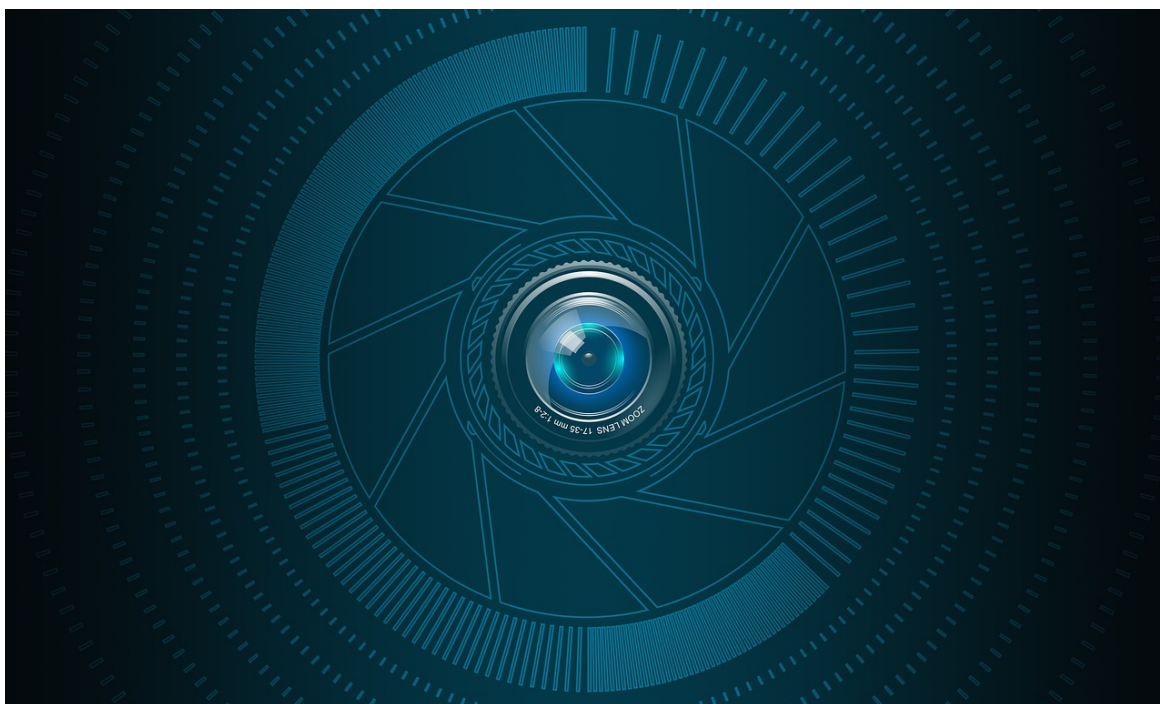


# Diritti analogici analoghi

di Rick Falkvinge



**20 modi in cui abbiamo perso il diritto alla privacy  
nell'era del digitale**

## Indice generale

Come abbiamo perso il diritto alla privacy nell'era del digitale.....	1
1. I nostri figli dovrebbero avere gli stessi diritti dei nostri genitori.....	3
2. La lettera analogica, anonima e The Pirate Bay.....	5
3. Scrivere messaggi pubblici anonimi.....	7
4. I nostri figli hanno perso la privacy della posizione.....	9
5. Che fine ha fatto la libertà di assemblea?.....	11
6. Tutto ciò che fai, dici o pensi oggi sarà usato contro di te in futuro.....	13
7. Le librerie analogiche erano luoghi di ricerca privata.....	15
8. L'utilizzo di servizi di terze parti non dovrebbe diminuire l'aspettativa di privacy.....	17
9. Quando il governo sa cosa leggi, in quale ordine, e per quanto tempo.....	19
10. Il giornalismo analogico era protetto, quello digitale no.....	21
11. I nostri genitori usavano denaro anonimo.....	23
12. I nostri genitori compravano senza essere tracciati. I loro movimenti nei negozi non erano registrati.....	25
13. I nostri figli digitali sono tracciati non solo in tutto ciò che comprano, ma anche in ciò che <i>non</i> comprano.....	27
14. Le preferenze dei nostri genitori analogici in materia di appuntamenti non venivano monitorate, registrate e catalogate.....	29
15. Le conversazioni digitali dei nostri bambini sono silenziate a seconda dell'argomento.....	31
16. La sorveglianza retroattiva di tutti i nostri figli.....	33
17. C'era una volta l'inviolabilità dei diari.....	35
18. I nostri genitori analogici avevano conversazioni private, sia in pubblico che a casa.....	37
19. I teleschermi in soggiorno.....	39
20. Il tuo boss analogico non poteva leggere la tua posta. Mai.....	41
21. Conclusione, la privacy è stata quasi completamente eliminata dall'ambiente digitale.....	43

# 1. I nostri figli dovrebbero avere gli stessi diritti dei nostri genitori

In una serie di 21 post su questo blog, esamineremo come i diritti alla privacy - libertà civili essenziali - sono stati completamente persi nel passaggio al digitale. L'erosione è a dir poco catastrofica.

Daremo uno sguardo a una grande quantità di aree diverse, dove la privacy è semplicemente svanita nel passaggio al digitale, e dove invece è finita. Per ciascuna questione, vedremo a che punto sono le diverse giurisdizioni e quali sono le tendenze. L'aspetto chiave è chiaro: non è affatto irragionevole che i nostri figli abbiano almeno la stessa serie di libertà civili dei nostri genitori, ma oggi non la hanno. Non la hanno affatto.

Per cominciare, esamineremo le libertà che garantiva la corrispondenza analogica, e quante libertà ad essa connesse - come il diritto di inviare una lettera anonima - sono state completamente perse. Lo stesso vale per i manifesti pubblici anonimi sui cartelloni pubblicitari; chi difende oggi il tuo diritto di fare una dichiarazione politica anonima?

Vedremo come non avete più il diritto di camminare in privato, senza che qualcuno vi segua. Un tempo gli aeroporti e le stazioni ferroviarie erano luoghi sicuri e anonimi per i nostri genitori; oggi, il tuo telefono è un faro di segnalazione in tempo reale non appena ti avvicini a loro.

