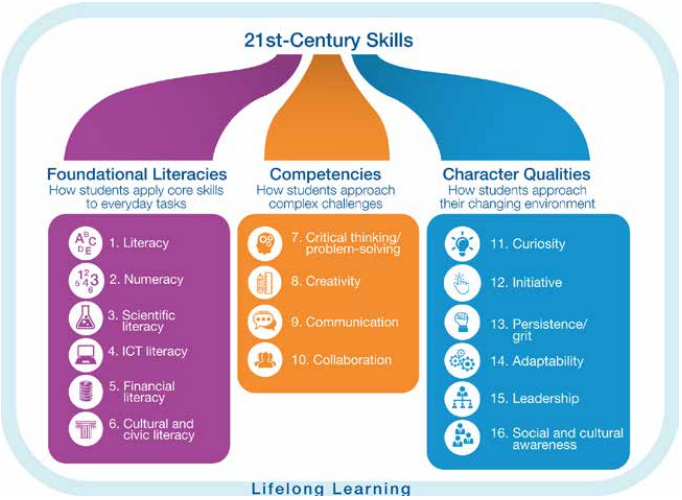


Figura 3.9: *Lifelong learning* in PNSD (dal documento di progetto)

re gli *spettrogrammi* che abbiamo mostrato finora, è un'analisi *qualitativa* che si basa sulla lettura *ragionata* del testo. Ogni azione del PNSD è stata esaminata da tutto il nostro gruppo (docenti e studenti) e per ognuna è stata concordata collegialmente (per discussione libera) una *tupla* di *pesi* che relazionano l'elemento con i livelli dell'Arcobaleno. Ad esempio una *tupla* $(0, 0, 0, 0, 0, 0, 0, 0)$ indica nessuna relazione con i livelli, una $(0, 0, 0.2, 0, 0, 0.8, 0, 0)$ indica un collegamento debole (20% di peso) con L2-access e forte (80%) con L5-participation e così via. La somma dei valori della *tupla* fa sempre 1.0 (i.e., 100%).

La tabella 3.1 mostra il risultato della nostra analisi per tutte le azioni del PNSD, ogni azione è legata, mediante un peso, ai livelli dell'Arcobaleno, la riga "Totali" in fondo alla tabella calcola le somme delle varie colonne.

Per rappresentare graficamente la relazione fra PNSD e Arcobaleno abbiamo generato lo *spettrogramma CDT* usando i valori della riga "Totali", il risultato è mostrato in figura 3.10.

Az.	Titolo	L0	L1	L2	L3	L4	L5	L6	L7
1	…banda ultra-larga…			1					
2	Cablaggio interno…			1					
3	Canone di connettività…			1					
4	… didattica digitale …		0.5	0.5					
5	Challenge Prize …							1	
6	…*Bring Your Own Device*			0.5	0.5				
7	… l'apprendimento pratico				1				
8	…Autenticazione unica…			1					
9	Un profilo … studente			1					
10	Un profilo … docente			1					
11	Digitalizzazione …		0.8	0.2					
12	Registro elettronico		0.8	0.2					
13	…"Dati della scuola"		0.2			0.8			
14	Un framework …				1				
15	Scenari innovativi…				0.6		0.2	0.2	
16	Una research unit …				0.6			0.3	0.1
17	…pensiero computazionale…				1				
18	Aggiornare il curricolo …				1				
19	…imprenditorialità …				0.6			0.4	
20	Girls in Tech & Science				1				
21	Piano Carriere Digitali				0.8			0.2	
22	… interoperabilità …		1						
23	…Risorse Educative Aperte…				0.6		0.2	0.2	
24	Biblioteche Scolastiche …			1					
25	Formazione …		0.3		0.7				
26	Assistenza tecnica …		0.8	0.2					
27	Rafforzare la formazione …				1				
28	Un animatore digitale …				0.6		0.2	0.2	
29	Accordi territoriali						0.2	0.8	
30	Stakeholders' Club …						0.2	0.8	
31	… raccolta di pratiche						0.5	0.5	
32	… ascolto permanente						0.2	0.8	
33	Osservatorio …					1			
34	…pratiche internazionali					0.2		0.8	
35	Il monitoraggio …					0.2	0.4	0.4	
	Totali →	0	4.4	8.6	11	2	1.7	6.2	0.1
		L0	**L1**	**L2**	**L3**	**L4**	**L5**	**L6**	**L7**

Tabella 3.1: Mappa 'azioni PNSD → livelli CDT'

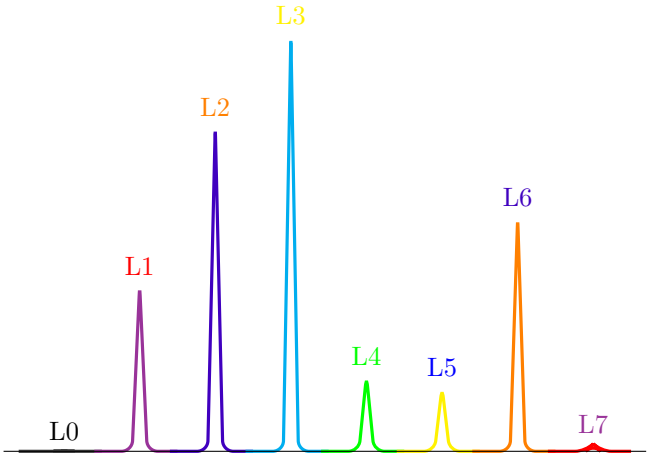


Figura 3.10: Spettrogramma del PNSD (generato usando i dati della tabella 3.1)

Dallo *spettrogramma* possiamo subito notare che:

- Livello 0 [*The Net*]: **assente**, non vengono prese in considerazione le distorsioni della Rete
- Livello 1 [*services*]: **abbastanza trattato**, i servizi digitali sono ritenuti importanti, giustamente
- Livello 2 [*access*]: **molto trattato**, finalmente si considerano molti servizi digitali come *di base*
- Livello 3 [*education*]: **estremamente trattato**, questo picco era atteso, essendo un piano dedicato alla formazione
- Livello 4 [*transparency*]: **lievemente considerato**, dichiarata l'esigenza di trasparenza, ma senza troppo impegno
- Livello 5 [*participation*]: **lievemente considerato**, non sono previste grandi attività sul tema
- Livello 6 [*consultation*]: **abbastanza trattato**, quindi si ritiene relativamente importante la partecipazione dal basso, l'*ascolto*
- Livello 7 [*democracy*]: **praticamente assente**, non si discute del livello più alto della partecipazione ci-

vica, cioè non sono stati previsti momenti formali di consultazione "impegnativa" (consulto sì, livello precedente, ma senza obbligo decisionale)

Le dolenti note

Lo *spettrogramma CDT* appena mostrato ci dice una prima cosa importante: la trasparenza sul PNSD stesso è un aspetto poco valorizzato, dichiarato ma forse solo "per dovere".

Un progetto di tale portata, oltre alle *finalità*, dovrebbe definire molto bene anche i *metodi di valutazione* dei risultati. Le misure si dovrebbero basare sui fattori che nel mondo anglosassone prendono il nome di KPI (*Key Performance Indicator*), ovvero gli *indicatori chiave*, preferibilmente quantitativo-oggettivi, che permettono di calcolare una "percentuale di completamento".

In effetti, nel documento di progetto del PNSD, ogni azione ha un *campo* "Obiettivi misurabili", anche se per alcune azioni (8 su 35) risulta non esplicitato; ecco riportato fedelmente l'elenco, con alcuni nostri commenti nelle parentesi quadre:

1. effettiva realizzazione degli interventi a favore delle scuole → [**non quantitativo, tautologico**]
2. cablaggio interno di tutte le scuole per un utilizzo più efficace delle dotazioni digitali; percentuale di copertura della rete infrastrutturale rispetto agli spazi scolastici (aule, laboratori, ecc.) → [**definizione non chiara**]
3. aumento del numero di scuole completamente connesse in Rete; potenziamento effettivo risparmio di spesa per la connettività delle scuole, monitoraggio delle modalità di approvvigionamento di connettività da parte delle scuole → [**difficilmente quantificabili**]
4. realizzazione degli interventi tramite monitoraggio Programma Operativo Nazionale; effettivo incremento della didattica digitale → [**non quantitativo, tautologico**]

5. realizzazione e distribuzione della soluzione individuata; risparmi di costo per la scuola → [**il primo dei due non è quantitativo**]
6. promozione di politiche BYOD (*Bring Your Own Device*) nelle scuole; risorse destinate a livello locale e regionale, anche attraverso finanziamenti dedicati; numero di studenti raggiunti da politiche attive → [**definizione non chiara, difficilmente quantificabile**]
7. numero di laboratori effettivamente potenziati, numero di laboratori "certificati" nel territorio, effettivo utilizzo dei laboratori, mappatura complessiva dei laboratori scolastici → [**non quantitativi o difficilmente quantificabili**]
8. effettiva razionalizzazione degli accessi e delle autenticazioni alle piattaforme MIUR → [**tautologico**]
9. copertura del numero di studenti raggiunti dallo strumento; quantità e qualità dei servizi associati al profilo digitale dello studente → [**il secondo è difficilmente quantificabile**]
10. copertura del numero di docenti raggiunti dallo strumento; servizi associati al profilo digitale del docente → [**il secondo è difficilmente quantificabile**]
11. copertura del servizio → [**tautologico**]
12. dotazione del 100% delle classi delle scuole primarie → [**è un obiettivo finale, non una misura del completamento**]
13. pubblicazione del portale; numero e qualità dei *data set* pubblicati → [**non quantificabile senza definire fattori di qualità**[139]]
14. revisione delle indicazioni nazionali; effettiva ricezione delle linee guida, documentata dall'inserimento nei Piano dell'Offerta Formativa e nei programmi di percorsi didattici coerenti; mappatura e certificazione delle competenze → [**non quantificabili**]
15. creazione e certificazione di almeno 20 format di percorsi didattici; effettiva diffusione dei percorsi nelle

[139]Saranno trattati in L4-transparency[140] dell'Arcobaleno

scuole e completamento da parte degli studenti; indicatori di impatto dei singoli percorsi → [**il primo è obiettivo finale, gli altri non sono quantificabili**]

16. apertura di nuove linee di ricerca; numero di progetti di ricerca realizzati o in corso; output dei progetti di ricerca → [**il primo è minimale, il terzo non è quantificabile**]
17. tutti gli studenti della scuola primaria praticano un'esperienza di pensiero computazionale nel prossimo triennio → [**non è una misurazione di completamento**]
18. livelli di apprendimento degli studenti → [**difficilmente quantificabile (forse via OCSE e simili)**]
19. numero di studenti coinvolti, complessivamente; numero di studenti per percorso; soluzioni sviluppate dagli studenti → [**l'ultimo è difficilmente quantificabile**]
20. numero di reti coinvolte, tasso di iscrizioni a discipline STEM fra 5 anni
21. creazione di percorsi sperimentali; numero di studenti in lauree STEM, in ingresso e in uscita → [**il primo è difficilmente quantificabile**]
22. incremento nell'utilizzo di contenuti e piattaforme digitali per la didattica → [**difficilmente quantificabile, troppo ampio**]
23. numero di istituzioni scolastiche che praticano l'autoproduzione, tipologia e qualità dei risultati → [**il secondo è difficilmente quantificabile**]
24. *NIL*
25. numero di docenti formati; indicatori di efficacia delle strategie territoriali, tra cui effettivo utilizzo delle tecniche apprese in classe e a livello di scuola → [**tranne il primo gli altri sono molto difficilmente quantificabili**]
26. effettiva copertura delle esigenze di assistenza tecnica delle scuole primarie e degli istituti comprensivi;

miglioramento nell'utilizzo delle dotazioni scolastiche → [**difficilmente quantificabili**]

27. effettivo aggiornamento dei percorsi formativi delle università; indicatori di impatto dei percorsi universitari; risultati dei docenti nell'anno di prova → [**difficilmente quantificabili**]
28. pubblicazione dei progetti costruiti dall'animatore digitale; efficacia delle progettualità; coinvolgimento del personale scolastico e di tutta la comunità → [**difficilmente quantificabili**]
29. *NIL*
30. *NIL*
31. *NIL*
32. *NIL*
33. *NIL*
34. *NIL*
35. *NIL* → [**questa azione è il monitoraggio stesso, ma avrebbe comunque senso ipotizzare dei KPI per valutarlo**]

Già da questa panoramica commentata sugli obiettivi misurabili dichiarati si evincono le pecche del PNSD: ottimi propositi, ma come verificare i risultati? Se manca il monitoraggio manca la possibilità per il cittadino di capire e verificare l'andamento dell'iniziativa.

Abbiamo quindi provato a cercare informazioni sul monitoraggio, sperando di trovare *opendata* 🕮 facilmente fruibili, ad esempio sul numero di plessi connessi in fibra. Purtroppo siamo stati molto delusi.

In effetti esiste il sito *opendata* 🕮[141]del Ministero dell'Istruzione su cui vengono pubblicati parecchi *data set*, ma cercando[142] le parole chiave "fibra", "PNSD", "Piano Nazionale Scuola Digitale", "lavagna digitale", "digitale", "connettività", "open source", "kpi" **non abbiamo ottenuto alcun risultato**. L'unico *data set* che poteva far

[141] *http://dati.istruzione.it/opendata*

[142] C'è un motore di ricerca interno al sito stesso: `http://dati.istruzione.it/opendata/ricerca/?searchinput=<parolachiave>`.

sperare è quello relativo all'anagrafica delle scuole[143], ma manca *esattamente* il campo relativo alla "connettività".

In generale vengono pubblicati[144] molti indicatori finanziari[145], ma non si riesce purtroppo a capire se queste spese sono state efficaci ai fini del PNSD.

Si noti che i dati **vengono effettivamente raccolti**, varie circolari ministeriali[146] chiedono periodicamente i dati alle scuole ma poi questi dati non vengono resi disponibili pubblicamente in *opendata* 🕮, **forse** (purtroppo non possiamo verificare) sono disponibili **internamente, accessibili solo al personale,** attraverso la piattaforma SIDI[147].

A conferma della mancanza di trasparenza si può citare l'iniziativa[148] del giornalista Riccardo Luna che nel 2017, ovvero a due anni dall'avvio del PNSD, aveva provato a raccogliere informazioni di monitoraggio: alla fine lui e la sua squadra dovettero ricorrere ad una richiesta FOIA (*Freedom Of Information Act*)[149] ottenendo dati disomogenei e molto deludenti, riportiamo una frase significativa dal rapporto pubblicato[150]:

> *Se devo dirvi la mia valutazione è che la direzione è giusta (il Piano Nazionale Scuola Digitale); ma la velocità di esecuzione no. É come se al Ministero in questi anni ci si fosse accontentati delle conferenze stampa; è come se si fosse*

[143] *http://dati.istruzione.it/opendata/opendata/catalogo/elements1/leaf/?area=Scuole&datasetId=DS0400SCUANAGRAFESTAT*

[144] Seppure in formati poco fruibili, ad esempio rapporti testuali in PDF invece di dati elaborabili direttamente. Tratteremo il tema della qualità degli *opendata* 🕮 in Livello 4 [*transparency*].

[145] Sugli investimenti fatti, si veda ad esempio il rapporto di Assolombarda "*Investire sul capitale umano*" (*http://www.assolombarda.it/servizi/formazione/il-futuro-della-formazione*).

[146] *http://www.orizzontescuola.it/osservatorio-permanente-scuola-digitale-aggiornamento-dati-entro-il-26-marzo*

[147] *http://www.istruzione.it/accesso-sidi*

[148] *http://www.agi.it/blog-italia/riccardo-luna/piano_scuola_digitale-2314157/post/2017-11-02*

[149] *http://www.foia4italy.it/cosa-e-un-foia*

[150] *http://www.agi.it/data-journalism/scuola_digitale_fedeli_piano_miur_foia-2313064/news/2017-11-02*

> *ritenuto che i titoli dei giornali bastassero a digitalizzare davvero la scuola; è come se qualcuno avesse ritenuto che gli annunci avessero un potere miracolistico. E invece no.*

E a conferma della inadeguatezza implementativa del PNSD possiamo usare il rapporto del febbraio 2019 "*Educare digitale - Lo stato di sviluppo della scuola digitale - Un sistema complesso ed integrato di risorse digitali abilitanti*" [AGC19] di AGCOM, ben riassunto da Eurispes[151]:

> *... le unità immobiliari raggiunte*[152] *dalla fibra ottica (a dicembre 2017), comprese quelle di competenza statale e, quindi, anche le scuole, superano il 64%, vale a dire circa 21 milioni di unità a fronte di 32,7 milioni di abitazioni e di edifici considerati. Tuttavia, la penetrazione*[153] *della banda ultra larga*[154] *nelle scuole italiane è solamente dell'11,2%*[155] *e mette in evidenza il forte dislivello fra la domanda e il potenziale dell'offerta.*
>
> ...
>
> *Un istituto scolastico che si possa definire "digitale" dovrebbe garantire una connessione veloce e sicura, in grado di permettere l'utilizzo simultaneo dei servizi didattici disponibili online – per una scuola di 20 classi, con 25 alunni ciascuna, la velocità di connessione necessaria stimata è di circa 700 Mbps – in modo da garantire il corretto svolgimento delle lezioni scolastiche.*

Cioè avere un alto livello di *infrastrutturalità* è condizione necessaria - sebbene non sufficiente e comunque non

[151] *http://www.leurispes.it/la-scuola-digitale-e-debole-solo-1-su-10-e-connessa-a-banda-ultra-larga*

[152] Vuol dire che all'edificio arriva la tecnologia, ma poi bisogna chiedere l'allacciamento.