Inoltre, vedremo come una volta le autorità avrebbero dovuto cogliervi in flagrante mentre facevate qualcosa che non piaceva loro, mentre ora sono in grado di riavvolgere il nastro di 20 anni o giù di lì per trovare qualcosa che non hanno trovato "in diretta"; e forse è qualcosa di cui neanche gli importava tanto, allora. Forse è qualcosa a cui a quei tempi non prestavi nemmeno attenzione, e di cui tanto meno puoi ricordarti 20 anni dopo.

I nostri genitori andavano in biblioteca e cercavano informazioni. I bibliotecari si spingevano fino all'estremo, inventando persino il [canarino del mandato](#), per assicurarsi che le persone potessero cercare qualsiasi informazione e leggere qualsiasi libro volessero senza che le autorità ne fossero al corrente. Oggi Google si spinge anch'esso fino all'estremo, ma per prendere nota di tutto ciò che si cerca, fino a includere ciò che *si stava per cercare ma non si è cercato* - e, naturalmente, tutto questo è a disposizione delle autorità e dei governi, che devono solo dire a Google di seguire la legge che hanno appena scritto.

**Non è affatto irragionevole pretendere che i nostri figli abbiano nel loro ambiente digitale almeno le stesse libertà civili - diritti alla privacy- che i nostri genitori avevano nel loro ambiente analogico. Tuttavia, i diritti alla privacy sono stati quasi aboliti nel passaggio al digitale.**

Parlando di lettura, i nostri genitori potevano comprare un giornale all'angolo della strada con qualche spicciolo. Potevano leggere un giornale senza che nessuno sapesse che l'avevano comprato o letto. Al contrario di quanto accade per i nostri figli, dove viene accuratamente registrato quali

giornali leggono, quando, quali articoli, in quale ordine e per quanto tempo - e forse peggio ancora, quali azioni hanno intrapreso subito dopo, e se queste sembrano essere state causate dalla lettura dell'ultimo articolo che hanno letto.

Ah sì, i contanti in edicola. I contanti ovunque, infatti. Diversi paesi stanno cercando di abolire il contante, rendendo tutte le transazioni rintracciabili. Una carta è più conveniente? Forse. Ma non è più sicuro. Ogni acquisto viene registrato. Peggio ancora, ogni quasi-acquisto dei nostri figli viene registrato, cosa inconcepibile nel mondo dei nostri genitori. Ancora peggio, ogni acquisto è anche autorizzato, e può essere negato da terzi.

I nostri genitori non avevano né videocamere, né TV che li guardavano. Ma se l'avessero avuti, sono ragionevolmente sicuro che sarebbero stati inorriditi dal fatto che i nostri figli siano spiati dai governi, che li guardano direttamente nel loro salotto, o attraverso videocamere private, incluse talvolta anche *molto* private.

Quando i nostri genitori avevano una conversazione privata al telefono, non c'era mai la voce di uno sconosciuto che spuntava nella telefonata e diceva "avete menzionato un argomento proibito; vi prego di astenervi dal discutere argomenti proibiti in futuro". Oggi invece questo è ciò che avviene nella messaggistica privata su Facebook, nel mondo dei nostri figli. Questo, naturalmente, si collega al concetto di avere conversazioni private nella nostra casa, e a come i nostri figli non capiranno nemmeno *il concetto* di avere una conversazione privata a casa (ma capiscono che possono chiedere biscotti e una casa delle bambole al piccolo box di ascolto [Alexa, Siri, *n.d.t.*]).

Vedremo anche come l'industria del copyright sfrutti praticamente tutto questo per tentare di cambiare il mondo in modo drammatico, in quello che può solo essere descritto come moralmente fallito.

Questo e molto altro ancora nella prossima serie di 21 articoli, di cui questo è il primo.

## 2. La lettera analogica, anonima e The Pirate Bay

I nostri genitori davano per scontate nel loro mondo analogico alcune libertà che non si tramandano ai nostri figli nel passaggio al digitale - come il semplice diritto di inviare una lettera anonima.

A volte, quando parlo, chiedo al pubblico quanti siti come The Pirate Bay vanno bene, anche se ciò significa che gli artisti stanno perdendo soldi per le loro operazioni. (Si noti che questa affermazione è controversa: pongo la domanda supponendo che se ne dia per scontata la veridicità). Alcune persone alzano la mano, la proporzione varia a seconda del pubblico e del luogo.

L'industria del copyright afferma che le leggi offline non si applicano su Internet quando vogliono citare in giudizio e perseguire persone che condividono conoscenza e cultura. Hanno ragione, ma non nel modo in cui pensano. Hanno ragione che la legge sul copyright si applica anche online. Ma le leggi sulla privacy non lo fanno, e invece dovrebbero.

Nel mondo offline, ad una lettera analogica è stato dato un certo livello di protezione. Questa non intendeva coprire solo la lettera fisica in quanto tale, ma *la corrispondenza in generale*; semplicemente, la lettera era l'unica forma di corrispondenza quando queste libertà sono state redatte.

In primo luogo, la lettera era *anonima*. Era vostra prerogativa scegliere di identificarvi come mittente della lettera all'esterno della busta, all'interno (quindi nemmeno il servizio postale sapeva chi l'ha inviata, solo il destinatario), o di non identificarvi affatto.

Inoltre, la lettera *non era rintracciabile durante il trasporto*. Gli unici governi che rintracciavano la corrispondenza popolare erano quelli a cui guardavamo con enorme disprezzo.

In terzo luogo, la lettera era *segreta*. La busta non avrebbe mai dovuto essere aperta durante il tragitto.

Quarto, il postino non era mai responsabile del contenuto, se non altro perché non gli era permesso esaminare il contenuto in primo luogo. Ma anche se avesse potuto farlo, come con una cartolina senza busta, non sarebbe mai stato responsabile, in quanto semplice esecutore di una funzione pubblica - questo principio, l'immunità del corriere o del messaggero, risale all'Impero Romano.

Questi principi, le libertà di corrispondenza, dovrebbero applicarsi alla corrispondenza offline (la lettera) così come alla corrispondenza online. Ma non è così. Non hai il diritto di inviare qualcosa che ti piace a chiunque ti piaccia online, perché potrebbe essere una violazione del copyright - anche se i nostri genitori avevano esattamente questo diritto nel loro mondo offline.