[153] L'effettivo allacciamento.

[154] Ricordiamo che si intende da 30Mbps in su.

[155] Cfr. Figura 2.1 del rapporto AGCOM, pagina 22.

raggiunta pienamente in Italia - per poter fare didattica digitale fruendo di contenuti online, ma anche collaborando in rete. Il mondo della conoscenza oggi è fortemente basato sulla cooperazione e sulla produzione collaborativa di contenuti, si pensi ad esempio a Wikipedia, ma anche a contesti più tecnici come GitHub (`http://github.com`) e GitLab (`http://gitlab.com`) o a strumenti di produttività online come GoogleDocs o Office365 e infine a strumenti *locali* di apprendimento tipo la c.d. LIM (Lavagna Interattiva Multimediale)[156].

Continuiamo:

> *È ancora Agcom a fornire il dato secondo cui il 47,1% dei docenti svolge quotidianamente l'attività didattica tramite l'impiego di supporti tecnologici; il 27,5% vi ricorre settimanalmente; il 13,9% qualche volta al mese; il 6,7% qualche volta all'anno e il 4,9% mai.*

Buona parte del corpo docente usa poco gli strumenti tecnologici, nell'articolo si ipotizza una mancanza di "competenze digitali adeguate", infatti:

> *E ancora, i dati forniti rivelano che ben 3 insegnanti su 4 ammettono di avere bisogno di una formazione specifica e ulteriore nell'ambito delle TIC, per poter svolgere adeguatamente e più facilmente la propria professione. Nel nostro Paese, sono il 75,2% gli insegnanti che manifestano tale necessità, rispetto al 58,3% della media Ocse.*

Nel rapporto AGCOM vengono riportati ulteriori dati interessanti, non tutti negativi:

- solo poco più della metà delle scuole hanno adottato una strategia specifica per il PNSD;

[156] O gli *editor* collaborativi (Gobby, CodiMD) che uno degli autori usa ormai da anni per le lezioni di programmazione.

- scontiamo, nelle scuole attrezzate con computer per gli studenti, un rapporto computer/studenti più basso che nel resto della UE;
- ma il 74% delle scuole ha tutte le aule connesse in rete;
- e ben l'84% delle scuole usa il registro elettronico, ma solo circa la metà lo *apre* ai genitori.

Concludendo: c'è ancora molto lavoro da fare.

3.4 Difese *grassroots*

Logo di "Readers Against DRM"

Il termine anglosassone *grassroots movements* indica quei movimenti *politici* (anche in senso lato) che nascono "dal basso" per aggregazione più o meno spontanea di gruppi di cittadini, che si organizzano in comunità (*community*), liste civiche, comitati, associazioni ecc. Viene spesso usato anche il termine, sempre inglese, *bottom-up* in contrapposizione al *top-down* associato alle organizzazioni

"istituzionali": partiti, pubblica amministrazione, aziende ecc.

L'idea sottostante al desiderio di organizzarsi autonomamente è quella di ovviare alle mancanze, spesso grandi, delle istituzioni: ad es. dove lo Stato non arriva[157] perché lontano dal problema in questione o perché agganciato a ideologie non più condivisibili oppure ancora perché spinto da lobby monopolistiche; forse un **ampio** gruppo di soggetti "rappresentativo" (ad es. legato al territorio o ad un tema particolare, i c.d. *stakeholders* - portatori di interesse) può risultare più efficiente, specie se ben coordinato. *Grassroots* viene spesso associato ad un altro termine inglese: *crowd*, cioè la massa (delle persone, dei cittadini) che può cambiare le cose: vale nel caso delle rivoluzioni, ma anche e soprattutto nel campo della **conoscenza**, tecnologica o meno. In particolare, qui nel L3-education, associamo il termine *grassroots* a tutti quei *movimenti dal basso* che si battono per la **libertà di accesso, diffusione e uso della conoscenza**, spesso in contrapposizione con le c.d. lobby della "proprietà intellettuale", che invece vorrebbero *limitare l'accesso per monetizzare* il più possibile.

Altri aspetti (es. *crowdsourcing*, *accountability through transparency* ecc.) verranno trattati in L4-transparency e L5-participation.

La storia dell'approccio *grassroots* alla conoscenza digitale ha origini "antiche" (per l'informatica), parliamo degli anni '60 del secolo scorso e della c.d. "Cultura Hacker" [Lev01]. In quegli anni, in alcune università statunitensi, si osservò un certo grado di *ribellione* alla "cultura del camice bianco": il camice bianco era indossato dagli operatori dei computer che facevano da tramite (da interfaccia) tra gli studenti e le risorse di calcolo che allora erano molto scarse e costose; tali operatori erano percepiti come ostacoli all'accesso alla conoscenza e quindi diventarono il simbolo del nemico da combattere.

Non a caso al primo posto tra i principi fondamenta-

[157] O ancor peggio, dove arriva generando più problemi che soluzioni.

li dell'*Etica Hacker*[158] troviamo proprio l'accesso alle risorse di calcolo, qui di seguito i punti originali tradotti fedelmente:

1. L'accesso ai computer - e a qualunque cosa possa insegnare come funziona il mondo - dovrebbe essere illimitata e totale. Cedi sempre all'imperativo "mettici sopra le mani"!
2. Tutta l'informazione deve essere *gratuita*[159].
3. Non fidarti dell'autorità - promuovi la decentralizzazione.
4. Gli Hacker dovrebbero essere giudicati per il loro *hacking*, per il loro operato, e non per qualche criterio fasullo come laurea, età, razza o ruolo.
5. Puoi creare arte e bellezza con un computer.
6. I computer possono cambiarti in meglio la vita.

Si ricordi che siamo sempre nei dintorni del 1968, però a parte una fraseologia "sessantottina" i concetti espressi sono molto interessanti e condivisibili: informazione accessibile, approccio critico e decentralizzazione, merito puro e apprezzamento nei confronti della tecnologia informatica.

Importante sottolineare qui che noi usiamo il termine *hacker*[160] nella sua accezione originale di "persona curiosa del mondo e della tecnologia (*in primis* informatica ma non solo), dedita allo studio, alla modifica, al perfezionamento degli oggetti e dei sistemi e fortemente coinvolta nella diffusione libera della conoscenza acquisita". Rigettiamo invece l'accezione tutta giornalistica dell'*hacker* come "pirata informatico".

La *Cultura Hacker*[161] fu l'inizio di una *rivoluzione* tecnica, scientifica e culturale che culminò nell'inizio di un'altra rivoluzione tecno-politica, quella del **Software Libero** ancora in corso e che tra poco tratteremo. Con la *Cultura Hacker* si cominciò a criticare il flusso della conoscen-

[158] *http://en.wikipedia.org/wiki/Hacker_ethic#The_hacker_ethics*

[159] Nel testo originale era "free", per ora lo traduciamo con *gratis* ma a breve declineremo ulteriormente il termine *free*.

[160] *http://it.wikipedia.org/wiki/Hacker*

[161] *http://it.wikipedia.org/wiki/Cultura_hacker*

za *top-down* (calato dall'alto) per integrarlo con un flusso *bottom-up* (dal basso), ciò che oggi è culminato nel c.d. *crowdsourcing*[162] (informazione creata da una massa di persone) che alimenta lo stesso Software Libero, ma anche iniziative lodevoli come Wikipedia e OpenStreetMap e perfino iniziative commerciali come Waze, TripAdvisor, Amazon e Ebay, Lego, Starbucks ecc.

Infine, anche la volontà di riprendere il controllo di quella che abbiamo definito "*La computing agency rubata*" - 3.1.4 è figlia di tale cultura e il Software Libero è la formalizzazione di uno dei suoi aspetti più importanti.

3.4.1 Software Libero

Se in campo legislativo la tendenza a iper-normare è figlia della cultura del controllo statalista o aziendalista, in campo contrattuale - ci riferiremo in particolare al contesto tecnologico - si osserva una tendenza alla verbosità sia per smania di controllo ma anche per *offuscamento* dei vari vincoli: le classiche *clausole scritte in piccolo* che nessuno legge, ma che sono importanti. In campo tecnologico la normativa che viene meno esaminata dagli utenti è probabilmente quella delle licenze software, le cosiddette EULA (*End-User License Agreement*).

Una licenza (cfr. [Ali12]) è una autorizzazione che il detentore dei diritti d'autore su un'*opera* concede, in toto o parzialmente, a un terzo. Dato che nel mondo digitale è molto facile esaminare, modificare e copiare un'*opera composta di bit*, le licenze software si preoccupano di stabilire dettagliatamente *cosa* può fare l'utente con la propria copia del software, in merito a installazione, duplicazione, modifica, possibilità di studio o analisi.

Ad esempio, la licenza d'uso di Windows 10[163] ha una corposa sezione "Installazione e Diritti di Utilizzo" in cui

[162] *http://it.wikipedia.org/wiki/Crowdsourcing*, da non confondere col *crowdfunding* (*http://it.wikipedia.org/wiki/Crowdfunding*), mi raccomando.

[163] *http://microsoft.com/en-us/Useterms/OEM/Windows/10/Useterms_OEM_Windows_10_Italian.htm*

si specifica che (grassetti nostri):

> *Il software **non viene venduto**, ma è concesso in licenza. Purché il licenziatario si conformi a tutte le condizioni contenute nel presente contratto, Microsoft gli concede il diritto di installare ed eseguire **un'istanza** del software sul dispositivo in uso (il dispositivo con licenza), che può essere utilizzata **da una sola persona** alla volta. L'aggiornamento di software non originale con software proveniente da Microsoft o da fonti autorizzate non rende originale la versione iniziale o la versione aggiornata e in tal caso il licenziatario non dispone di una licenza per l'utilizzo del software.*

In particolare al licenziatario **è vietato** (grassetti e parentesi quadre nostri):

- *utilizzare o virtualizzare alcune funzionalità del software separatamente;*
  [O tutto o nulla? Non significa molto dato che un oggetto complesso come un sistema operativo lo si usa per forza a piccoli pezzi.]
- ***pubblicare, duplicare (ad eccezione della copia di backup autorizzata), noleggiare, concedere in locazione o in prestito il software**;*
  [Non si può condividere lo strumento con altri utenti.]
- *trasferire il software (salvo nei modi previsti dal presente contratto);*
- ***aggirare le restrizioni o le limitazioni** tecniche presenti nel software;*
  [L'oggetto va preso così com'è, comprese "restrizioni" non meglio dichiarate a cui l'utente deve sottostare]
- *utilizzare il software come software server, **per l'hosting di servizi commerciali,***

> ***renderlo disponibile per l'uso simultaneo da parte di più utenti su una rete**, installarlo su un server e consentire agli utenti di accedervi da remoto o installarlo su un dispositivo per l'utilizzo solo da parte di utenti remoti;*
> *[Non si può condividere lo strumento con altri utenti via rete.]*
> - ***decompilare o disassemblare il software**, né tentare di fare ciò, fatta eccezione per i casi in cui la suddetta limitazione sia: (a) consentita dalla legge applicabile, (b) consentita dalle condizioni di licenza ...*
> *[Non si può studiare il funzionamento dell'oggetto che si sta usando... tranne il fatto che la legge, generalmente, lo consente (pensiamo in particolare alla decompilazione e analoghe tecniche di reverse engineering).]*

Molte EULA di software usati comunemente contengono clausole simili e tempo fa ci divertimmo a scrivere una parodia di licenza d'uso per l'acqua in bottiglia applicando vincoli analoghi per mostrare le assurdità di tali licenze, si veda figura 3.11, ma **esistono alternative più interessanti**.

Agli inizi[164] della storia dei computer il software, quando c'era, veniva semplicemente regalato assieme all'hardware, i produttori di computer degli albori facevano *revenue* vendendo il c.d. "metallo" nudo e crudo o poco più. Quando[165] il progresso e la concorrenza di mercato abbassarono i prezzi dell'hardware, i produttori videro una fonte di ricavo anche nel software e cominciarono a vendere anche quello introducendo meccanismi di licenza, anche molto restrittivi, per mantenere il controllo della propria clientela: era infatti pratica comune copiare programmi per

[164] Anni '50 e '60 del XX secolo.
[165] Anni '70 del XX secolo.

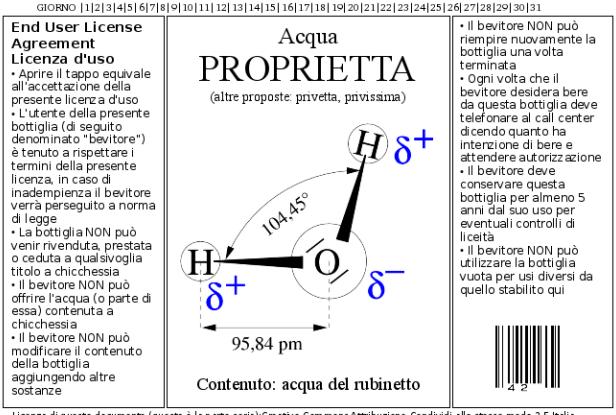


Figura 3.11: Una licenza per l'acqua?

poterli usare su più computer contemporaneamente, ovviamente questa pratica faceva perdere potenziali vendite al produttore.

Dopo il 1980[166] la situazione divenne "insostenibile" per un ricercatore del MIT (*Massachusetts Institute of Technology*) diventato poi famoso, RMS (Richard Matthew Stallman), che decise di dare una **svolta rivoluzionaria** inventando il concetto di **SL (Software Libero)**[167].

L'idea geniale alla base del SL è quella di **concedere formalmente** diritti all'utente del software invece di (cercare di) togliergli. Utilizzando il meccanismo del *copyright* RMS scrive una licenza che "vincola" (in realtà si dovrebbe dire "libera") l'utente del software alle seguenti[168]:

[166] Cfr. *http://gnu.org/gnu/gnu-history.html* e *http://gnu.org/gnu/thegnuproject.html*.

[167] *http://gnu.org/philosophy/free-sw.html*

[168] Numerate a partire da 0 perché nella maggior parte dei linguaggi di programmazione si usa così e RMS volle appunto dare un *imprinting software*.

Libertà fondamentali del Software Libero

0) uso per **qualunque** scopo
1) **studio** del funzionamento, anche attraverso il *codice sorgente* fornito sempre
2) **redistribuzione** *as is* (senza modifiche) a chiunque
3) redistribuzione dei **lavori derivati** (modificati) usando la stessa licenza, la c.d. "viralità"

Da quel momento in poi il mondo del software venne diviso in due macro categorie: il Software Libero, concesso in licenza rispettando le quattro libertà sopra elencate, e il *software proprietario*, ovvero qualunque software con una licenza che non conceda all'utente anche solo una di quelle libertà.

Già ad un primo esame queste quattro libertà dovrebbero entusiasmare qualunque utente di software: prendo un programma e posso farne l'uso che voglio? Posso studiarne il funzionamento interno fin nei minimi dettagli? E mi danno pure un aiuto (il codice sorgente) nell'operazione? Posso perfino modificarlo per adattarlo alle mie necessità e posso distribuire copie sia del programma originale sia di quello modificato da me?

Ma allora dov'è la "fregatura"? Si potrebbe domandare l'utente sospettoso.

Perdonate lo *spoiler*: **non c'è alcuna fregatura**. Non ci sono ulteriori vincoli o clausole da rispettare *tranne* in un caso: diverse licenze per Software Libero richiedono che il codice sorgente del software derivato sia fornito[169] *con la stessa licenza* del software originale: è un modo per **incoraggiare la condivisione** invece di ostacolarla, per questo motivo questa classe di licenze è stata definita *copyleft*[170], sfruttando il gioco di parole con *copyright* per invertirne il senso: da "tutti i diritti riservati" a **tutti i diritti riversati**[171]. Altre licenze invece consentono di

[169] Nel caso il codice binario sia distribuito a terzi.

[170] *http://it.wikipedia.org/wiki/Copyleft*

[171] Anche in italiano il gioco di parole è esteticamente soddisfacente.

poter modificare il software senza richiedere di condividere il sorgente allo stesso modo, producendo per esempio software proprietario: questa classe di licenze è definita *permissiva*.

Naturalmente i vantaggi del SL sono enormi [PCA18], ecco i principali:

- è impossibile creare *scarsità artificiale* del prodotto: chiunque può legalmente distribuirne copie;
- è impossibile implementare *obsolescenza programmata*: avendo i sorgenti chiunque può manutenere indefinitamente il prodotto senza essere vincolato al produttore originale;
- è possibile adattare il prodotto alle proprie esigenze senza dover sottostare alle esigenze di mercato del produttore;
- è impossibile implementare meccanismi di *lock-in* (cfr. sezione "*Lock-in*" - 1.1.5) perché i dati sono memorizzati in formati che possono essere studiati e utilizzati da software alternativo, interoperabile;
- azioni come l'inserimento di codice malevolo nelle applicazioni[172] sono più difficili perché il sorgente è sotto gli occhi di chi voglia guardare, i.e., il Software Libero è l'unica via per la riappropriazione della *Computing Agency* citata in sezione "*La computing agency rubata*" - 3.1.4.

Occupandoci qui del Livello 3 [*education*], a noi interessano in modo particolare le **ricadute positive** nel campo della conoscenza: il Software Libero **si lascia conoscere**, ci permette di capire cosa fa e come lo fa fin nei minimi dettagli. Certo, occorre comprendere la programmazione, ma il diritto di sapere non viene negato, anzi! Al contrario nel mondo del software proprietario potete essere il miglior programmatore del mondo ma non avendo accesso al codice sorgente sareste costretti ad un durissimo lavoro di *reverse engineering*[173] per poterne comprendere anche solo una

[172] *http://www.wsj.com/articles/u-s-government-contractor-embedded-software-in-apps-to-track-phones-11596808801*

[173] Usare strumenti informatici che tentano di ricostruire il sorgente

parte del funzionamento. In altre parole con il SL si può imparare il funzionamento interno, non solo l'operatività esteriore, di ciò che si usa. **Si può quindi combattere efficacemente l'*analfabetismo meta-operativo*** citato in sezione "*Deficit di conoscenza*" - 3.2.2.

Inoltre, se pensiamo ad un quadro in cui anche la pura conoscenza (e.g., documentazione, testi scritti, video, audio ecc.) viene distribuita tramite licenze libere analoghe a quelle del SL ma create apposta per i media come le c.d. *Licenze Creative Commons*[174] ecco che otteniamo una "catena del valore" completa che possiamo chiamare ***conoscenza libera***.

Attenzione: ciò che stiamo immaginando e descrivendo non è un mondo di fantasia, è **un mondo reale, perfettamente esistente e florido**. Purtroppo è poco conosciuto al di fuori del nostro ambiente anche perché nel corso degli anni è stato denigrato da chi aveva e ha tutto l'interesse a mantenere lo *status quo* del mondo *proprietario*, per dirla con una famosa affermazione di Clay Shirky[175]:

> *Le istituzioni cercheranno sempre di preservare i problemi di cui loro sono le soluzioni*

Ci riferiamo in questo caso ai grandi produttori di software (e.g., Microsoft, Apple, Adobe ecc.) che *vivono* di scarsità artificiale e di obsolescenza programmata e hanno tutto l'interesse a diffondere il c.d. FUD (*Fear, Uncertainty and Doubt*)[176] per impedire che i loro clienti decidano di passare ad *alternative libere*. Questa propaganda negativa purtroppo funziona abbastanza bene: attualmente solo *lato server* (web e storage) la penetrazione del SL è effettiva (più del 60%[177]) e consapevole (frutto di scelta tecnologica), mentre *lato desktop* (pc e portatili) si fatica a raggiungere il 10%. Discorso a parte è il contesto

originale esaminando l'oggetto eseguibile.

[174] *http://creativecommons.org*

[175] *http://kk.org/thetechnium/the-shirky-prin*

[176] *http://en.wikipedia.org/wiki/Fear,_uncertainty,_and_doubt*

[177] *http://news.netcraft.com/archives/category/web-server-survey*

smartphone dato che la penetrazione è altissima (Android, basato su Linux, ha raggiunto l'80%[178] del mercato già anni fa), ma purtroppo non è frutto di scelta "consapevole": la libertà del software non è tipicamente un aspetto preso in considerazione dall'acquirente medio. Naturalmente *ça va sans dire* che gli autori del presente testo utilizzano SL anche su desktop e portatili e usano Android - particolari versioni "ripulite" da componenti proprietarie - per scelta consapevole[179].

Interessante (far) notare che da alcuni anni a questa parte le istituzioni governative, sia nazionali che internazionali, si sono accorte dei vantaggi del SL e hanno cominciato a introdurre normative per (tentare di) incrementarne l'adozione. Facciamo riferimento ad esempio al CAD (Codice dell'Amministrazione Digitale)[180] italiano il cui articolo 68 impone come scelta privilegiata l'uso e la *produzione* di soluzioni software libere. E sono molte le P.A.[181] che adottano SL per gli strumenti di produttività (LibreOffice[182]), per la navigazione in rete (Firefox[183]), per la gestione della posta elettronica (Thunderbird[184]) ecc.

In conclusione, il nostro *cittadino digitale* ideale è quello che almeno usa, e spinge per far usare[185] solo Software Libero. Meglio ancora se prova a "guardare sotto al cofano" per cercare di capire l'architettura degli strumenti che usa.

[178] *http://techcrunch.com/2013/08/07/android-nears-80-market-share-in-global-smartphone-shipments-as-ios-and-blackberry-share-slides-per-idc*

[179] E a volte facendo anche un po' di fatica per riuscire ad usare ciò che abbiamo **scelto**, ma ne vale la pena.

[180] *http://docs.italia.it/italia/piano-triennale-ict/codice-amministrazione-digitale-docs/it/v2018-09-28/index.html*

[181] *http://en.wikipedia.org/wiki/Adoption_of_free_and_open-source_software_by_public_institutions*

[182] *http://libreoffice.org*

[183] *http://mozilla.org*

[184] *http://thunderbird.net*

[185] In azienda, nella scuola dei suoi figli, nella amministrazione comunale dove vive ecc.

3.4.2 *Right to repair*

Riprendiamo qui un concetto importante per poi proporre una soluzione *politica* che dovremo, noi come cittadini, chiedere a gran voce.

Negli anni '90 del secolo scorso i produttori *automotive* (auto, veicoli commerciali, mezzi pesanti ecc.) cominciarono a inserire nei loro mezzi parecchi sottosistemi elettronici: inizialmente erano solo le centraline di controllo dei motori[186], in seguito si aggiunsero controllo della accelerazione e della frenata, gestione emergenze (airbag) ecc. per arrivare fino ai giorni nostri in cui vediamo sistemi di intrattenimento multimediali, riconoscimento dei segnali stradali e aiuto alla guida.

Parallelamente al progresso funzionale vennero introdotti dei meccanismi vincolanti per l'accesso a tali apparati, che di fatto sono dei veri e propri computer: per poterli riparare (*repair*) o modificare (*tinker*) divennero necessari sia hardware e software specialistici sia credenziali di accesso (login e password), limitando fortemente l'accessibilità da parte dei c.d. "meccanici non autorizzati", ma anche degli stessi proprietari dei mezzi che a questo punto non avevano più alcun controllo sul funzionamento degli oggetti di loro *proprietà*[187]. Questo rappresenta ancora oggi un chiaro vantaggio dei produttori che possono così vendere anche le *licenze* software di gestione e far pagare al cliente, potenzialmente, ogni accesso ai parametri di funzionamento attraverso il meccanismo del *Anything As a Service* (ogni cosa come un servizio). Peggio ancora, questo meccanismo porta ad una *scarsità artificiale* e ben pilotata delle informazioni necessarie ai professionisti, anche le più banali, per poter riparare macchine e altri dispositivi: diventando software, quelle informazioni sono *embedded* nei compu-

[186] L'imperativo era ed è la riduzione delle emissioni: un controllo digitale permette una gestione pulita della combustione rispetto ad un sistema puramente meccanico.

[187] Rimarchiamo sempre questo termine: dubitiamo molto sulla applicabilità della definizione di "proprietà" ad un oggetto su cui non abbiamo controllo.

ter e, *ça va sans dire*, **proprietarie**. Come già citato in precedenza, pioniere di questo innalzamento artificiale del *gap di ingresso* per nuovi fornitori di servizi, in questo caso i meccanici, fu la casa produttrice di macchine agricole John Deere[188], ma questa tendenza è purtroppo in rapida espansione in tutti i settori.

Si può trovare un commento pittoresco e colorito su queste tecnologie a partire dal minuto 6:15 di questa[189] puntata di "Texas Metal"[190] in cui si afferma: "il problema delle auto nuove è che ormai sono dei computer". Noi ovviamente aggiungiamo che il problema non è che sono dei computer, ma che sono **computer controllati da altri**.

Dal punto di vista della CDT e in particolare del livello L3-education che stiamo trattando, si potrebbe affermare che con questi meccanismi in atto non bastano più le competenze, ci vuole ormai anche un'**autorizzazione**. Assistiamo alla *commodification* (mercificazione) della conoscenza.

I produttori di elettronica digitale e informatica erano già attivi da tempo nell'introduzione di meccanismi di vincolo[191] ma a partire dagli anni 2000 aumentarono la produzione di tali tecnologie[192]. Tra i produttori più "forti" in questo campo troviamo sicuramente Apple che utilizza sovente *chip*[193] dedicati alla sola funzione di **impedire l'uso di componenti** non autorizzati. Inoltre Apple combatte "politicamente"[194] contro chi vorrebbe modificare le

[188] *http://www.bloomberg.com/news/features/2020-03-05/farmers-fight-john-deere-over-who-gets-to-fix-an-800-000-tractor*

[189] *http://youtube.com/watch?v=Rvrdfk9gNfk*

[190] Una serie TV sulla *customizzazione* di auto.

[191] Si pensi ad esempio ai famosi *dongle* ("chiavi" hardware) per avviare certi programmi proprietari molto costosi.

[192] Dopo l'introduzione del già citato DRM (*Digital Restriction Management*).

[193] *http://gizmodo.com/heres-the-chip-apple-is-using-to-stop-you-from-buying-c-5945889*

[194] *http://time.com/4828099/farmers-and-apple-fight-over-the-toolbox*

norme[195] che consentono queste pratiche e "legalmente"[196] contro chi cerca di svolgere *onestamente* il proprio lavoro di riparatore, usando il combinato disposto di copyright e brevetti come una **clava** (metaforicamente parlando, per carità).

Per risolvere **il problema**, allo scopo di **impedire** questi "attacchi alla sovranità digitale del cittadino" e restituirgli la propria "*La computing agency rubata*" - 3.1.4, oltre al già citato Software Libero[197] sono nate un po' in tutto il mondo iniziative per il "*right to repair*"[198] che fanno pressione sui governi affinché varino normative a favore del diritto di riparazione e modifica degli apparati[199], con qualche successo eclatante[200], ma c'è ancora **molto lavoro da fare**.

3.4.3 *Learn to code*

Arrivati fin qui, dopo aver parlato di *difese* a vari livelli, ci potremmo domandare se per poter esercitare i diritti di cui sopra (accesso alla conoscenza, controllo sulla *computing agency* ecc.) dobbiamo come Cittadini imparare a padroneggiare ogni tipo di tecnologia digitale. "*Learn to code*" alla lettera verrebbe tradotto con "impara a programmare", è il nome con cui nel mondo si indica il tema legato all'ipotesi di introdurre nei corsi di studio, *anche fin dai primi anni* [Sen+15], materie legate alla tecnologia digitale, arrivando anche a insegnare la programmazione dei computer.

[195] Agganciandosi strumentalmente a leggi come il DMCA citato in sezione "*L'ignoranza della legge..*" - 3.1.2.

[196] *http://www.macrumors.com/2018/04/13/apple-lawsuit-repair-shop-norway*

[197] Che storicamente si è sempre indirizzato verso il software, appunto, salvo aver più recentemente abbracciato anche il problema dell'hardware, avvicinando quindi i due movimenti.

[198] Usiamo il nome dell'associazione più nota, "The Repair Association" (*http://repair.org*), come *parte per il tutto*.

[199] *http://en.wikipedia.org/wiki/Electronics_right_to_repair*

[200] *http://en.wikipedia.org/wiki/Motor_Vehicle_Owners'_Right_to_Repair_Act*

Un revisore delle bozze di questo capitolo ha fortemente negato l'ipotesi di risposta affermativa adducendo come motivazione il fatto che: "il cittadino medio non deve avere conoscenza delle tecnologie digitali come non deve conoscere le tecniche dentistiche, le norme fiscali, i metodi per costruire e riparare trattori ecc. è assolutamente normale e giusto che ognuno di noi sia esperto, forse, di poche cose".

Noi però riteniamo di poter proporre una *calibrata* risposta affermativa.

La metafora del dentista (del commercialista, del trattorista) non funziona perché, come visto anche nella sezione "*Il cittadino inconsapevole*" - 3.2, la conoscenza tecnologica digitale del cittadino medio è fallata ad un *livello superiore*, meta-operativo. Il cittadino medio non distingue la tecnologia dalla magia (Clarke, epigrafe della sezione "*Tecnologia mascherante*" - 3.1.1) e, sempre metaforicamente parlando, si "destreggia" come se ragionasse così:

- ho mal di denti
- sarà una gomma sgonfia
- vado dal commercialista

Invece il Cittadino Digitale che vorremmo è quello che almeno riesce a descrivere le differenze fra[201] ad esempio:

- un programma e una pagina web
- una chat e una telefonata VoIP
- una pubblicità e un testo
- un contenuto locale e uno "in cloud"
- bluetooth, WiFi, 3G/4G/5G
- ADSL e fibra
- immagine *bitmap* e *vettoriale*

Cioè concetti comparabili nel mondo analogico ad esempio col distinguere tra benzina e gasolio, 'TAC' e 'TAC con contrasto', riconoscere un cartello stradale, cucinare un piatto di pasta, andare a comprare un giornale in edicola, leggere un libro.

Quindi stiamo affermando che "tutti dovrebbero imparare a programmare"?

[201] E riesce anche a distinguere tali oggetti quando li incontra.

No, non intendiamo *letteralmente* il titolo di questa sezione, vorremmo invece interpretare il "to code" in senso più generale e astratto, per dirla con Shein [She14]: "Not everyone needs coding skills, but learning how to think like a programmer can be useful in many disciplines" (non a tutti servono abilità di programmazione, ma imparare a pensare come uno sviluppatore può essere utile in molti ambiti).

Ci riferiamo al c.d. *computational thinking* (pensiero computazionale, algoritmico) più che di programmazione vera e propria: insegna a pensare in maniera astratta, a suddividere un problema in sotto-problemi e in sequenze di operazioni per raggiungere uno scopo, ragionando anche sulle ramificazioni fallimentari e sulle azioni correttive. Un po' come nel contesto degli scacchi dove si deve ragionare per sequenze di azioni e possibili reazioni, solo che il pensiero computazionale è molto più generale e applicabile nella vita reale. In questo senso iniziative come il citato Piano Nazionale Scuola Digitale vorrebbero, pur con tutti i problemi evidenziati, andare in tale direzione.