Quindi l'industria del copyright ha ragione - inviare un disegno copiato in una lettera è una violazione del copyright, e inviare un brano musicale copiato in rete è lo stesso tipo di violazione del copyright. Ma offline, ci sono pesi e contrappesi a queste leggi - anche se si tratta di una violazione del copyright, a nessuno è permesso aprire la lettera in transito solo per vedere se viola la legge, perché la segretezza della corrispondenza privata è considerata più importante che scoprire

violazioni del copyright. Questo è il punto. Questa serie di pesi e contrappesi non è stata trasferita nell'ambiente digitale.

L'unico momento in cui una lettera viene aperta ed esaminata è quando qualcuno è stato *precedentemente e individualmente* sospettato di un reato grave. Le parole "precedentemente" e "individualmente" sono importanti in questo caso: aprire le lettere solo per vedere se contengono un reato non grave in corso, come la violazione del diritto d'autore, semplicemente non è permesso.

Non c'è motivo per cui le libertà offline dei nostri genitori non possono essere trasferite nelle stesse libertà online per i nostri figli, a prescindere dal fatto che ciò significhi che qualcuno non sa più come gestire un'azienda.

Dopo aver evidenziato questi punti, ripeto la domanda se il pubblico sarebbe d'accordo con siti come The Pirate Bay, anche se ciò significa che un artista sta perdendo reddito. E dopo aver fatto questi punti, fondamentalmente tutti alzano la mano per dire che a loro andrebbe bene, che i nostri figli abbiano la stessa libertà dei nostri genitori, e che i *check and balances* del mondo offline debbano valere anche online.

Nella prossima puntata della serie, ci occuperemo di un tema correlato - gli annunci pubblici anonimi e l'importante ruolo che i comizi di piazza nelle città hanno svolto nel plasmare la libertà.

### 3. Scrivere messaggi pubblici anonimi

**Le libertà dei nostri genitori non vengono ereditate dai nostri figli - si perdono all'ingrosso nel passaggio al digitale. Oggi esamineremo l'importanza di inviare messaggi pubblici anonimi.**

Quando ero adolescente, prima di Internet (sì, davvero), c'era una cosa chiamata [BBSES - Bulletin Board Systems](#). Erano gli equivalenti digitali di un Bulletin Board analogico, che a sua volta era un bellissimo foglio di legno destinato all'invio di messaggi al pubblico. In un certo senso, erano un equivalente anonimo dei Forum di oggi, ma ci si collegava dal proprio computer di casa direttamente alla BBS tramite una linea telefonica, senza prima connettersi a Internet.

I Bulletin Boards analogici esistono ancora, naturalmente, ma sono utilizzati soprattutto per la promozione di concerti e per occasionali annunci politici o religiosi marginali.

All'inizio degli anni '90, strane leggi sono entrate in vigore in tutto il mondo come risultato della pressione delle lobby del copyright: i proprietari di sistemi di bacheca potevano essere ritenuti responsabili di ciò che altre persone pubblicavano sopra di esse. L'unico modo per evitare la punibilità era far sparire le pubblicazioni entro sette giorni. Tale responsabilità non aveva alcun equivalente analogico; era un'idea assolutamente ridicola che il proprietario di un pezzo di terra dovesse essere ritenuto responsabile per un manifesto affisso su un albero di quella terra, o anche che il proprietario di un pezzo di cartone pubblico potesse essere citato in giudizio per i manifesti che altre persone avevano incollato su quella tavola.

Ribadisco: è estremamente strano, dal punto di vista legale, che un fornitore di hosting elettronico sia in qualsiasi modo, forma o maniera responsabile per i contenuti ospitati sulla sua piattaforma. Non ha alcun equivalente analogico.

Certo, la gente poteva affiggere manifesti analogici illegali su una bacheca analogica. Era un atto illegale. Ma quando ciò accadeva, era un problema delle forze dell'ordine, e mai del proprietario della bacheca. Il pensiero è ridicolo e non ha posto neanche nel panorama digitale.

L'equivalente digitale corretto non è quello di richiedere la registrazione per consegnare l'upload di IP alle forze dell'ordine. Un proprietario di una bacheca analogica non ha l'obbligo di identificare in qualche modo le persone che utilizzano la bacheca, o addirittura monitorare se viene utilizzata.

Il diritto alla privacy equivalente analogico per un fornitore di hosting di posta elettronica, consiste nello stabilire che chi esegue un upload deve essere ritenuto responsabile di tutto ciò che carica, senza alcuna responsabilità per il fornitore di hosting in nessuna circostanza, senza neanche alcun obbligo di registrare i dati in upload per aiutare le forze dell'ordine a trovare chi carica quei dati. Tale monitoraggio non era richiesto nel mondo analogico dei nostri genitori: non c'era una responsabilità analogica per qualsiasi cosa pubblicata, e non c'è ragione che le cose vadano diversamente nel mondo digitale dei nostri figli solo perché qualcuno non sa come gestire un'attività in altro modo.

Come nota a margine, gli Stati Uniti non esisterebbero se le odierne leggi sulla responsabilità per l'hosting fossero state in vigore al momento della sua formazione. All'epoca circolavano molti scritti che discutevano di rompere con la Corona britannica e formare una Repubblica Indipendente; sotto il profilo penale, questo incitava e favoriva l'alto tradimento. Questi testi erano comunemente inchiodati agli alberi e nei luoghi pubblici, affinché il pubblico leggesse e decidesse da solo. Immaginate per un momento se i proprietari dei terreni in cui si trovavano tali alberi fossero stati accusati di alto tradimento per "ospitare contenuti" - il pensiero è ridicolo nell'analogico, come lo è davvero anche nel digitale. Dobbiamo solo mettere da parte l'illusione che le attuali leggi sull'hosting digitale abbiano senso. Queste leggi sono davvero ridicole nel mondo digitale dei nostri figli, come lo sarebbero state nel mondo analogico dei nostri genitori.