A supporto riportiamo alcuni passaggi molto condivisibili di un'intervista a Douglas Rushkoff[202], autore di "*Program Or be Programmed: Ten Commands for a Digital Age*" [Rus10]. Parlando della differenza fra *semplice utente* e *utente programmatore* (con mentalità da):

> *La vera differenza è che il programmatore capisce che la macchina può modellare quasi tutto. L'utente sa solo come comportarsi all'interno di quel modello. Quindi è come la differenza tra un drammaturgo e un personaggio o, nella migliore delle ipotesi, un attore che sa di leggere una sceneggiatura.*

E offre suggerimenti per migliorare la situazione:

> *Il primo passo verso il mantenimento dell'autonomia in qualsiasi ambiente programmato è*

[202] `http://www.wired.com/2011/07/douglas-rushkoff`

> *essere consapevoli che è in corso una programmazione. È semplice come capire che le pubblicità sono lì per aiutare a vendere le cose. E che gli spettacoli televisivi sono lì per vendere pubblicità e così via.*

E continua con:

> *Il secondo passo sarebbe decidere se vuoi o meno essere in grado di partecipare attivamente alla creazione del mondo in cui vivi. A volte lo farai, a volte no. Dipende se puoi fidarti delle persone che stanno costruendo la tua realtà per te.*

Parlando invece della cultura *mainstream* che vorrebbe *tarpare* la presa di coscienza, di conoscenza e di controllo da parte dei cittadini:

> *Mettiamo gli stigmi su di loro per diversi motivi. ... Devi capire, però, che la sovra-cultura cercherà sempre di denigrare qualcosa di veramente minaccioso. Se accedi al pannello di controllo della civiltà, sarai chiamato un geek*[203]*. Devono tenerci lontani da qualsiasi cosa che dia veramente potere. Quindi fanno sembrare le cose belle poco cool e le cose stupide belle.*

Il soggetto di quel "mettiamo" sono i governi e le grandi aziende, mentre quel "loro" sono gli *hacker*[204] che fanno paura perché sono coloro che *rivendicano il diritto* di conoscere, sono i Cittadini Digitali che vogliono esaminare, modificare e condividere[205] il *programma* che fa girare la società civile, siamo noi autori e puoi ora essere tu, cara lettrice[206]: tocca a te fare la tua parte.

[203] Spregiativo di *hacker*.
[204] Nel significato spiegato poco sopra.
[205] Naturalmente nel pieno rispetto delle licenze libere.
[206] Inteso come persona, non è affatto una questione di genere.

Appendice A

Profilazione WiFi

Solo per dare un piccolo assaggio di quello che si può fare anche soltanto analizzando alcuni dati di *traffico* (in senso generale, in questo esempio intendiamo riferirci a informazioni legate ad un servizio di connettività), vogliamo mostrare un lavoro di profilazione, molto *homemade*, fatto da uno degli autori elaborando i *log file* 🕮 di un *router* 🕮 casalingo.

Vedremo che sarà possibile trarre parecchie *conclusioni* sui pattern di utilizzo della casa in cui quel router è stato installato.

Iniziamo col descrivere il contesto: l'oggetto di studio è un appartamento situato in una città molto turistica. Negli scorsi anni è stato prima gestito da un'agenzia per affitti brevi (che utilizzava piattaforme come Airbnb, Booking ecc. per "vendere notti") e successivamente è stato dato in affitto stabile per quasi un anno ad una coppia. Nell'appartamento è presente un router che fornisce accesso a Internet agli ospiti cui è sempre stata fornita la password[1]. Il router *tiene traccia* di chi si connette, nel senso che attraverso il meccanismo standard del *DHCP* 🕮

[1] Era presente un cartello appeso all'ingresso, è importante specificarlo perché implica che chiunque entrasse nell'appartamento aveva di fatto la possibilità di agganciarsi al WiFi senza dover chiedere permessi né lasciare credenziali a chicchessia.

le assegnazioni di indirizzo vengono registrate assieme all'identificativo *hardware* del *device* (il cosiddetto *mac address* 🕮) e alla data (e ora, che però non viene utilizzata in questo caso). Quindi nel corso del tempo si otterrà un *dataset* composto da *record* contenenti:

- *hostname*: durante la procedura di negoziazione dell'indirizzo effettuata al collegamento alla rete WiFi il device dichiara al gestore DHCP il proprio *nome*, tale nome viene normalmente generato in maniera pseudocasuale all'installazione del dispositivo, es. "DESKTOP-0T4PIJG", oppure qualche utente lo imposta manualmente, a volte usando il proprio nome o nickname, es. "iPhone-di-Arturo";
- *macaddress*: anch'esso comunicato all'atto della interazione col DHCP, è una stringa di otto cifre esadecimali separate da ':', ad es. 'd4:90:9c:83:76:99';
- *IP*: l'indirizzo (si veda box 0.1.1) assegnato al *device*, quattro numeri separati da un '.', ad esempio 192.168.100.185;
- *data*: il *timestamp* (data e ora) dell'assegnazione.

Il *dataset* copre attualmente un periodo di circa tre anni, di cui mostreremo solo le parti salienti.

L'elaborazione viene fatta mediante alcuni script in R[2] e in Graphviz[3] che generano anche i grafici mostrati nelle figure A.1 e A.2.

I **primi due grafici, in figura A.1,** mostrano i *plot* del numero di *device* collegati per data: il grafico in alto è relativo al periodo "affitti turistici di pochi giorni" mentre in basso si vede il periodo "affitto stabile a coppia". Già in questa prima visualizzazione si può effettivamente verificare che i pattern di utilizzo (turistico vs. affitto) sono diversi:

- in alto ci sono più buchi (periodi in cui l'appartamento non è stato "venduto");

[2]Software, ovviamente libero, di analisi matematico statistica, *http://r-project.org*.

[3]Ambiente (un vero e proprio linguaggio in realtà) di visualizzazione, *http://graphviz.org*, anch'esso libero.

- in alto il numero di *device* è più variabile (N.B. le scale sono diverse).

I **due grafi in figura A.2** invece sono molto più interessanti, rappresentano dei *grafi di associazione* fra date e *device*, cioè ci dicono ***chi* (nel senso di *quale device*) era presente nell'appartamento in un certo giorno**. In entrambi i grafici gli ovali sul bordo sinistro rappresentano le singole date mentre quelli sul lato destro i *device*, gli archi che connettono date con *device* ci mostrano le informazioni sulle presenze. Il grafo di sinistra rappresenta l'utilizzo *affitto turistico* mentre quello di destra l'*affitto stabile*. Si può ben notare come sul grafo di sinistra non ci sia una *presenza forte* come è invece ben visibile nel grafo di destra, marcata dall'ovale rosso a linea spessa, che **identifica i *device* degli affittuari**, presenti praticamente sempre. Ancora, nel grafo di sinistra si possono identificare perfettamente i *device* dei gestori dell'appartamento (agenzia e personale di pulizia, marcati dall'ovale rosso fine), presenti saltuariamente (a consegna/restituzione appartamento da parte dei turisti) e i turisti, che a parte le date a loro assegnate non si ripetono mai. Sul grafo di destra invece si possono vedere ancora un paio di informazioni interessanti:

- gli ospiti di una giornata (magari una cena) che sono i *device* che appaiono legati ad una sola data e ...
- ... **gli ospiti che si sono fermati per alcuni giorni** (amanti/subaffittuari?), marcati coi rettangoli verdi.

Naturalmente in questa analisi abbiamo lavorato conoscendo già il risultato (l'uso dell'appartamento) per verificare che la profilazione potesse dare informazioni utili, come infatti è stato. Ora che conosciamo la *forma* dei grafici in funzione dei vari usi potremmo applicare la stessa analisi ad un altro appartamento per capire:

- tipo di uso dell'appartamento (affitto temporaneo o stabile);
- chi fa le pulizie (in caso di affitto temporaneo);
- quanti (e circa quali, dal *macaddress*) *device* possie-

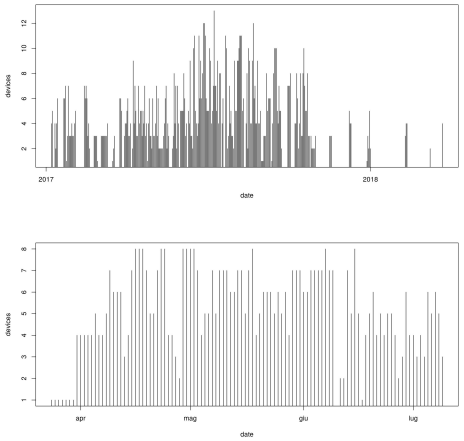


Figura A.1: Turistico (sopra) vs. affittuario

dono gli affittuari, i.e., un lasco *proxy* del censo;
- (circa) quanti sono effettivamente gli affittuari, utile per evidenziare dichiarazioni mendaci e/o subaffitti di singole stanze;
- quando e (circa) quante persone invitano gli affittuari (feste);
- quando e chi (sempre in termini di identificativo del *device*) frequenta abitualmente gli affittuari;
- quando gli affittuari sono in casa.

In una situazione più ampia e generale (si pensi ad esempio ai dati relativi ad un centro commerciale o a un'azienda) probabilmente bisognerà combinare qualche dataset aggiuntivo (ad esempio i dati sugli scontrini o sulle *strisciate dei badge aziendali*) per poter capire meglio i comportamenti delle persone che utilizzano uno spazio, informazioni che però sono facilmente reperibili, specie se chi gestisce i vari servizi (commerciali, accesso, wifi ecc.) è un'unica entità.

E finora non abbiamo mai citato la possibilità di tracciare anche l'effettivo traffico effettuato (siti visitati, da chi e quando), analizzando anche questo tipo di dataset si

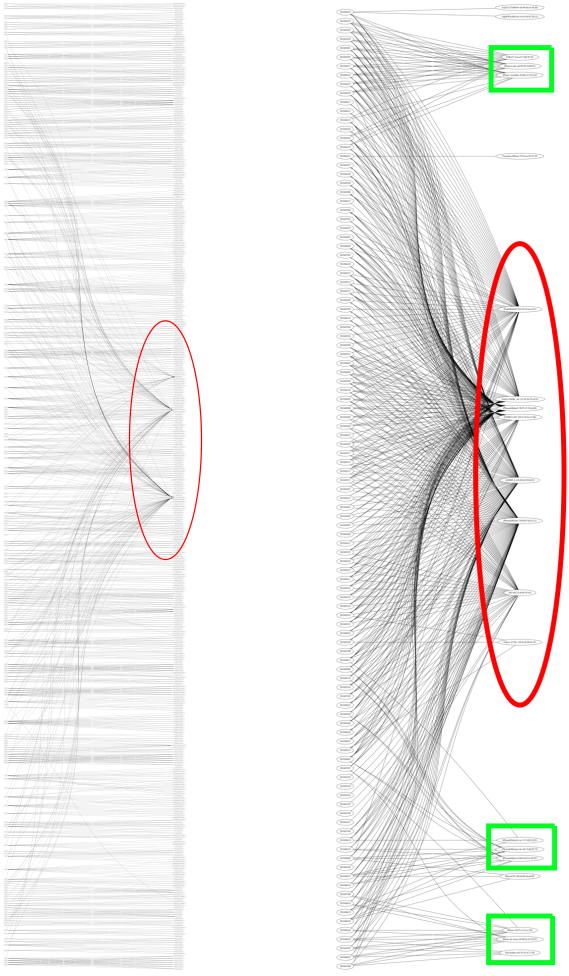


Figura A.2: Turistico (sinistra) vs. affittuario

possono evincere età e sesso dell'utente, gusti e abitudini, relazioni con altre persone (ricordiamo che, purtroppo, ancora buona parte del traffico in rete non è crittografata quindi è facilmente analizzabile da chiunque abbia accesso alla stessa rete di un *device*) ecc.

L'analisi presentata richiede pochissime risorse, basta un minimo di conoscenza tecnica per registrare pochi dati e poi visualizzarli opportunamente, pensate ora a quali siano le possibilità di analisi per chi abbia pressoché illimitate risorse hardware, software e di personale come alcune agenzie governative (es. la NSA statunitense o il GCHQ inglese, si veda sezione "*DataGate*" - 0.4) o grandi aziende con migliaia di utenti/clienti (Facebook, Google, Apple, Amazon).

Appendice B

"*Altri giorni altri occhi*"

```
Da ultimo, gli uomini si
abituarono alla presenza
universale delle spie di
Retardite, e impararono a
vivere senza sotterfugi e
senza vergognarsi come
facevano nel lontano passato
quando si sapeva che solo
l'occhio di Dio poteva vedere
dappertutto.
```

Bob Shaw

Nota bene

Questa sezione è stata lasciata in prima persona per scelta, è l'adattamento di un *blogpost* 🕮 che l'autore (A. Trentini) ha presentato in occasione di un Linux-Day milanese. Vuole essere una nota distopica su cosa ci riserva il futuro nel caso vincessero quelli del "non ho nulla da nascondere".

Al liceo ero un avido lettore di fantascienza. Oggi la fantascienza è stata quasi uccisa. Dal fantasy. Ma non è di questo che vi voglio parlare.

Uno dei miei autori preferiti, oltre ai classici naturalmente, era famoso nell'ambiente della SF[1], ma ben poco noto al di fuori: Bob Shaw.

Preferiti perché aveva (è morto nel 1996) un modo pulito di scrivere e i suoi schemi erano relativamente semplici, ma molto stimolanti e intelligenti.

Il *template* delle sue storie prevedeva di solito un singolo protagonista e il tutto si svolgeva in un contesto dominato da una qualche invenzione fantascientifica (appunto) che condizionava le vite di tutti e in particolare di quella del protagonista. Ad esempio l'antigravità ("*Vertigo*"), un sistema un po' erratico per navigare nell'iperspazio ("*Il cieco del non-spazio*"), l'immortalità ("*Un milione di domani*") ecc.

Uno dei suoi più noti romanzi, nato dall'unione di tre racconti, è "*Altri giorni altri occhi*" [Sha73]. Perché lo voglio citare qui? Perché trovo che sia una delle più azzeccate previsioni del futuro che io abbia mai letto. Non in termini di tecnologia (infatti non ci ha azzeccato per nulla), ma in termini di **conseguenze** di una tecnologia.

Leggiamone qualche brevissimo estratto, ecco l'*incipit*:

> *L'altra macchina era solo una piccola macchia rosso sangue nell'ondeggiante prospettiva dell'autostrada, ma anche a quella distanza e nonostante il barbaglio provocato dalla pupilla a forma di toppa del suo occhio sinistro, Garrod riuscì a identificare l'anno e il modello. Era una Stiletto del 1982. Spinto da un illogico senso di apprensione, sollevò il piede dall'acceleratore e la sua macchina, che marciava a centoquaranta chilometri all'ora, cominciò a rallentare.*
>
> *- Cosa c'è? - Come d'abitudine, sua moglie s'era subito allarmata.*

[1] Science Fiction.

- Niente.

- E allora perché rallenti? - A Esther piaceva tenere sempre d'occhio tutto quello che era di sua proprietà, categoria in cui era compreso anche il marito.

- Nessun motivo particolare. - Garrod sorrise protestando per l'interrogatorio senza smettere di osservare la Stiletto che ingrandiva a vista d'occhio. D'un tratto, come lui aveva previsto, il lampeggiatore di sinistra della Stiletto cominciò a emettere la sua luce arancione. Con una rapida occhiata, Garrod notò che la traversale cominciava in un punto a metà distanza tra le due macchine. Frenò facendo inclinare il muso della sua Turbo-Lincoln mentre i pneumatici aderivano stridendo alla strada. La Stiletto rossa li sorpassò con una sbandata e svanì nella strada laterale in mezzo a una nuvola di polvere color zafferano. Garrod ebbe la fulminea visione di una faccia giovanile dietro il finestrino sinistro della vettura sportiva. La bocca era un cerchio nero, turbato, accusatore.

- Ma l'hai visto? - I lineamenti fini di Esther si alterarono per un istante. - L'hai visto?

Dal momento che sua moglie si faceva portavoce della loro ira, Garrod fu capace di rimanere calmo.

- Certo che l'ho visto.

- Se tu non avessi rallentato, quello stupido ragazzo ci sarebbe piombato dritto addosso! - Esther tacque e si voltò a guardare, come se una idea l'avesse colpita.

- Ma perché hai rallentato, Alban? Sembrava quasi che sapessi cosa stava per succedere…

Si scopre poco oltre che il problema risiede nel parabrezza della Stiletto, fatto di un vetro speciale appena inventato, ma con un difetto molto particolare…

È l'invenzione che condiziona tutto il romanzo, il *vetro lento* (nel libro il materiale viene chiamato *Retardite*): un particolare tipo di vetro in cui la luce non viaggia alla velocità della luce, ma ad una velocità enormemente inferiore[2].

Il protagonista è coinvolto nella progettazione del nuovo parabrezza e ha già avuto alcune notizie su incidenti dovuti a ritardi di visione del guidatore.

Il vetro lento *trattiene* - senza distorsioni, cioè senza perdere informazione - la luce per molto tempo: ad esempio potreste prendere una lastra di vetro lento, starci davanti per qualche secondo, girarlo di 180 gradi e vedervi apparire poco dopo.

Man mano che si avanza nel libro il vetro lento viene sempre più perfezionato fino ad ottenere lastre sottilissime con tempi di attraversamento lunghissimi (anche di anni). Con più o meno ovvie conseguenze: vengono creati lampioni usando semplici pezzi di vetro lento con periodo 12 ore (di giorno assorbono la luce solare, di notte la rilasciano dall'altra parte), si possono *vendere* paesaggi semplicemente esponendo per qualche mese lastre di vetro su un bel panorama per poi venderle come pannelli da muro a chi sta in città... e via così.

Bello, voi direte, sarebbe fantastico avere una tecnologia del genere!

Già, quasi.

Il fatto è che il perfezionamento del vetro si spinge così in avanti che verso la fine del libro riescono ad ottenere lastre di vetro lentissimo e sottilissimo nonché un meccanismo per estrarre le informazioni a comando. Questo permette la creazione di scaglie di vetro lento microsocopiche che, come viene raccontato nelle ultime pagine del libro, vengono sparpagliate a miliardi su tutta la terra... ora capite dove si va a parare?

[2]Inteso, la luce viaggia alla velocità della luce solo nel vuoto, negli altri mezzi è più lenta, ma di poco, nella Retardite parliamo di tempi che variano dai secondi agli anni per centimetro di materiale da attraversare.

Vediamo il finale che oserei definire *visionario*, in senso profetico, del nostro tempo:

> *Esther gli pose le mani sulle spalle, e mormorò:*
> *- Mio povero Alban.*
> *Garrod nascose la faccia tra le mani. «Non ci sono satelliti» pensava. «Niente razzi che portano giù dall'orbita le spie di Retardite. Non ce n'è bisogno, dal momento che stanno cospargendo tutto il mondo di polvere di vetro lento!»*
> *Una calma soprannaturale scese sulla sua mente mentre traeva le deduzioni. La Retardite aveva una struttura cristallina così microscopica che era possibile ricavare immagini utili da frammenti di pochi micron, frammenti invisibili a occhio nudo in condizioni normali. L'usavano a migliaia di tonnellate... polvere di Retardite con periodi di ritardo graduati, che scendevano roteando sul continente spruzzati da piccoli aerei. E le minuscole particelle ricadevano ovunque: sulle case, sui fiori, sui pali del telegrafo, sulle pendici delle montagne, sugli uccelli, sugli insetti che volavano, sugli abiti, sui cibi, nell'acqua...*
> *«D'ora in avanti» urlò una voce silenziosa nel suo cervello, «chiunque, purché disponga delle apparecchiature adatte, può scoprire qualunque cosa su CHIUNQUE! Questo pianeta sta diventando un unico, enorme occhio sempre all'erta, intento a osservare tutto quello che avviene sulla sua superficie.*
> *Siamo chiusi in una prigione di vetro che ci soffoca, come insetti nella bottiglia di un entomologo. E io... io sono la causa di tutto!»*

Questa è la vera visione futuristica (e distopica?) che ci propone Shaw sul finale, un nuovo mondo che sta nascendo… Un mondo in cui tutti sono *oggetto* di una sorveglianza

globale controllata da chi dispone delle apparecchiuature adatte: **un mondo senza privacy.**

In questo mondo pervaso da scaglie microscopiche di vetro lento è pressoché impossibile trovare (o creare, tentando una *disinfezione*) un ambiente perfettamente pulito, completamente privo di scaglie. Qualunque avvenimento, ovunque accada, verrà con altissima probabilità catturato da qualche scaglia di vetro lento e sarà facilissimo per chiunque raccogliere quelle scaglie ed estrarne le informazioni.

Ecco infatti l'epilogo:

> *Jane lo aiutò standogli vicina quando lui andò alla sede di un giornale a raccontare la sua storia, fu accanto a lui nei lunghi mesi in cui il governo, preso dal panico, fu costretto a furor di popolo a emanare nuove leggi che vietavano la produzione di vetro lento.*
>
> *Fu accanto a lui durante gli anni ancora più difficili durante i quali si scoprì che altri paesi continuavano a produrre Retardite, adulterando con essa gli oceani, l'aria stessa, e perfino la stratosfera. Da ultimo, gli uomini si abituarono alla presenza universale delle spie di Retardite, e impararono a vivere senza sotterfugi e senza vergognarsi come facevano nel lontano passato quando si sapeva che solo l'occhio di Dio poteva vedere dappertutto.*
>
> *Jane gli fu vicina durante tutte queste vicissitudini, e uno dei motivi per cui lui l'amava era che, per quanto si sforzasse, non riusciva a vedere invecchiare il suo bellissimo viso. Per lui era senza età, eterna. Una stupenda immagine racchiusa per sempre in un prisma di vetro lento.*

Fantascienza per fortuna, dai, non si avvererà mai, non esiste il vetro lento. Sicuri? Il mondo senza privacy in realtà è già qui: **i pezzetti di vetro lento sono già**

tra noi. E la Retardite sarebbe (se esistesse davvero) un oggetto fisico, tutto sommato difficile da forgiare, ricordate che invece i bit sono molto più malleabili.

In sezione "*DataGate*" - 0.4 abbiamo descritto programmi di sorveglianza globale, vedremo a breve anche cosa fanno le *app* che raccolgono (o che sempre più spesso noi stessi forniamo loro) dati su di noi, poi ci sono i device indossabili (oggi solo telefoni e *smartwatch*, domani?) dotati di microfoni, telecamere e dispositivi di localizzazione e infine i *device smarthome*[3], alcuni dei quali si introducono nella vostra vita privata senza chiedere il permesso[4].

Non dico che queste cose sono *Il Male™*, ci mancherebbe, non faccio crociate contro la tecnologia, sono pur sempre un tecnofilo, ma retoricamente mi domando: dobbiamo davvero rassegnarci ad avere tecnologie che *annientano il nostro diritto all'anonimato*, sono controllate *da altri* indipendentemente dalla nostra volontà e consentono ai *controllori* di raccogliere moli impressionanti di dati potenzialmente eterni per una *eterna profilazione* delle nostre persone?

"Non sono convinto" direte voi, "hai descritto un mondo fantascientifico e impossibile da realizzare: il vetro lento non esiste, non c'è modo di fare *data harvesting*[5] su così larga scala!" Se ciò che vi abbiamo raccontato fin qui, specie a proposito del DataGate (sezione "*DataGate*" - 0.4) non vi ha ancora convinto provate a leggere quest'ultima notizia[6] di cui forniamo un breve estratto:

> ***La polizia usa i lampioni per spiare la cittadinanza***

[3] Amazon Echo, Google Home.

[4] Termostato Nest (*http://theverge.com/circuitbreaker/2019/2/20/18232960/google-nest-secure-microphone-google-assistant-built-in-security-privacy*), Samsung TV (*http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/index.html*)

[5] Raccolta dati, il termine inglese (*mietitura*) è molto più immaginifico rispetto a quello italiano.

[6] *https://www.zerohedge.com/news/2019-08-09/san-diego-cops-used-streetlamps-spy-public-more-140-times*

...

La città [di San Diego] ha installato circa 3.200 lampioni-telecamera e prevede di averne circa 4.200 entro l'estate prossima. I funzionari della General Electric e del governo hanno promosso il sistema come "la più grande piattaforma di smart city al mondo".

Trasformare San Diego nella "più grande piattaforma di smart city al mondo" assume un significato completamente nuovo quando ti rendi conto che la città ha almeno 40.000 lampioni.

Riesci a immaginare un'intera città coperta di 40.000 lampioni-spia? Riesci a immaginare gli USA coperti da oltre 26 milioni di lampioni-spia?

...

Altro che vetro lento, entro pochi anni tra IoT (*Internet of Things*) pervasivo, droni invasivi, monitoraggio e controllo fatto tramite *machine learning* e profilazione saremo letteralmente invasi da tecnologia per la sorveglianza di massa e ciascuno di noi sarà **schedato** da decine di enti, ognuno di essi con il proprio *nobile* scopo.

Concludo con una domanda provocatoria: "sareste voi veramente capaci di vivere sotto l'occhio costante di Dio?"[7]

[7] Il Dio tecnologico ovviamente, quello che esiste.

Glossario

account - Indica un insieme di informazioni che identificano l'utente di un sistema, al minimo si tratta di *nome utente* e *password*, solitamente include anche altri dati come telefono, mail, dati anagrafici vari, ecc.
. . . . . 128, 320

algoritmo - Un algoritmo è un procedimento che risolve un determinato problema attraverso un numero finito di passi elementari, chiari e non ambigui, in un tempo ragionevole. Il termine deriva dalla trascrizione latina del nome del matematico persiano al-Khwarizmi vissuto nel IX secolo d.C., che è considerato uno dei primi autori ad aver fatto riferimento a questo concetto scrivendo il libro "*Regole di ripristino e riduzione*" (Wikipedia).
. 42

app (contrazione di *application*) - Termine che indica un programma per computer nel contesto degli smartphone/tablet.
. 126

banda passante (larghezza di banda) - Ai fini di questo testo è di fatto un sinonimo di *velocità di trasmissione* dei dati.
. 23

bit - Un *bit* è l'unità minima di informazione, può assumere solo i valori 0 e 1, il suo multiplo, il *byte* consta di 8 *bit*.
. . . . . 33, 37, 46, 70

bit/s (*bit per second*) - bit al secondo, unità di misura della velocità di trasmissione per i dati, attualmente si usano i suoi multipli: k(ilo) 1000bit/s e M(ega) 1000kbit/s. Ad esempio un filmato da 100MB su una linea da 30Mbit/s viene trasmesso in

$$\frac{100*1024*1024*8bit}{30*1000*1000bit/s} \approx 30s$$

(circa perché vanno conteggiati anche gli *overhead* per il controllo degli errori di trasmissione).
. 183

blackbox - Alla lettera: *scatola nera, opaca*. Descrive un oggetto, un apparecchio, un sistema, di cui si **non** può conoscere il funzionamento interno in **nessuna** sua parte, contrario di *whitebox* 🕮.
. 323

blockchain - In pratica sono database distribuiti (nel senso che ogni nodo appartenente alla blockchain possiede una copia dell'intero database) a cui si possono soltanto aggiungere dati in maniera firmata e crittografata.
. 84

blogpost - Un *blog* è una sorta di diario, di raccolta di articoli (a volte personali, a volte tecnici ecc.) accessibile via web, un *blogpost* (o anche semplicemente *post* o *blog* - ma il termine fa confondere la parte per il tutto - da soli) è semplicemente una *pagina* del diario.
. . . . . 31, 302

bot - contrazione di "robot", un programma che esegue accessi in rete simulando un essere umano, di solito

vengono creati per tentare di accedere a servizi in maniera programmativa (senza intervento umano) sia a scopi utili e benefici (aggregazione/trasformazione di informazioni) sia a scopi criminali (tipicamente *password guessing*).
. 206

byte - Multiplo del *bit*, un *byte* contiene 8 *bit*.
. . . . . 33, 37, 63

crowdfunding (finanziamento di massa) - Meccanismo per cui i proponenti di un progetto che necessitano di finanziamenti ne pubblicano la descrizione (su un sito di *crowdfunding*, appunto) e chiedono microfinanziamenti ad una larga base di utenti. Questi ultimi ricevono in cambio riconoscimenti formali (ringraziamenti sul sito stesso) o sostanziali (ad esempio i primi prototipi prodotti).
. 191

crowdsourcing - Meccanismo di raccolta di informazioni basato sulla *massa di persone* (*crowd*): se ognuno raccoglie e notifica un dato (anche piccolo, ad esempio la foto di una buca stradale, geolocalizzandola) l'insieme delle notifiche fatte da un nutrito gruppo di utenti (nell'esempio: utenti della strada) rappresenta un completo *dataset* dello stato di un sistema (es.: le strade), se questa informazione è (ri)condivisa verso tutti gli utenti tutti ci guadagnano perché otterranno anche le informazioni non raccolte personalmente. Faranno tutti parte di un sistema *collaborativo*. Un esempio commerciale è `http://waze.com` che raccoglie le informazioni sul traffico dai guidatori stessi. Un esempio libero, sempre in tema *stradale* è `http://openstreetmaps.org`, gigantesco archivio di informazioni geografiche caricate da singoli utenti sparsi per il mondo.
. . . . . 14, 29, 112, 216

data cap - Genericamente (e letteralmente) indica un *tappo* per i dati, un meccanismo secondo cui una connessione che normalmente fornisce una certa prestazione (velocità, costo ecc.) al raggiungimento di una certa condizione, tipicamente quando si supera una certa quantità di dati trasmessi in un periodo di tempo, cambia regime prestazionale.Esempio: una connessione *flat* con *data cap* da 10GB al mese a 10 euro indica che la connessione costa 10 euro al mese fino a che non si raggiungono i 10GB di traffico totale, al superamento della soglia alcuni provider rallentano la velocità ma non applicano tariffe aggiuntive; altri lasciano la velocità invariata ma applicano tariffe aggiuntive; altri ancora disabilitano in toto la funzione dati. Cfr. *http://berec.europa.eu/eng/netneutrality/zero_rating*.
. . . . . 61, 62, 193

default - Opzione "di default" indica quell'impostazione che viene utilizzata se non intervengono scelte dell'utente, e.g., la suoneria *di default* di un telefono è quella impostata in fabbrica.
. . . . . 54, 108, 223

DHCP (*Dynamic Host Configuration Protocol*) - Meccanismo per cui in un tratto di rete esiste un gestore autoritativo degli *identificativi* che si occupa di assegnare indirizzi IP univoci ai nodi che vi si connettono, in modo da non avere duplicati. Il protocollo prevede che ogni device che voglia connettersi debba prima consultare il gestore per farsi assegnare l'indirizzo e solo dopo possa comunicare normalmente con gli altri nodi della rete.
. 296

firewall - Apparato di rete analogo ad un router (spesso i due ruoli sono inglobati nello stesso device), ma specializzato nel *filtraggio* sull'instradamento dei pacchetti: il firewall infatti decide **se** instradare o meno

un flusso/pacchetto in funzione di varie *policy* (orario, provenienza, tipo di traffico ecc.).
. 56

FISA - *Foreign Intelligence Surveillance Act* del 1978 è una legge federale USA che stabilisce le procedure per la intercettazione e raccolta fisica e elettronica di informazioni di intelligence tra potenze straniere e agenti delle potenze straniere sospetti di spionaggio o terrorismo.
. . . . . 92, 96

Five Eyes - (cinque occhi) Anche abbreviato FVEY: le aziende di intelligence di Australia, Canada, Nuova Zelanda,UK e USA.
. . . . . 89, 92, 93, 96, 97, 102

Hello World - Termine che indica l'esempio veramente banale da provare quando si inizia a studiare un linguaggio di programmazione, giusto per capire il processo minimo di produzione di un programma. Si veda `http://helloworldcollection.de` per una collezione di esempi nei vari linguaggi.
. 128

in chiaro - Non crittografato, visibile/leggibile da chiunque.
. 108

IoT (*Internet of Things*) - *Internet delle cose*, oggetti digitali come sensori e attuatori capaci di connettersi in rete per implementare funzioni di monitoraggio e controllo di ambienti qualsivoglia.
. 106

ISP (*Internet Service Provider*) - Azienda che fornisce connettività agli utenti sia via cavo che wireless. Può utilizzare strutture (cavi, fibre ottiche, ponti radio ecc.) proprie o può *comprare connettività all'ingrosso* da altri ISP per rivenderla sul territorio (in questo

caso si parla di fornitore *virtuale*).
. . . . . 54, 67, 84, 190–193, 198, 230

jailbreak (evasione) - Quasi tutti gli smartphone odierni impediscono (o rendono macchinoso) all'utente di assumere il rango di *amministratore* del *device*, tale ruolo serve quando si vuole ad esempio installare un *firewall* (filtro di rete) o un *adblocker* (anti pubblicità); la pratica del *jailbreak* è un insieme di tecniche per scavalcare gli impedimenti e avere finalmente il pieno controllo del *device* acquistato.
. 146