## 4. I nostri figli hanno perso la privacy della posizione

**Nel mondo analogico dei nostri genitori, come cittadino comune e non sotto sorveglianza perché sospettato di un crimine, si dava per scontato il poter camminare in una città senza che le autorità ti seguissero passo per passo. I nostri figli non hanno più questo diritto nel loro mondo digitale.**

Nemmeno le distopie degli anni '50 - 1984, Brave New World, Colossus etc- sono riuscite a immaginare gli orrori di questo aspetto: il fatto che ogni cittadino ora porta con sé un dispositivo di tracciamento governativo. E non solo lo stanno portando con sé, ma l'hanno persino comprato loro stessi. Nemmeno Brave New World avrebbe potuto immaginare questo orrore.

E' iniziato in modo innocente, naturalmente. Succede sempre così. Con i nuovi "telefoni portatili" - che, a questo punto, significava qualcosa come "non incatenato al pavimento" - le autorità hanno scoperto che le persone avrebbero comunque chiamato il numero dei servizi di emergenza (112, 911, eccetera) dai loro telefoni cellulari, ma non sempre sarebbero state in grado di comunicare la loro posizione, cosa che la rete telefonica era ormai in grado di fare. Così le autorità hanno ordinato che le reti telefoniche fossero tecnicamente in grado di fornire sempre la posizione dell'abbonato, nel caso in cui dovessero chiamare i Servizi di Emergenza. Negli Stati Uniti, questo era conosciuto come il regolamento E911 ("Enhanced 9-1-1").

Era il 2005. Le cose sono andate degenerando rapidamente. Immaginate che, solo 12 anni fa, avevamo ancora il diritto di girare liberamente senza che le autorità fossero in grado di seguire ogni nostro passo - questo non era più di poco più di una decina di anni fa!

Prima di questo punto, i governi vi hanno fornito servizi per permettere *a voi* di conoscere la *vostra* posizione -come era stata la tradizione fin dal faro navale- ma non per permettere *a loro* di conoscere la vostra posizione. C'è una differenza cruciale. E, come sempre, la prima breccia è stata quella di fornire ai cittadini dei servizi -in questo caso servizi medici di emergenza- cosicché solo i distopici più lungimiranti si sarebbero opposti.

Che cosa è successo da allora?

Intere città stanno usando il wi-fi tracking passivo per tracciare le persone a livello individuale, in tempo reale e a livello di passo in tutto il centro città.

Le stazioni ferroviarie e gli aeroporti, che un tempo erano rifugi sicuri dell'anonimato nel mondo analogico dei nostri genitori, hanno cartelli che dicono di utilizzare wi-fi passivo in tempo reale e bluetooth tracking di tutti coloro che si avvicinano, e stanno collegando il loro tracking ai dati personali di identificazione. Anzi, mi correggo: hanno dei cartelli *nel migliore dei casi*, ma lo fanno comunque, anche dove i cartelli non ci sono.

L'ubicazione delle persone è tracciata in almeno tre modi diversi..... cioè, più che "in modi diversi", direi "in categorie di modi diversi":

- **Attivo:** Portate con voi un sensore della vostra posizione (sensore GPS, ricevitore Glonass, triangolatore a torre di celle, o anche un identificatore visivo attraverso la fotocamera). Si utilizzano i sensori per trovare la posizione, in un determinato momento o in modo continuo. Il governo si assume il diritto di leggere il contenuto dei sensori attivi.
- **Passivo:** non si intraprende alcuna azione, ma si sta ancora trasmettendo la propria posizione al governo in modo continuo attraverso una terza parte. In questa categoria, troviamo la triangolazione dei ripetitori cellulari, così come il wi-fi passivo e il tracking bluetooth che non richiedono alcuna azione da parte di un utente se non quella di essere acceso.
- **Ibrido:** Il governo trova la vostra posizione in occasionali ping attraverso draghe attive e spedizioni di pesca tecnica in corso. Questo includerebbe non solo le tecniche relative ai telefoni cellulari, ma anche il riconoscimento del volto collegato alle reti TVCC urbane.

La privacy della posizione è una delle Sette Privacy, e possiamo tranquillamente dire che senza contromisure attive, è stata completamente persa nella transizione dall'analogico al digitale. I nostri genitori avevano la privacy della posizione, specialmente in luoghi affollati come aeroporti e stazioni ferroviarie. I nostri figli non hanno la privacy di posizione, non in generale, e in particolare non in luoghi come gli aeroporti e le stazioni ferroviarie che erano i rifugi più sicuri dei nostri genitori analogici.

Come si ripristina la Privacy di Location oggi? La si dava per scontato solo 12 anni fa.

## 5. Che fine ha fatto la libertà di assemblea?

I nostri genitori analogici avevano il diritto di incontrare chi volevano, dove volevano, e discutere di ciò che volevano, senza che il governo lo sapesse. I nostri figli digitali hanno perso tutto questo, solo perché usano oggetti più moderni.

Per molte delle attività dei nostri figli digitali non esiste più la privacy, in quanto esse si svolgono naturalmente in rete. Per chi è nato nel 1980 e oltre, non ha senso parlare di attività "offline" o "online". Ciò che gli anziani vedono come "persone che passano il tempo con il loro telefono o computer", per i più giovani è *socializzare usando il loro telefono o computer*.

Questa è una distinzione importante che la generazione più anziana tende a non capire.

Forse questo è meglio illustrarlo con un aneddoto della generazione precedente: i genitori dei nostri genitori si lamentavano che i nostri genitori stavano parlando *con il telefono*, e non con *un'altra persona che usava il telefono*. Ciò che i nostri genitori vedevano come socializzare (usando un vecchio telefono fisso analogico), i loro genitori a loro volta vedevano come ossessione per un dispositivo. Non c'è niente di nuovo sotto il sole.

(Nota: quando dico "figli digitali", qui, non mi riferisco ai bambini come nei giovani al di sotto della maggiore età; mi riferisco alla prossima generazione di professionisti adulti pienamente capaci.)