JavaScript - Linguaggio di programmazione vero e proprio, utilizzato principalmente per rendere *attive* le pagine web. Oggigiorno una pagina web è di fatto un insieme di programmi che girano all'interno del browser del personal computer dell'utente che ha aperto la pagina stessa.
. 58

log - Nome generico per un *diario di bordo* digitale, tipicamente sottoforma di un insieme di *log file* 🕮, serve a tenere uno storico del funzionamento di un computer, ad esempio per risalire alle cause di eventuali errori e malfunzionamenti, ma anche per sapere *chi ha fatto cosa* in caso di necessità di attribuzione di responsabilità delle azioni.
. 78

log file - I cosiddetti *file di log* sono quei dati, che un sistema genera durante il suo funzionamento, che registrano lo stato di salute del sistema stesso, gli eventi significativi e quanto altro possa essere utile a capire se un sistema sta facendo (o ha fatto, dato che a volte si usano *post mortem*) quello per cui era stato installato.
. . . . . 159, 296, 315

lossy - Letteralmente *in perdita*, si dice di protocolli di rete o di immagazzinamento che non garantiscono l'integrità completa del dato in ingresso a favore di un miglior rapporto di compressione. Un esempio comprensibile è quello di una immagine a colori, alcuni formati di immagazzinamento *lossy* (es. jpeg) decidono di accorpare sfumature di colore che magari non sarebbero facilmente distinguibili all'occhio umano risparmiando preziosi (su una connessione lenta) bit.
. 59

mac address - Il *mac address* è un particolare tipo di indirizzo fisico assegnato ad un device di rete in sede di costruzione, solitamente non cambia nel corso della vita del device e ne permette l'identificazione univoca sulla rete locale.
. 297

meme - tipicamente un'immagine (anche un fumetto composto da una sequenza di immagini) o una frase che rappresenta molto bene ma sinteticamente un concetto, spesso con stile umoristico/ironico/satirico, e che si propaga *viralmente* (ad esempio attraverso *repost* sui *social network*) e diventa molto noto e riutilizzato.
. 174

motore di ricerca - Un servizio che *conosce* buona parte dei contenuti in rete e che quindi sa dire dove si trova un particolare contenuto. Un m.d.r. passa la sua vita consultando la rete in lungo e in largo leggendo pagine e pagine (web, ma non solo) e registrando i relativi URL incamerando tutta questa informazione in un proprio (enorme) database. Tale database funziona da mappa ($contenuto \rightarrow URL$).
. 53

neo-luddismo - rivisitazione dell'antico luddismo (movimento anti-tecnologico dei primi del 1800, contrario

alle macchine che "rubavano il lavoro" come i telai). I neo-luddisti applicano il filosoficamente fallace "principio di precauzione" a qualunque nuova tecnologia (es. del 2020: il 5G) chiedendone la non adozione o l'abbandono. Sono spesso associati a ideologie anti-globalizzazione, anti-scientifiche ed eco-estremiste.
. . . . . 31, 224

opendata - Vanno sotto il nome di *opendata* tutti quei dati, più o meno strutturati, che vengono resi disponibili su web in forma standardizzata, accessibile programmativamente (i.e., analizzabile attraverso programmi per computer) e libera (il cui accesso/uso/elaborazione non è vincolato). Oggigiorno quasi tutte le amministrazioni pubbliche rendono disponibili *dataset* accessibili liberamente tramite i cosiddetti *opendata portal*, ad esempio `http://dati.gov.it` o `http://dati.lombardia.it`.
. . . . . 19, 140, 260, 275, 276

peer-to-peer - Tecnica di scambio file per cui ogni nodo della rete che partecipa alla condivisione dei file funge sia da fruitore che da fornitore, i programmi di scambio P2P (abbreviazione) scaricano i file e contemporaneamente li condividono verso altri utenti in modo da distribuire il traffico di rete su tutti i partecipanti e non aggravare un singolo server di carichi troppo elevati. Inoltre questa distribuzione dell'informazione rende molto più robusta l'architettura perché anche se qualche nodo *cade* (viene spento o va offline) gli altri continuano a condividere avendo ognuno copie dei contenuti. Questa tecnica viene spesso criminalizzata dato che è uno dei principali modi per scambiare *illegalmente* contenuti sotto copyright.
. . . . . 55, 62, 116

PKI - *Public Key Infrastructure* è l'unsieme di ruoli, regole e risorse (hardware e software) necessarie a creare,

gestire, distribuire, usare, immagazzinare e revocare i certificati digitali necessari per la crittografia a chiave pubblica.
. 111

proxy - Un *proxy* è un servizio/device che accetta connessioni per *conto terzi*: esso si trova in un qualche punto della rete e attende richieste (ad esempio l'apertura di un URL http) da parte di altri device (tipicamente autenticati mediante password), quando ne riceve una la effettua restituendo il contenuto ottenuto al richiedente originale. L'effetto pratico è che la connessione effettiva avviene dal luogo dove si trova il proxy e non da quello del richiedente originale.
. 55

repository - genericamente il termine indica un'area di immagazzinamento di file strutturata e *versionata*, nel contesto del mondo Android si riferisce ad una fonte da cui installare programmi per il proprio telefono.
. 145

reverse engineering - In informatica, il *reverse engineering* è il processo di analisi di un sistema software esistente, eseguito al fine di comprenderne il funzionamento per essere in grado di crearne una rappresentazione ad alto livello di astrazione. In genere le pratiche di reverse engineering vengono utilizzate quando un produttore software mantiene segreto il codice sorgente e non documenta protocolli e formati utilizzati, in questo caso si deve ricorrere al reverse engineering per essere in grado di progettare e realizzare sistemi interoperabili.
. . . . . 135, 138, 142, 143, 156

ROM - (*Read Only Memory*) nel contesto del mondo Android si riferisce alla *versione* del sistema operativo

installato, esistono le cosiddette *stock ROM* (quelle installate in origine dal produttore del telefono) e quelle alternative, realizzate da sviluppatori indipendenti, che sono di solito più configurabili dell'originale.
. 145

rooting/jailbreaking - Alla lettera: *diventare amministratore / uscire di prigione*. Nel contesto degli *smartphone* il termine si riferisce alla pratica (tecnica e non burocratica) di ottenere i diritti di amministrazione (il pieno possesso e controllo) dei device acquistati. Un telefono Android o (peggio) Apple appena comprato relega l'acquirente a mero utilizzatore con pochissime possibilità di reale controllo dell'apparato, mediante il *rooting* (operazione a volte complessa e spesso contrattualmente "scoraggiata" dai produttori che cercano di non riconoscere la garanzia di un telefono così modificato) si riesce a diventare i reali possessori dell'oggetto.
. 223

router - Apparato di rete (computer specializzato) che si occupa di gestire l'*instradamento* (appunto) dei pacchetti che lo attraversano. Ha solitamente più interfacce di rete e deve scegliere, per ogni flusso entrante da un'interfaccia, verso quale ramo della rete inviare i dati, in funzione di parametri di efficienza, costo, scelta politica, scelta contrattuale ecc.
. . . . . 42, 296

scam - Tecnica di raggiro che sovente prevede l'invio di una comunicazione che sembra legittima e che invita a collegarsi ad un sito (finto, ma il cui URL assomiglia molto ad un sito noto all'utente) per "cambiare password perché è stata *craccata*", l'utente disattento si collega al sito trappola (la pagina viene costruita copiando quella del sito reale) e digita le proprie credenziali (login e password) che a questo punto ven-

gono a conoscenza dello *scammer* (il criminale).
. 54

SIGINT - *Signal INTelligence*, attività di raccolta di informazioni mediante l'intercettazione e analisi di segnali, sia emessi tra persone (ad esempio comunicazioni radio) sia tra macchine. Dal momento che molte comunicazioni riservate sono criptate, le operazioni di SIGINT spesso si avvalgono di strumenti di crittoanalisi.
. 93

silos informativi - un silo informativo è un sistema di gestione isolata delle informazioni nel quale ciascun singolo sistema informativo non è in grado di operare con gli altri che sono o dovrebbero essere correlati. In tal modo l'informazione non è adeguatamete condivisa ma piuttosto resta confinata in ciascun sistema, figurativamente intrappolata in un contenitore come il grano in un silo. Un esempio di silo informativo sono le reti sociali come Facebook, Whatsapp o Telegram.
. 30

sniffing - (annusare) tecnica passiva di cattura delle informazioni, viene osservato (agganciandosi alla stessa rete da *attaccare*) il traffico dati nella speranza che passino informazioni *utili* (password e altri codici di accesso ai sistemi).
. 149

SPID (Sistema Pubblico di Identità Digitale) - Meccanismo di autenticazione nazionale per l'identificazione degli utenti/cittadini. Fornisce un *account* 🕮 certificato (l'identità viene controllata tramite verifica dei documenti fisici) unico per l'accesso a molti servizi sul territorio nazionale italiano. Per ottenerlo ci si può presentare presso gli sportelli fisici dei vari fornitori SPID o si può anche effettuare un riconoscimento via webcam mostrando online il proprio documento

di identità.
. . . . . 128, 129, 207

SSD (*Solid State Drive*) - *Disco* (tra virgolette perché non ha più forma circolare) a stato solido, di fatto una memoria (come RAM, ROM, flash, …) velocissima, alcuni ordini di grandezza più veloce di un un disco tradizionale (*rotational*), che viene utilizzata al posto dei dischi meccanici. Ha un costo per GB superiore ai dischi tradizionali.
. 75

SSH (*Secure Shell*) - Protocollo crittografico per comunicazioni sicure su reti non sicure, attraverso un *client* e un *server* è possibile aprire una *sessione* remota (protetta crittograficamente da *sguardi indiscreti*) per operare su un computer molto distante come se ci si trovasse davanti, usato tipicamente per manutenzione di server.
. 57

stringa - Una sequenza di simboli.
. 80

timeout - Termine che indica un tempo oltre il quale un evento atteso si deve dare per perso.
. 56

TLD (*Top Level Domain*) - Sono i domini di *primo livello*, la parte finale di un *URL* 🕮, i vari ".it", ".com", ".gov", ecc.
. . . . . 64, 65

UKUSA - Accordo SIGINT sotttoscritto nel 1948 fra Gran Bretagna (Regno Unito, UK), Stati Uniti (USA), Australia, Canada e Nuova Zelanda.
. . . . . 93, 104

ultimo miglio - Si definisce *ultimo miglio* quel tratto della rete che va dalla casa/ufficio dell'utente finale fino

al primo concentratore (ad es. l'armadio di rete in strada), è il tratto più problematico perché è difficilmente *aggiornabile*; tipicamente è il doppino in rame della rete telefonica che viene utilizzato per veicolare dati; il rame è un buon conduttore di elettricità, ma quando si tratta di inviare dati (segnali ad alta frequenza) invece di voce (segnali a bassa frequenza) il doppino diventa una pessima soluzione per le lunghe (centinaia di metri) distanze. Nel corso del tempo sono stati inventati protocolli sempre più sofisticati (il più recente è il VDSL2) che permettono velocità dell'ordine del centinaio di Mbit/s, ma la vera soluzione radicale è la sostituzione con la fibra ottica (Gigabit/s) ove possibile.
. . . . . 33, 59

URL (*Uniform Resource Locator*) - Meccanismo standardizzato per identificare una *risorsa* (ad es. un documento, una foto, un video ecc.) in rete specificando dove si trova (sito, nodo della rete). Es. http://tecnocivismo.di.unimi.it/index.html indica la risorsa *index.html* che si trova sul server *tecnocivismo* nella rete interna a *di.unimi.it*, raggiungibile attraverso il protocollo HTTP.
. . . . . 53, 134, 158, 321

VPN (*Virtual Private Network*) - Meccanismo software che permette di creare un *tunnel di rete* tra il luogo dove ci si trova (tipicamente in giro per il mondo, magari presso clienti o da un albergo o un wifi pubblico) e una propria rete conosciuta (ad esempio la propria rete aziendale). Una volta instaurato il tunnel, il computer connesso tramite VPN appare in rete come se fosse connesso alla propria rete e non a quella temporanea che fa solo da trasporto. Esempio pratico, mi trovo in un albergo e utilizzo il wifi offerto dalla struttura: a) senza alcuna VPN il mio traffico di rete appare provenire dalla rete dell'albergo e *vede* lo stato della rete Internet visibile dall'albergo

stesso; b) con una VPN verso la mia rete aziendale il mio traffico di rete appare provenire dalla stessa e *vede* lo stato della rete Internet visibile dalla mia azienda. Ovviamente nel bene e nel male: nel caso a) sono vincolato al firewall dell'albergo, nel b) a quello dell'azienda. Se il firewall dell'albergo impedisce l'uso di VPN sono costretto a usare la soluzione a).
. . . . . 66, 68, 114, 155

walled garden - in tecnologia, un *walled garden* - detta anche piattaforma chiusa - è un sistema software all'interno del quale il fornitore del servizio ha il controllo sulle applicazioni e sui contenuti, impedendo l'accesso agli utenti non autorizzati.
. 30

whistleblower - Alla lettera: *colui che soffia nel fischietto*. Indica un soggetto che, a volte violando norme e regole (il caso classico è l'esfiltrazione di documenti interni/segreti) o addirittura a rischio della propria incolumità, porta all'attenzione del pubblico fatti deprecabili e/o criminosi.
. 122

whitebox - Alla lettera: *scatola bianca, trasparente*. Descrive un oggetto, un apparecchio, un sistema, di cui si può conoscere il funzionamento interno in ogni sua parte, contrario di *blackbox* 🕮.
. . . . . 214, 311

Acronimi

2FA *Two Factor Authentication* 146, 150

ACLU *American Civil Liberties Union* 62, 191

ACTA *Anti Counterfeiting Trade Agreement* 215, 230

ADSL *Asymmetrical Digital Subscriber Line* 41, 58, 59, 194, 244, 293

AFR *Annualized Failure Rate* 73

AGCOM Autorità per le Garanzie nelle Comunicazioni 193, 277, 278

AICA Associazione Italiana per l'Informatica e il Calcolo Automatico 251

API *Application Programming Interface* 139, 140

b2b *business to business* 139

BEREC *Body of European Regulators for Electronic Communications* 192

BGP *Border Gateway Protocol* 42, 109

BYOD *Bring Your Own Device* 270, 273

CA *Computing Agency* 238, 239, 242, 243, 287

CAD Codice dell'Amministrazione Digitale 289

CDP Cassa Depositi e Prestiti 198

CDT Cittadinanza Digitale e Tecnocivismo 12, 16, 19, 21, 26, 30, 33, 34, 88, 94, 132, 195, 221, 259, 261, 262, 268, 270, 291

CIA *Central Intelligence Agency* 90

CIE Carta Identità Elettronica 209

CISA *Cybersecurity Information Sharing Act* 231

CISPA *Cyber Intelligence Sharing and Protection Act* 231

DMCA *Digital Millennium Copyright Act* 232, 292

DNS *Domain Name System* 54–56, 64, 65, 110, 119

DRM *Digital Rights Management* 215, 240

DRM *Digital Restriction Management* 215, 230, 240, 291

DSL *Digital Subscriber Line* 27

ECDL *European Computer Driving License* 266

EFF *Electronic Frontier Foundation* 191

EULA *End-User License Agreement* 282, 284

FCC *Federal Communication Commission* 192, 193

FOIA *Freedom Of Information Act* 276

FTTP *Fiber To The Premises* 186

FUD *Fear, Uncertainty and Doubt* 288

GCHQ *Government Communications Headquarters* 100

GDPR *General Data Protection Regulation* 149, 160, 168, 201

GNS *GNU Naming System* 119

GSoC *Google Summer of Code* 136

HADOPI *Haute Autorité pour la Diffusion des Œuvres et la Protection des droits d'auteur sur Internet* 215, 229

HCI *Human Computer Interaction* 151

ICMP *Internet Control Message Protocol* 42

ICT *Information and Communication Technologies* 13, 185, 243, 247

IETF *Internet Engineering Task Force* 24

IoT *Internet of Things* 120, 215, 216, 218, 239, 309, 314

IP *Internet Protocol* 51

ISDN *Integrated Services Digital Network* 244

KPI *Key Performance Indicator* 24, 140, 272, 275

L0-network Livello 0 [*The Net*] 17, 21–24, 33, 262, 271

L1-services Livello 1 [*services*] 17, 22–27, 35, 124, 157, 262, 271

L2-access Livello 2 [*access*] 17, 21–23, 25, 28, 35, 172, 262, 269, 271

L3-education Livello 3 [*education*] 3, 17, 21, 23–29, 35, 216, 262, 271, 280, 287, 291

L4-transparency Livello 4 [*transparency*] 17, 18, 21, 23, 25–29, 35, 260, 262, 271, 273, 276, 280

L5-participation Livello 5 [*participation*] 17, 18, 25–29, 35, 174, 262, 269, 271, 280

L6-consultation Livello 6 [*consultation*] 17, 18, 25, 26, 28, 35, 174, 262, 271

L7-democracy Livello 7 [*democracy*] 17, 18, 25, 26, 35, 174, 262, 271

LIM Lavagna Interattiva Multimediale 266, 278

LOC *Lines Of Code* 218, 219

MdT Macchina di Turing 81, 82

MIT *Massachusetts Institute of Technology* 285

MITM *Man-In-The-Middle* 111

MTBF *Mean Time Between Failures* 73, 74

NGA *Next Generation Access* 183, 184

NGA-VHCN *Next Generation Access - Very High Capacity Networks* 183, 184, 198

NSA *National Security Agency* 89–101, 103, 106, 301

OCSE Organizzazione per la Cooperazione e lo Sviluppo Economico 249, 268, 274

OECD *Organisation for Economic Co-operation and Development* 25

OSI *Open Systems Interconnection* 18

OTP *One Time Password* 209

P.A. Pubblica Amministrazione 124, 140, 151, 171, 203, 207, 289

PEC Posta Elettronica Certificata 202–204

PIPA *PROTECT IP Act* 215, 231

PNSD Piano Nazionale Scuola Digitale 264, 267–270, 272, 275–278, 294

POF Piano dell'Offerta Formativa 273

PON Programma Operativo Nazionale 272

RAID *Redundant Array of Inexpensive Disks* 74–76, 79

RAM *Random Access Memory* 73

REST *REpresentational State Transfer* 139

RFC Request For Comments 134

RMS Richard Matthew Stallman 285

SIP *Session Initiation Protocol* 210

SL Software Libero 285–289, 292

SLA *Service Level Agreement* 177, 179–181

SOPA *Stop Online Piracy Act* 215, 231

SSO *Single Sign On* 206

TCP/IP *Transmission Control Protocol / Internet Protocol* 2, 33, 48, 191, 236, 237

TPP *Trans Pacific Partnership* 230

TTIP *Transatlantic Trade and Investment Partnership* 230

UE Unione Europea 144, 197, 255, 268, 279

UEFI *Unified Extensible Firmware Interface* 215

UX User Experience 131

VDSL *Very-high-bit-rate Digital Subscriber Line* 27, 58, 244

VoIP *Voice over Internet Protocol* 210, 293

WYSIWYG *What You See Is What You Get* 221

XML *eXtensible Markup Language* 210

Bibliografia

[AAV87] AAVV. *Constitution of the United States*. USA government, 1787. URL: http://www.loc.gov/rr/program/bib/ourdocs/Constitution.html.

[Ack14] Spencer Ackerman. «US tech giants knew of NSA data collection, agency's top lawyer insists». In: *The Guardian* (2014). URL: http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de.

[AD08] Alessandro Aurigi e Fiorella De Cindio. *Augmented urban spaces: articulating the physical and electronic city*. Ashgate Publishing, Ltd., 2008.

[AGC16] AGCOM. «Attività di vigilanza in materia di net neutrality». In: (2016). URL: http://www.agcom.it/documents/10179/8099412/Documento+generico+19-07-2017/22e98e3c-09f2-414e-9b78-a3642898f6b1?version=1.0.

[AGC19] AGCOM. *Educare digitale - Lo stato di sviluppo della scuola digitale - Un sistema complesso ed integrato di risorse digitali abilitanti*. Feb. 2019. URL: http://www.agcom.it/documents/10179/14037496/Studio-Ricerca+

28-02-2019/af1e36a5-e866-4027-ab30-5670803a60c2?version=1.0.

[Ali12] Simone Aliprandi. *Capire il copyright : percorso guidato nel diritto d'autore*. Milan, Italy: Ledizioni, 2012. ISBN: 9788867050116.

[Ali14] S. Aliprandi. *Apriti standard!: Interoperabilità e formati aperti per l'innovazione tecnologica*. CopyLeft Italia. Ledizioni, 2014. ISBN: 978-88-95994-87-1.

[All+17] J. Allen et al. «Study on net-neutrality regulation». In: (2017). URL: http://berec.europa.eu/eng/document_register/subject_matter/berec/others/7243-study-on-net-neutrality-regulation.

[And+97] Robert H Anderson et al. «Universal access to e-mail: Feasibility and societal implications». In: *Educational Media International* 34.2 (1997), pp. 86–87.

[Arn69] Sherry R Arnstein. «A ladder of citizen participation». In: *Journal of the American Institute of planners* 35.4 (1969), pp. 216–224.

[Bar18] Raffaele Barberio. «Parliamo di Russia, ma la vera anomalia sul "data retention" è l'Italia». In: *Huffington Post* (Luglio 2018).

[Bau09] M. Bauerlein. *The Dumbest Generation: How the Digital Age Stupefies Young Americans and Jeopardizes Our Future (or, Don't Trust Anyone Under 30)*. Jeremy P. Tarcher/Penguin, 2009. ISBN: 9781585427123. URL: http://books.google.it/books?id=yaYADQEACAAJ.

[BG13] Luke Harding James Ball e Juliette Garside. «BT and Vodafone among telecoms companies passing details to GCHQ». In: *The Guardian* (2 ago. 2013). URL: http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq.

[Bia16] Simonetta Biagio. «L'India boccia l'Internet gratis di Zuckerberg: non rispetta la net neutrality». In: (2016). URL: http://www.ilsole24ore.com/art/tecnologie/2016-02-08/l-india-boccia-internet-gratis-zuckerberg-non-rispetta-net-neutrality-140053.shtml.

[Bil14] Nick Bilton. «Corsie preferenziali». In: *Internazionale (da The New York Times)* 1038 (feb. 2014), p. 91.

[Bir+17] Henry Birge-Lee et al. «Using BGP to Acquire Bogus TLS Certificates». In: *PETS 2017*. Privacy Enhancing Technologies Symposium (PETS). 2017. URL: http://www.petsymposium.org/2017/papers/hotpets/bgp-bogus-tls.pdf.

[BL10] M. Boldrin e D. K. Levine. *Against Intellectual Monopoly*. Cambridge University Press, 2010. ISBN: 978-0-521-12726-4.

[BN16] F. Brunton e H. Nissenbaum. *Obfuscation: A User's Guide for Privacy and Protest*. Mit Press. MIT Press, 2016. ISBN: 978-0-262-52986-0.

[Bra96] S Bradner. «The Internet standards process. Revision 3 (rfc 2026, bcp 9)». In: (1996). URL: http://datatracker.ietf.org/doc/rfc2026/.

[Bro13] Jon Brodkin. «Why YouTube buffers: The secret deals that make - and break - online video». In: (Luglio 2013). URL: http://arstechnica.com/information-technology/2013/07/why-youtube-buffers-the-secret-deals-that-make-and-break-online-video.

[But18] Giancarlo Butti. «Data retention policy». In: *Europrivacy* (mar. 2018). URL: http://europrivacy.info/it/2018/03/10/data-retention-policy.

[Cam00] Duncan Campbell. «Echelon: World under watch, an introduction». In: *ZDNet* (22 mag. 2000). URL: http://www.zdnet.com/echelon-world-under-watch-an-introduction-3002079845/.

[Can14] Cengiz Candar. «Il governo turco mette il bavaglio a Internet». In: *Internazionale (da Al Monitor)* 1038 (feb. 2014), p. 18.

[Cas96] Manuel Castells. «The information age: Economy, society and culture (3 volumes)». In: *Blackwell, Oxford* 1997 (1996), p. 1998.

[CB09] Stephen Coleman e Jay G Blumler. *The Internet and democratic citizenship: Theory, practice and policy*. Cambridge University Press, 2009.

[CH99] Duncan Campbell e Mark Honigsbaum. «Britain and US spy on world». In: *The Guardian* (22 mag. 1999). URL: http://www.theguardian.com/uk/1999/may/23/duncancampbell.markhonigsbaum.

[Chi14] F. Chiusi. *Critica della democrazia digitale: la politica 2.0 alla prova dei fatti*. Tempi moderni. Codice edizioni, 2014. ISBN: 978-88-7578-408-9.

[Com01] Commissione temporanea sul sistema d'intercettazione Echelon. *Relazione sull'esistenza di un sistema d'intercettazione globale per le comunicazioni private ed economiche (sistema d'intercettazione ECHELON) (2001/2098 (INI))*. Rapp. tecn. Commissione Europea, 2001. URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//IT.

[CS00] Andrew Clement e Leslie R Shade. «The access rainbow: Conceptualizing universal access to the information/communications infrastructure». In: *Community informatics: Enabling communities with information and communications technologies*. IGI Global, 2000, pp. 32–51.

[Das13] Jennifer C Daskal. «Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention». In: *Cornell L. Rev.* 99 (2013), p. 327.

[De 00] Fiorella De Cindio. «Community networks for reinventing citizenship and democracy». In: *Community informatics: Enabling communities with information and communications technologies*. IGI Global, 2000, pp. 213–231.

[Dep19] Camera dei Deputati. «Introduzione dell'insegnamento scolastico dell'educazione civica». In: (2019). URL: `http://documenti.camera.it/leg18/dossier/pdf/AF0682A.pdf`.

[DG11] A. Di Corinto e A. Giglioli. *I nemici della rete*. BUR Futuropassato. RIZZOLI LIBRI, 2011. ISBN: 9788858618165.

[DGH16] Alexa Domachowski, Joachim Griesbaum e Ben Heuwing. «Perception and Effectiveness of Search Advertising on Smartphones». In: *Proceedings of the 79th ASIS&T Annual Meeting: Creating Knowledge, Enhancing Lives Through Information & Technology*. ASIST '16. Copenhagen, Denmark: American Society for Information Science, 2016, 74:1–74:10. URL: `http://dl.acm.org/citation.cfm?id=3017447.3017521`.

[DST12] Fiorella De Cindio, Leonardo Sonnante e Andrea Trentini. «Cittadinanza Digitale: un arcobaleno di diritti e opportunità». In: *Mondo Digitale (in italian)* nr. 42 (2012). URL: `http://mondodigitale.aicanet.net/2012-2/`.

[DT14] Fiorella De Cindio e Andrea Trentini. «A Layered Architecture to Model Digital Citizenship Rights and Opportunities». In: *Conference for E-Democracy and Open Governement*. 2014, p. 403.

[Eha12] Brian Patrick Eha. «Verizon for blocking mobile apps». In: (Luglio 2012). URL: http://www.smithsonianmag.com/innovation/how-other-countries-deal-net-neutrality-180967558.

[Ein55] L. Einaudi. *Prediche inutili*. pt. 2. 1955.

[ES00] Carl Ellison e Bruce Schneier. «Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure». In: *Computer Security Journal* 16.1 (2000), pp. 1–8. URL: http://www.schneier.com/academic/paperfiles/paper-pki.pdf.

[EU18] Consiglio EU. *Raccomandazione del Consiglio relativa alle competenze chiave per l'apprendimento permanente*. IT. EU, 2018. URL: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32018H0604(01).

[Eud11a] Yves Eudes. «Battaglia annunciata». In: *Internazionale (da Le Monde)* 899 (mag. 2011), p. 99.

[Eud11b] Yves Eudes. «Internet in pericolo». In: *Internazionale (da Le Monde)* 899 (mag. 2011), p. 98.

[Eud16] Yves Eudes. «Alta velocità in fondo al mare». In: *Internazionale (da Le Monde)* 1137 (gen. 2016), pp. 59–61.

[Eur15] European Commission. *Digital Agenda Scoreboard 2013. Chapter 3*. report. EU, 2015. URL: http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/DAE%20SCOREBOARD%202013%20-%203-INTERNET%20USE%20AND%20SKILLS_0.pdf.

[Far13] Cyrus Farivar. «New leak shows feds can access user accounts for Google, Facebook and more». In: *Art Technica* (6 lug. 2013). URL: http://arstechnica.com/tech-policy/2013/06/new-leak-feds-can-access-

anything-in-your-google-facebook-and-more/.

[Fin17] Klint Finley. «The who's who of the net neutrality's "day of action"». In: (2017). URL: http://www.wired.com/story/the-whos-who-of-net-neutralitys-day-of-action/.

[Fis16] Lawrence M. Fisher. «A Decade of ACM Efforts Contribute to Computer Science for All». In: *Commun. ACM* 59.4 (mar. 2016), pp. 25–27. ISSN: 0001-0782. DOI: 10.1145/2892740. URL: http://doi.org/10.1145/2892740.

[For18] A. Forchielli. *Muovete il culo!: Lettera ai giovani perché facciano la rivoluzione in un Paese di vecchi*. I Saggi B&C. Baldini&Castoldi, 2018. ISBN: 978-88-938855-3-9.

[Fri17] Nick Frish. «Viaggio su Internet senza neutralità della rete». In: *Internazionale (da The New York Times)* 1236 (dic. 2017), p. 123.

[Fug18] A. Fuggetta. *Cittadini ai tempi di Internet: Per una cittadinanza consapevole nell'era digitale*. OrientaMenti / Conoscere per decidere - diretta da C. Bottani, C. Maffei. Franco Angeli Edizioni, 2018. ISBN: 978-88-917844-5-2.

[Gar14] Juliette Garside. «Vodafone reveals existence of secret wires that allow state surveillance». In: *The Guardian* (6 giu. 2014). URL: http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance.

[Giu17] Gabriella Giudici. «La fine della neutralità di Internet». In: (2017). URL: http://gabriellagiudici.it/la-fine-della-neutralita-di-internet.

[GK17] Hannes Grassegger e Michael Krogerus. «La politica ai tempi di Facebook». In: *Internazionale (da Das Magazin)* 1186 (gen. 2017), pp. 40–47.

[GM13] Glenn Greenwald e Ewen MacAskill. «NSA Prism program taps in to user data of Apple, Google and others». In: *The Guardian* (6 giu. 2013). URL: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[Gol80] Herman H. Goldstine. *The computer from Pascal to Von Neumann*. Princeton University Press, 1980.

[Goo13] Dan Goodin. «Repeated attacks hijack huge chunks of Internet traffic, researchers warn». In: *Ars Technica* (2013). URL: http://arstechnica.com/information-technology/2013/11/repeated-attacks-hijack-huge-chunks-of-internet-traffic-researchers-warn.

[GP13] Barton Gellman e Laura Poitras. «Documents: U.S. intelligence mining data from nine U.S. Internet companies in broad secret program». In: *Washington Post* (6 giu. 2013). URL: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

[GR18] Sarah Gordon e Aliya Ram. «Un nuovo inizio per la privacy». In: *Internazionale (da Financial Times)* 1257 (mag. 2018), pp. 112–113.

[Gre14] Glenn Greenwald. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Henry Holt e Company, 2014. ISBN: 978-1-62779-074-1.

[Gri15] Angus Grigg. «La grande muraglia digitale». In: *Internazionale (da The Australian Financial Review)* 1116 (ago. 2015), pp. 52–56.

[Gui19] M. Gui. *Il digitale a scuola: rivoluzione o abbaglio?* Universale paperbacks Il Mulino. Il Mulino, 2019. ISBN: 978-88-15-28320-7.

[HMU06] John E. Hopcroft, Rajeev Motwani e Jeffrey D. Ullman. «Automata theory, languages, and computation». In: *International Edition* 24 (2006).

[Hor72] David Horowitz. «U.S. Electronic Espionage: A Memoir». In: *Rampants* 11.2 (ago. 1972), pp. 35–50. URL: http://cryptome.org/jya/nsa-elint.htm.

[Ita19] Governo Italiano. «IV Piano d'azione nazionale per l'open government». In: (2019). URL: http://open.gov.it/wp-content/uploads/2019/09/Quarto_Piano_Azione_Nazionale_OGP_Finale_06.2019.pdf.

[Kai19] B. Kaiser. *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again*. Harper, 2019. ISBN: 9780062965806. URL: http://books.google.it/books?id=zguYDwAAQBAJ.

[Kan14] Cecilia Kang. «Concorrenza sleale». In: *Internazionale (da The Washington Post)* 1049 (mag. 2014), p. 99.

[Kir14] Keith Kirkpatrick. «Technology confounds the courts». In: *Communications of the ACM* 57.5 (mag. 2014), pp. 27–29. DOI: 10.1145/2591231. URL: http://doi.org/10.1145/2591231.

[Kir53] P. L. Kirk. *Crime investigation: physical evidence and the police laboratory*. Interscience Publishers, 1953.

[Kul14] Alexandra Kulikova. «Nella rete di Putin». In: *Internazionale (da Open Democracy)* 1058 (2014), pp. 46–49.

[Laf11] Sharon Lafraniere. «La guerra di Pechino contro Internet e TV». In: *Internazionale (da The New York Times)* 922 (nov. 2011), p. 32.

[Lan17] John Lanchester. «La merce sei tu». In: *Internazionale (da London review of Books)* 1222 (set. 2017), pp. 46–57.

[Lee10] Annabelle Lee. *Guidelines for smart grid cyber security*. Rapp. tecn. pagina 210 schema riportato in libro. 2010.