Questa socializzazione digitale, tuttavia, può essere limitata, può essere..... autorizzata. Per esempio, richiedere il permesso di qualcuno per socializzare nel modo in cui voi e i vostri amici volete, o addirittura per socializzare in senso lato. Gli effetti di rete sono forti e creano una pressione centralizzata verso alcune piattaforme dove tutti si incontrano, e siccome questi sono servizi privati, i gestori di tali servizi possono stabilire i termini e le condizioni che preferiscono per le persone che si riuniscono e socializzano - per i *miliardi* di persone che vi si riuniscono e socializzano.

Un esempio: Facebook sta usando i valori americani per socializzare, non valori universali. Essere super-contro qualsiasi cosa anche solo leggermente nuda mentre si accettano comparativamente i discorsi di odio non è qualcosa di intrinsecamente globale; è strettamente americano. Se Facebook fosse stato sviluppato in Francia o in Germania invece che negli Stati Uniti, ogni forma di nudità sarebbe stata accolta come arte e cultura del corpo libero (Freikörperkultur) e un modo del tutto legittimo di socializzare, ma il minimo genocidio interrogatorio porterebbe ad un insta-kickban e alla denuncia alle autorità per l'azione penale.

Quindi, solo usando il dominante Facebook come esempio, qualsiasi modo non americano di socializzare è effettivamente vietato in tutto il mondo, ed è probabile che le persone che sviluppano e lavorano con Facebook non ne siano nemmeno consapevoli. Ma la libertà di assemblea non è stata limitata solo nella sfera online, ma anche nel classico mondo analogico offline dove i nostri genitori analogici si frequentavano (e continuano a farlo).

Dal momento che i luoghi delle persone sono tracciati, come abbiamo visto nel post precedente, è possibile abbinare i luoghi tra gli individui e capire chi stava parlando con chi, quando e dove questo è successo, anche se si trattava solo di parlare faccia a faccia. Mentre guardo fuori dalla finestra dell'ufficio a scrivere questo pezzo, mi capita di guardare il vecchio quartier generale della Stasi di fronte ad Alexanderplatz, nell'ex Berlino Est. Era un po' come l'Hotel California; chi ha fatto il check-in tendeva a non andarsene mai. La Stasi rintracciava anche chi stava parlando con chi, ma richiedeva che un sacco di persone eseguissero questo compito manualmente, solo per poter camminare dietro ad altre persone e fotografare con chi stavano parlando - e quindi, c'era un limite economico a quante persone potevano essere rintracciate in qualsiasi momento prima che l'economia nazionale non potesse sostenere una maggiore sorveglianza. Oggi, quel limite è completamente scomparso, e tutti sono monitorati per tutto il tempo.

Hai davvero libertà di assemblea, quando il fatto che hai avuto un contatto con una persona - anzi, magari ha appena trascorso del tempo nella loro vicinanza fisica - può essere usato contro di te?

Lo illustrerò con un esempio. In una grande fuga di notizie di recente, non importa quale, ad un mio collega lontano è capitato di festeggiare un grande evento con una grande festa in prossimità fisica al luogo in cui i documenti venivano in quel momento trafugati; lui si trovava lì completamente inconsapevole del fatto e per pura coincidenza. Mesi dopo, questo collega faceva parte del team di giornalisti che indagava su quei documenti trapelati e sulla loro veridicità, mentre in quel momento ancora inconsapevole della fonte e del fatto che avevano organizzato una grande festa molto vicina all'origine dei documenti.

Il governo era ben consapevole della vicinanza fisica della fuga di notizie combinata con l'accesso giornalistico di questa persona ai documenti; tuttavia emetteva non uno, ma due mandati di arresto a vista per questo lontano collega, sulla base di quella coincidenza. Ora vivono in esilio fuori dalla Svezia e non si aspettano di poter tornare presto a casa.

## 6. Tutto ciò che fai, dici o pensi oggi sarà usato contro di te in futuro

“Tutto ciò che dici o fai può e sarà usato contro di te, in qualunque momento del futuro lontano, quando il contesto e la ragionevolezza di ciò che hai detto o fatto saranno completamente cambiati”. All'epoca della sorveglianza analogica dei nostri genitori, tutto era preso nel contesto del momento. La sorveglianza digitale dei nostri figli salva tutto per usarlo contro di loro in un secondo momento.

È una realtà così orribile, per i nostri figli digitali, che neanche *1984* di Orwell era riuscito ad immaginarla. Nel mondo della sorveglianza analogica, dove le persone erano messe sotto sorveglianza solo *dopo* essere state identificate come sospettate di un crimine, tutto ciò che dicevamo e facevamo era *effimero*. Se il [teleschermo di Winston](#) lo avesse mancato mentre faceva qualcosa di male, Winston sarebbe stato salvo.

La sorveglianza analogica era effimera per due motivi: *primo*, perché si basava sul presupposto che fossero persone a guardare altre persone, e *secondo*, perché nessuno aveva la capacità di trovare istantaneamente le parole dette da una persona nelle conversazioni degli ultimi 20 anni. Nel mondo analogico dei nostri genitori, ciò avrebbe significato che *qualcuno* dovesse materialmente ascoltare venti anni di registrazioni audio in cassette, e ci sarebbero voluti 60 anni per farlo (visto che lavoriamo 8 ore su 24 al giorno). Ma nel mondo digitale dei nostri figli, alle agenzie di sorveglianza basta digitare poche parole per avere una trascrizione automatica di video/audio salvati per sempre su uno schermo, e non solo dalla conversazione di una persona, ma da parte di chiunque. (Non si tratta di un'esagerazione: era realtà già nel 2010, col programma GCHQ-NSA [XKEYSCORE](#)).

Nel mondo dei nostri genitori analogici, *la sorveglianza era una cosa riferita solo a uno specifico momento* nel tempo, nel quale l'individuo era sospettato di aver già commesso uno specifico e grave crimine.

Invece, nel mondo dei nostri figli digitali, *la sorveglianza può essere retroattivamente attivata per qualsiasi ragione o anche senza alcuna ragione specifica*, con l'effetto di Rete che *tutti siamo sotto sorveglianza per qualsiasi cosa abbiamo detto o fatto*.

Potremmo direttamente dire alle persone che la frase è diventata “qualsiasi cosa dici o fai potrà essere usata contro di te, per qualsiasi ragione o senza alcuna ragione, in qualsiasi momento del futuro”.