[Lee17] Kalev Leetaru. «Why 2017 Was The Year Of The Filter Bubble?» In: *Forbes* (2017). URL: `http://www.forbes.com/sites/kalevleetaru/2017/12/18/why-was-2017-the-year-of-the-filter-bubble`.

[Les16] L. Lessig. *Free Culture*. Lulu.com, 2016. ISBN: 978-1-365-29461-7. URL: `http://www.free-culture.cc`.

[Lev01] S. Levy. *Hackers: Heroes of the computer revolution*. Vol. 4. New York, NY, USA: Penguin Books New York, 2001. ISBN: 0-385-31210-5.

[Lev14] P. Levi. *Se questo è un uomo*. Super ET. Einaudi, 2014. ISBN: 978-88-06-21935-2.

[Lic18] Patrizia Licata. «Net neutrality USA, le big tech al contrattacco». In: *Corcom* (2018).

[Loc25] E. Locard. *Manuale di polizia tecnica (inchiesta criminale): Traduzione italiana sulla prima edizione francese con moltissime note ed aggiunte originali dello avv. dott. prof. F. Geraci, ad uso dei laboratori di polizia tecnica, degli ufficiali di polizia giudiziaria, dei medici legisti, dei magistrati e degli avvocati ...* V. Carciola, 1925.

[Mac13] Ewen MacAskill. «NSA paid millions to cover Prism compliance costs for tech companies». In: *The Guardian* (22 ago. 2013). URL: http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid.

[Mag18] Alberto Magnani. «Privacy, che cos'è il Gdpr e perché ci riguarda». In: (Maggio 2018). URL: http://www.ilsole24ore.com/art/mondo/2018-05-02/privacy-che-cos-e-gdpr-e-perche-ci-riguarda-125716.shtml.

[Man11] Farhad Manjoo. «La fine del gusto». In: *Internazionale (da Slate)* 918 (ott. 2011), p. 99.

[Man17] Farhad Manjoo. «Senza neutralità possiamo dire addio a Internet». In: *Internazionale (da The New York Times)* 1234 (dic. 2017), pp. 128–129.

[Man18] Farhad Manjoo. «La corsa sfrenata a mettere Internet in tutte le cose». In: *Internazionale (da The New York Times)* 1279 (ott. 2018), pp. 106–107.

[Mar18] Roberto Maraglino. «GDPR e data retention (conservazione dati): policy e linee guida per farla bene». In: *Cybersecurity360* (2018).

[Mas43] Abraham Harold Maslow. «A theory of human motivation.» In: *Psychological review* 50.4 (1943), p. 370.

[Mau14] Hermann Maurer. «Does the internet make us stupid?» In: *Communications of the ACM* 58.1 (dic. 2014), pp. 48–51. DOI: 10.1145/2629544. URL: http://doi.org/10.1145/2629544.

[McG02] Richard McGregor. «Il governo cinese contro google». In: *Internazionale (da Financial Times)* 455 (set. 2002), p. 58.

[ML15] Chiara Marchetti e Matteo Longeri. *Behind DataGate*. Rapp. tecn. Dipartimento di Informatica, 2015. URL: http://tecnocivismo.di.unimi.it/infodiscs/getfile/334.

[MP09] Jude McCulloch e Sharon Pickering. «Pre-Crime and Counter-Terrorism: Imagining Future Crime in the 'War on Terror'». In: *The British Journal of Criminology* 49.5 (2009), pp. 628–645.

[MSW11] K.D. Mitnick, W.L. Simon e S. Wozniak. *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2011. ISBN: 978-07-6453-839-1.

[Nie00] J. Nielsen. *Designing Web Usability*. Designing Web Usability no. 667. New Riders, 2000. ISBN: 978-1-56205-810-4.

[Nor13] D. Norman. *The Design of Everyday Things: Revised and Expanded Edition*. Basic Books, 2013. ISBN: 978-0-465-07299-6.

[NSA11] NSA. «Blast from the past: yrs in the beginning». In: *The Notrhwest Passage* 2.1 (gen. 2011), pp. 8–10. URL: http://www.documentcloud.org/documents/2189960-nwp-nsa.html.

[NSA12] NSA. «Blast from the past: yrs in the beginning». In: *Yrs gears up to celebrate 40 years* 8.7 (lug. 2012), p. 1. URL: http://www.documentcloud.org/documents/2189961-nwp2-nsa.html.

[NV18] T. Nichols e C. Veltri. *La conoscenza e i suoi nemici. L'era dell'incompetenza e i rischi per la democrazia*. Luiss University Press. Luiss University Press, 2018. ISBN: 978-88-6105-311-3.

[OC13] Jonathan Obar e Andrew Clement. «Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty». In: *SSRN Electronic Journal* (gen. 2013). DOI: 10.2139/ssrn.2311792. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311792.

[ONe16] C. O'Neil. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown/Archetype, 2016. ISBN: 978-0-553-41882-8.

[Orw45] G. Orwell. *Animal Farm*. 1945.

[PCA18] C. Piana, R. di Cosmo e S. Aliprandi. *Open source, software libero e altre libertà: Un'introduzione alle libertà digitali*. Copyleft Italia. Ledizioni, 2018. ISBN: 978-88-6705-766-5.

[Pen14] Laurie Penny. «La censura su Internet con la scusa dei bambini». In: *Internazionale* 1033 (gen. 2014), p. 31.

[Pre15] Presidenza del Consiglio dei Ministri. «Strategia per la Crescita Digitale 2014–2020». In: (2015). URL: http://www.agid.gov.it/sites/default/files/repository_files/documentazione/strategia_%20crescita_digitale_ver_def_21062016.pdf.

[Puu+18] Aare Puussaar et al. «Making open data work for civic advocacy». In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (2018), p. 143.

[Roc19] C. Rocca. *Chiudete Internet: Una modesta proposta*. Marsilio, 2019. ISBN: 978-88-297-0167-4.

[Rod15] Stefano Rodotà. *Il diritto di avere diritti*. Gius. Laterza & Figli Spa, 2015.

[Rus10] Douglas Rushkoff. *Program Or be Programmed: Ten Commands for a Digital Age*. OR Books, 2010. ISBN: 9781935928157.

[Rus13] Dominic Rushe. «Facebook and Google insist they did not know of Prism surveillance program». In: *The Guardian* (8 giu. 2013). URL: http://www.theguardian.com/world/2013/jun/07/google-facebook-prism-surveillance-program.

[Saf+17] Bardia Safaei et al. «Reliability side-effects in Internet of Things application layer protocols». In: *2017 2nd International Conference on System Reliability and Safety (ICSRS)*. IEEE, dic. 2017. DOI: 10.1109/icsrs.2017.8272822. URL: http://doi.org/10.1109/icsrs.2017.8272822.

[Sch16] Jason Schultz. «The internet of things we don't own?» In: *Communications of the ACM* 59.5 (apr. 2016), pp. 36–38. DOI: 10.1145/2903749. URL: http://doi.org/10.1145/2903749.

[Sen+15] Pratim Sengupta et al. «Programming in K-12 science classrooms». In: *Communications of the ACM* 58.11 (ott. 2015), pp. 33–35. DOI: 10.1145/2822517. URL: http://doi.org/10.1145/2822517.

[Sha73] B. Shaw. *Altri giorni altri occhi.* (trad. D. Frattina). A. Mondadori, 1973.

[She14] Esther Shein. «Should everybody learn to code?» In: *Communications of the ACM* 57.2 (feb. 2014), pp. 16–18. DOI: 10.1145/2557447. URL: http://doi.org/10.1145/2557447.

[sit16] Turkey Blocks (site). *Tor blocked in Turkey as government cracks down on VPN use*. EN. 18 Dic. 2016. URL: https://turkeyblocks.org/2016/12/18/tor-blocked-in-turkey-vpn-ban/.

[SL16] Olivia Solon e Sam Levin. «How Google's search algorithm spreads false information with a right-wing bias». In: *The Guardian* (16 dic. 2016).

[Sno19] E. Snowden. *Permanent Record*. Henry Holt e Company, 2019. ISBN: 9781250237248.

[Som14] Ravi Somaiya. «I giornali al tempo di Facebook». In: *Internazionale (da The New York Times)* 1076 (nov. 2014), pp. 106–107.

[SS13] Sheryl Gay Stolberg e Michael D Shear. «Inside the race to rescue a health care site, and Obama». In: *New York Times* (2013).

[Ste90] Guy Steele. *Common LISP: the language*. Elsevier, 1990.

[Sun01] Cass Sunstein. «Republic. com Princeton». In: *Telhami, Shibley: 2010 Arab Public Opinion Poll (conducted by the University of* (2001).

[SW19] Helene Strandell e Pascal Wolff. *Ageing Europe*. 2019. ISBN: 978-92-76-09815-7. DOI: 10.2785/811048. URL: http://ec.europa.eu/eurostat/web/products-statistical-books/-/KS-02-19-681.

[Tao16] Ian Goldberg Tao Wang. «On Realistically Attacking Tor with Website Fingerprinting». In: *Proceedings on Privacy Enhancing Technologies*. Vol. 4. 2016, pp. 21–36. URL: http://www.freehaven.net/anonbib/cache/websitefingerprinting-pets2016.pdf.

[TB15] A. S. Tanenbaum e H. Bos. *Modern Operating Systems: Global Edition*. Pearson Education Limited, 2015. ISBN: 978-1-292-06195-5.

[TD13] Andrea Trentini e Fiorella De Cindio. «L'arcobaleno dei diritti della cittadinanza digitale alla prova». In: *CONGRESSO NAZIONALE AICA 2013* ISBN 9788898091164 (2013).

[Toz+15] Tozza et al. *Studenti, computer e apprendimento: dati e riflessioni*. Rapp. tecn. Dic. 2015. DOI: 10.3386/w22989. URL: http://doi.org/10.3386/w22989.

[TS18] A. Trentini e P. Sciarelli. «La smart-cittadinanza attraverso la compliance dei siti web della Pubblica Amministrazione: il caso di studio dei Comuni italiani». In: *Città sostenibili*. Broni: Altravista, 2018.

[TW12] A. S. Tanenbaum e D. J. Wetherall. *Computer Networks*. Pearson Education, 2012. ISBN: 978-0-13-307262-4.

[Van17] Graham Vanbergen. «Pre-Crime Surveillance Technology, Social Blacklisting». In: *Global Research* (2017). URL: `http://www.globalresearch.ca/pre-crime-surveillance-technology-social-blacklisting/5596465`.

[Ver19] Jules Verne. *Dalla Terra alla Luna*. De Agostini, 2019. ISBN: 978-88-511-7540-5.

[Wei11] Sharon Weinberger. «Terrorist 'pre-crime' detector field tested in United States». In: *Nature* (2011). URL: `http://www.nature.com/news/2011/110527/full/news.2011.323.html`.

[Win96] T. Winograd. *Bringing design to software*. ACM Press Books. ACM Press, 1996. ISBN: 978-0-201-85491-6.

[Wri08] Scott Wright. «Digital Citizenship: The Internet, Society, and Participation, by Karen Mossberger, Caroline J. Tolbert, and Ramona S. McNeal». In: *Journal of Information Technology & Politics* 5.2 (2008), pp. 262–264. DOI: `10.1080/19331680802290972`. URL: `http://doi.org/10.1080/19331680802290972`.

[WTM13] Maria A Wimmer, Efthimios Tambouris e Ann Macintosh. «Electronic Participation». In: *5th IFIP WG 8.5 International Conference, ePart 2013*. Springer, 2013.

[Wu03] Tim Wu. «Network neutrality, broadband discrimination». In: *J. on Telecomm. & High Tech. L.* 2 (2003), p. 141.

[Yet14] Murat Yetkin. «La battaglia di Erdogan contro Twitter». In: *Internazionale (da Hürriyet Daily News)* 1044 (mar. 2014), p. 20.

[Zet08] Kim Zetter. «Revealed: The Internet's Biggest Security Hole». In: *Wired* (26 ago. 2008). URL: http://www.wired.com/2008/08/revealed-the-in/.

[Zub19a] S. Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books, 2019. ISBN: 9781782832744.

[Zub19b] Shoshana Zuboff. «Il capitalismo della sorveglianza». In: *Internazionale (da Financial Times)* 1306 (mag. 2019), pp. 40–45.

[Zwa14] Hans de Zwart. «How your innocent smartphone passes on almost your entire life to the secret service». In: *Bits Of Freedom* (30 lug. 2014). URL: http://www.bitsoffreedom.nl/2014/07/30/how-your-innocent-smartphone-passes-on-almost-your-entire-life-to-the-secret-service/.

Nella stessa collana

Titolo: Open Source, Software libero e altre libertà
Sottotitolo: Un'introduzione alle libertà digitali
Autore: Carlo Piana
ISBN: 9788867057665
Formato: cartaceo, 157 p.
Prezzo: 16 €

Titolo: DIDATTICADUEPUNTOZERO
Sottotitolo: Scenari di didattica digitale condivisa
A cura di: Alberto Panzarasa
ISBN: 9788867055456
Formato: cartaceo, 140 p.
Prezzo: 14,00 €

Titolo: La battaglia per l'open
Sottotitolo: Come l'open ha vinto, ma non sembra una vittoria
Autore: Martin Weller
ISBN: 9788855263436
Formato: cartaceo, 140 p.
Prezzo: 16 €
In preparazione

Per questi e altri titoli visita www.ledizioni.it

Nella stessa collana

Titolo: Fare Open Access
Sottotitolo: La libera diffusione del sapere scientifico nell'era digitale
Autore: Simone Aliprandi
ISBN: 9788867056019
Formato: cartaceo, 194 p.
Prezzo: 14 €

Titolo: Creative Commons: manuale operativo
Sottotitolo: Una guida pratica e un'introduzione teorica al mondo CC
Autore: Simone Aliprandi
ISBN: 9788867051342
Formato: ePub
Prezzo: 1,99 €

Titolo: Il fenomeno open data
Sottotitolo: Indicazioni e norme per un mondo di dati aperti
Autore: Simone Aliprandi
ISBN: 9788867051687
Formato: cartaceo, 112 p.
Prezzo: 12 €

Per questi e altri titoli visita www.ledizioni.it

CITTADINANZA DIGITALE E TECNOCIVISMO

IN UN MONDO DIGITALE LA CITTADINANZA INIZIA DAI BIT

VOLUME PRIMO

Digitalizzazione pervasiva e iperconnessione ci rendono automaticamente cittadini più informati e partecipi? La Rete deve essere neutrale o "indirizzata" *per il nostro bene*? Il diritto alla riservatezza va asservito all'*interesse superiore*? Le infrastrutture digitali sono *diritti* o *merci*? La conoscenza deve essere accessibile a tutti? E la tecnologia: trasparente o oscura? La Cittadinanza Digitale è possibile? Risponderemo a queste ed altre domande rivolgendoci a chi inizia a rendersi conto che la piena consapevolezza sugli aspetti tecnologici sottostanti i processi sociali, politici ed economici è importante. Ci aggrapperemo a questa consapevolezza costruendo un quadro, pur a tratti tecnico, delle tecnologie connesse alla Cittadinanza Digitale.
I nostri lettori ideali sono in particolare gli studenti, gli attivisti politici, gli accademici, gli amministratori pubblici, i *policy makers*, i professionisti delle tecnologie (ad esempio gli sviluppatori) e i politici, categorie che tradizionalmente ricoprono ruoli di "influenza" sociale, politica e tecnologica e che quindi potrebbero e dovrebbero indirizzare la società verso il *bene comune*.

Andrea Trentini

PhD in Informatica, è ricercatore presso il Dipartimento di Informatica dell'Università degli Studi di Milano dove insegna "Cittadinanza Digitale e Tecnocivismo" e "Sistemi Embedded". Propugnatore del Software Libero e della condivisione della conoscenza. Curioso sulla vita, l'universo e tutto quanto.

Giovanni Biscuolo

Hacker (a sua insaputa) dall'infanzia, oggi è direttore tecnico di un'azienda informatica di Milano dove si occupa di progettazione, sviluppo e supporto di infrastrutture IT *on premises* e in *hosting*. Ha scoperto il Software Libero *non per caso* e da allora non ha mai smesso di chiedersi come riesca a *funzionare*: nel frattempo qualcosa è riuscito a capire.

Andrea Rossi

Da sempre consapevole dell'impatto sociale del digitale è *founder&CEO* di un'impresa informatica vincolata al Software Libero e impegnata per la ri-decentralizzazione di Internet.

www.ledizioni.it
www.ledipublishing.com

PDF Open Access

9 788855 263481 >