**La nostra generazione ha completamente fallito nel preservare la *presunzione di innocenza*, almeno applicata alla sorveglianza, nel passaggio dai nostri genitori analogici ai nostri figli digitali.**

Questa sottile aggiunta – che tutto è registrato per un successivo uso contro di te - amplifica l'orrore degli aspetti precedentemente menzionati.

Immagina se qualcuno ti chiedesse dov'eri nel pomeriggio del 13 marzo 1992. A malapena potresti avere una vaga idea di cosa hai fatto in quell'anno ("Vediamo...Mi ricordo che il mio servizio militare iniziò il 3 marzo di quell'anno...e le prime settimane ero in un accampamento nella foresta, con un inverno freddissimo...quindi stavo probabilmente...di nuovo in caserma dopo la prima settimana, avendo la prima lezione di teoria militare di qualcosa? O forse quella data era un sabato o una domenica, nel qual caso sarei andato in vacanza nel fine settimana? "Si tratta della massima precisione che la tua memoria può produrre dopo venticinque anni).

Comunque, quando messo a confronto con i dati di ciò che hai fatto, le persone che ti fanno la domanda avranno a disposizione una *totale e completa* informazione, perché semplicemente tu non la puoi rifiutare. "Eri in questa stanza e hai detto queste parole, secondo la trascrizione dei nostri dati. Insieme a te c'erano altre persone nella stessa stanza. Dobbiamo presumere che ciò che hai detto sia stato comunicato con l'intento di essere udito da loro. Cos'hai da dire in tua difesa"?

Non deve essere necessariamente 25 anni fa. Pochi mesi potrebbero essere sufficienti alla maggior parte delle memorie umane per non essere più molto dettagliate.

Giusto per spingerci oltre: considera che si sa che la NSA custodisce copia anche di tutta la corrispondenza criptata oggi, partendo dal presupposto che anche se oggi non è tecnicamente decrittabile, potrebbe esserlo un domani. Considera anche che ciò che comunichi criptato oggi -sotto forma di testo, voce o video- potrebbe essere usato contro di te fra 20 anni. Probabilmente non conosci neanche metà di esso, perché la gamma di comportamenti socialmente accettabili può mutare in modi imprevedibili, come ha sempre fatto. Negli anni '50 erano del tutto normali certi commenti su alcune minoranze, mentre oggi commenti analoghi porterebbero all'ostracizzazione. Altre minoranze sono ancora "insultabili", ma potrebbero non esserlo in futuro.

Quando ascolti qualcuno che parla da cinquant'anni fa, stavano parlando nel contesto del loro tempo, forse anche con le migliori intenzioni secondo gli standard odierni. Tuttavia, potremmo giudicarli duramente per le loro parole interpretate dal contesto - completamente diverso- di oggi.

**I nostri figli digitali si troveranno ad affrontare esattamente questo scenario, perché tutto ciò che fanno e dicono potrà e sarà utilizzato contro di loro, in qualsiasi momento nel futuro. Non dovrebbe essere così. Dovrebbero avere tutto il diritto di godere degli stessi diritti alla privacy del mondo analogico.**

## 7. Le librerie analogiche erano luoghi di ricerca privata

Quando i nostri genitori analogici cercavano informazioni, quell'attività si svolgeva nelle biblioteche, luoghi in cui la privacy era al sicuro al massimo grado. Quando i nostri figli digitali cercano informazioni, i loro pensieri più profondi vengono raccolti all'ingrosso per il marketing. Come è potuto accadere?

Se stai guardando una particolare professione del mondo analogico che era assolutamente ossessionata dalla privacy dei suoi mecenati, quella era il bibliotecario. Le biblioteche erano luoghi in cui le persone potevano cercare i loro segreti più oscuri, riguardassero la letteratura, scienza, shopping o qualcos'altro. La segretezza delle biblioteche era assolutamente leggendaria.

Quando le istruzioni per fabbricare bombe iniziarono ad apparire sul proto-Internet negli anni '80 - i cosiddetti [BBS](#) - e alcuni politici tentarono di giocare sul panico morale, molti individui dotati di buonsenso si affrettarono a sottolineare che questi "file di testo con ricette di bombe" non erano nulla di diverso da quanto si poteva trovare nella sezione di chimica di una biblioteca -mediocre o poco meglio- e le biblioteche erano sacre. Bastò questo a stroncare il panico morale: ricordare che tutto era già disponibile nelle biblioteche, dove il pubblico poteva accedere in modo anonimo.

Le biblioteche erano luoghi così riservati che i bibliotecari s'indignarono in massa quando l'FBI iniziò a chiedere alle biblioteche la documentazione di chi aveva preso in prestito quale libro - ed è così che furono inventati i famigerati [Warrant Canaries](#). Sì, furono inventati da un bibliotecario, per proteggere i clienti della biblioteca. I bibliotecari sono sempre stati la categoria professionale che ha rappresentato il più strenuo baluardo a difesa della privacy, tanto nel mondo analogico quanto in quello digitale.

**Nel mondo analogico dei nostri genitori, la loro libertà di informazione era sacra: la loro più profonda sete di apprendimento, conoscenza e comprensione. Nel mondo digitale dei nostri figli, i loro pensieri più intimi vengono invece raccolti all'ingrosso e venduti come bigiotteria sul loro viso.**

Qui in palio non c'è solo ciò che i nostri figli digitali hanno studiato con successo. Per i nostri genitori analogici, è quello per cui sono sempre andati in biblioteca. È quello per cui hanno sempre pensato che valesse la pena di andare in biblioteca. Nel mondo dei nostri figli digitali, tutto ciò che cercano viene registrato, e anche tutto ciò che hanno pensato di cercare senza farlo.

Pensateci per un attimo: qualcosa che era per i nostri genitori analogici così sacro che intere categorie professionali avrebbero scioperato per preservarlo, ora è usato casualmente per il marketing all'ingrosso nel mondo dei nostri figli digitali.

E ora unite questo articolo col precedente (#6), ossia sul fatto che tutto ciò che fai, può essere registrato per un uso futuro contro di te, e avremo bisogno di un grande cambiamento nel pensarci molto presto.

Non c'è motivo per cui i nostri figli debbano avere meno libertà di informazione solo perché vivono in un ambiente digitale, rispetto all'ambiente analogico dei nostri genitori. Non c'è motivo per cui i nostri figli digitali non debbano godere dei diritti di privacy equivalenti a quelli dell'era analogica.

Naturalmente, si può obiettare che i motori di ricerca su Internet sono servizi privati, e in quanto tali sono liberi di offrire qualsiasi servizio a loro piacimento a qualsiasi condizione. Ma c'erano anche biblioteche private nel mondo analogico dei nostri genitori. Comunque ritorneremo su questo concetto (*è privato quindi tu non hai voce in capitolo*) un po' più avanti in questa serie.



## **8. L'utilizzo di servizi di terze parti non dovrebbe diminuire l'aspettativa di privacy**

**Ross Ulbricht ha presentato il suo appello alla Corte Suprema degli Stati Uniti la scorsa settimana, evidenziando un importante diritto alla privacy equivalente analogico equivalente nel processo: solo perché stai usando apparecchiature che rendono una terza parte consapevole della tua situazione, questo davvero annulla ogni aspettativa di privacy?**

Nella maggior parte delle costituzioni, c'è una qualche forma di protezione della privacy. Nella Carta Europea dei Diritti Umani, questo è specificato come diritto alla vita privata e familiare, alla casa e alla corrispondenza. Nella Costituzione degli Stati Uniti, ha una struttura leggermente diversa, ma con lo stesso risultato: è un divieto per il governo di invadere la privacy senza giusta causa ("perquisizione e sequestro immotivati").

I tribunali statunitensi ritengono da tempo che, se avete rinunciato volontariamente a una parte della vostra privacy memorizzata digitalmente a terzi, allora non potete più aspettarvi di avere privacy in quell'area. Quando si esamina l'equivalenza analogica per i diritti alla privacy, questa dottrina è atroce, e per capire quanto sia atroce, dobbiamo tornare all'alba dei centralini telefonici manuali.

All'inizio dell'era telefonica, i centralini erano completamente manuali. Quando si richiedeva una chiamata telefonica, un operatore manuale del centralino collegava manualmente il filo del telefono al filo del telefono del ricevitore, e metteva in moto un meccanismo che faceva squillare il telefono. Gli operatori potevano sentire ogni chiamata se volevano e sapevano chi aveva parlato con chi e quando.

Avete ceduto la vostra privacy a terzi quando utilizzate questo servizio telefonico manuale? Sì, probabilmente l'avete fatto. Secondo la dottrina digitale applicata ora, le chiamate telefoniche non avrebbero alcuna privacy, in nessuna circostanza. Ma, come sappiamo, le chiamate telefoniche sono private. Infatti, gli operatori delle telefonate hanno giurato di non dire mai la minima parte di quello che hanno imparato sul lavoro sui rapporti privati delle persone - così seriamente è stata presa in considerazione la privacy, anche da parte delle aziende che gestiscono i centralini.

È interessante notare che questa dottrina della "rinuncia alla privacy da parte di terzi" sembra essere apparsa nel momento in cui l'ultimo operatore di centralino ha lasciato il lavoro per gli odierni interruttori automatici di circuito telefonico. Era il 1983, proprio all'alba della tecnologia digitale di livello consumer come il Commodore 64.

Questa falsa equivalenza da sola dovrebbe essere sufficiente ad affondare la dottrina di cedere "volontariamente" la privacy a terzi nel mondo digitale, e quindi rinunciare all'aspettativa di privacy: l'equivalenza nel mondo analogico era l'esatto contrario.

Ma c'è di più. Da qualche parte in questo concetto è l'idea che si sta scegliendo volontariamente di rinunciare alla propria privacy, come atto attivo e informato - in particolare, un atto che si distingue

dall'ordinario, poiché le Costituzioni del mondo sono molto chiare sul fatto che “di default” si ha un'aspettativa di privacy.

In altre parole, poiché la vita quotidiana delle persone è coperta da aspettative di privacy, ci deve essere qualcosa di fuori dall'ordinario che un governo può rivendicare, dandogli il diritto di togliere la privacy a qualcuno. E questo "fuori dall'ordinario" è stato che le persone in questione portavano un telefono cellulare, e così "volontariamente" hanno rinunciato al loro diritto alla privacy, in quanto il telefono cellulare cede la loro posizione all'operatore di rete contattando le torri dei telefoni cellulari.

Ma portare con sé un cellulare è un comportamento che ci si aspetta oggi. E 'completamente all'interno dei confini del "normale". In termini di aspettative, questo non è molto diverso dall'indossare un jeans o una giacca. Questo ci porta alla domanda: nell'esperimento di pensiero che i produttori di jeans di ieri erano stati in grado di individuare la vostra posizione, era stato ragionevole per il governo di sostenere che si rinuncia a qualsiasi aspettativa di privacy quando si indossano i jeans?

No. No, certo che non lo era.

Non è che tu stia portando con te un dispositivo di monitoraggio della natura selvaggia per l'espresso scopo dei servizi di soccorso per trovarti durante una pericolosa escursione. In una tale circostanza, si potrebbe sostenere che state trasportando volontariamente un dispositivo di localizzazione. Ma non quando si trasporta qualcosa che ci si aspetta da tutti - anzi, qualcosa che tutti devono portare per poter funzionare anche nella società di oggi.

Quando l'unica alternativa ad avere la vostra privacy garantita dalla Costituzione è l'esilio dalla società moderna, un governo dovrebbe avere un caso davvero sottile. Soprattutto quando l'equivalente analogico – i vecchi centralini telefonici - non è mai stato un gioco leale in ogni caso.

Le persone meritano il diritto alla privacy equivalente al mondo analogico.

Fino a quando un governo non lo riconosce e cede volontariamente un potere che si è preso, che non è qualcosa su cui la gente dovrebbe trattenere il fiato, la privacy rimane sotto la propria responsabilità.

## 9. Quando il governo sa cosa leggi, in quale ordine, e per quanto tempo

I nostri genitori analogici avevano la possibilità di leggere notizie in modo anonimo, *in qualunque modo, ovunque e ogniqualvolta* volessero. Per i nostri figli digitali, un agente governativo potrebbe essere alle loro spalle a sorvegliarlo: il Governo sa quali sono le fonti di informazioni che leggono, quali articoli, per quanto tempo e in quale ordine.

Per i nostri genitori analogici, leggere le notizie era una questione privata in cui né il Governo né qualche impresa giocavano alcun ruolo. I nostri genitori compravano un giornale la mattina con pochi spiccioli all'angolo della strada, lo portavano in qualche posto tranquillo in cui potevano trascorrere qualche minuto in santa pace, e se lo leggevano senza che nessuno potesse interferire.

Quando i nostri figli digitali leggono le notizie, il Governo non solo sa quale fonte scelgono di leggere, ma anche quali specifici articoli leggono da quella specifica fonte, in quale ordine, e per quanto tempo. Lo stesso fanno diverse imprese private commerciali. Ci sono almeno 3 gravi problemi in questa situazione.

**Il primo** è che, dal momento che il Governo *possiede* questi dati, potrebbe provare ad *utilizzarli*. Più nello specifico, cercherà di usarli *contro l'individuo in questione*, possibilmente in qualche schema di [pre-crimine](#). Sappiamo questo (cioè che i dati raccolti da un Governo verranno infine usati contro le persone) con [certezza matematica](#).

**In un'economia dell'attenzione, i dati su cosa attira la nostra attenzione, quanto e per quanto tempo, sono assolutamente cruciali per predire i comportamenti. E nelle mani di un Governo che compia il cruciale errore di usarli per scenari di tipo pre-crimine, i risultati possono essere disastrosi per gli individui e chiaramente sbagliati per il Governo.**

Ovviamente, nell'istante in cui un Governo utilizza questi dati in ogni modo immaginabile, positivo o negativo, emergeranno le *Metriche di Heisenberg* -ossia l'atto di usare i dati plasmerà i dati stessi. Per esempio, se qualche membro del Governo decide che informarsi sulla frugalità sia un probabile indicatore di povertà, che rende le persone [che si informano su di essa, *n.d.t.*] più idonee a ricevere sussidi governativi, allora questa situazione farà sì che più gente inizi a informarsi sulla frugalità. Le Metriche di Heisenberg si hanno quando una misurazione non può essere fatta senza invalidare l'intero processo.

(Questo fenomeno è stato così chiamato sulla base del [Principio di Indeterminazione di Heisenberg](#), che viene solitamente confuso con l'[Effetto dell'Osservatore](#), secondo il quale non si può misurare qualcosa senza alterare il processo. Il Principio di Indeterminazione di Heisenberg è in realtà qualcosa di completamente diverso; afferma che non si può misurare un preciso momento e posizione di una particella subatomica allo stesso tempo, e non si applica a tutte le Metriche di Heisenberg)

**Il secondo problema** consiste nel fatto che non solo il Governo, ma anche altre imprese private agiranno secondo queste metriche (siano esse di Heisenberg o meno). E se qualcuno pensasse che leggere i magazine di motociclismo acrobatico possa avere effetti sulla salute e i premi delle polizze assicurative?

**Il terzo problema** è sottile e infido, ma anche più grave: il Governo non solo sa quali articoli hai letto e in quale ordine, ma -corollario di ciò- sa *cosa hai fatto subito dopo letto*. In altre parole, sa in modo preciso quale segmento di informazione ti ha fatto interrompere la lettura e intraprendere una specifica azione. E questa è un'informazione *molto* più pericolosa rispetto all'essere a conoscenza in generale delle tue fonti di informazioni e preferenze.

**Essere in grado di predire le azioni di qualcuno con un alto grado di certezza è molto più pericoloso rispetto all'abilità di essere vagamente a conoscenza dei gusti di qualcuno in fatto di intrattenimento.**

I nostri genitori analogici avevano il diritto alla privacy nello scegliere le fonti di informazione in modo anonimo, senza che nessuno avesse il permesso (o fosse tecnicamente in grado) di dire quali articoli avessimo letto, in quale ordine, per quale motivo. Non è affatto irragionevole pretendere che i nostri figli abbiano lo stesso diritto alla privacy.

La privacy resta una tua responsabilità personale.

## 10. Il giornalismo analogico era protetto, quello digitale no

Nel mondo analogico dei nostri genitori, le “soffiate” (orig. *leaks*) alla stampa erano altamente protette da entrambi i lati -sia per colui che faceva la soffiata sia per il reporter che la riceveva. Nel mondo digitale dei nostri figli, tutto ciò è stato buttato dalla finestra senza troppe cerimonie, mentre si discuteva di cose completamente privo di correlazione con ciò. Perché i nostri figli digitali non dovrebbero aver diritto agli stessi pesi e contrappesi?

Un altro settore in cui i diritti alla privacy non sono sopravvissuti al passaggio dall'analogico al digitale è quello del giornalismo, un ombrello di diverse attività che noi consideriamo un importante fattore nel sistema di pesi e contrappesi (orig. *Checks-and-balances*) nella società. Quando qualcuno consegnava documenti fisici a un giornalista, si trattava di un'azione analogica che era protetta da leggi federali e statali, e talvolta anche da costituzioni. Quando qualcuno consegna l'accesso digitale alle stesse informazioni allo stesso tipo di giornalista, riflettendo il modo in cui lavoriamo oggi e il modo in cui i nostri figli lavoreranno in futuro, è invece perseguibile da entrambe le parti.

Lasciate che vi illustri questa affermazione con un esempio tratto dal mondo reale.

Durante le elezioni svedesi del 2006, ci fu uno scandalo su una disastrosa falla di sicurezza informativa sul comportamento del partito allora al governo (sì, lo stesso partito che in seguito amministrò [la più grave fuga di notizie di sempre](#)). Uno username e una password che circolavano e che davano completo accesso ai più remoti file sui server del partito Socialdemocratico, da qualsiasi postazione. Lo username apparteneva a Stig- Olof Friberg, che utilizzava “sigge” sia come username che come password, e aveva diritto di accedere ai più segreti file degli uffici Social democratici attraverso una rete wireless aperta e non criptata.

Definire questa situazione “scarsa sicurezza” è riduttivo. Considerate che queste erano -e sono tuttora- le Istituzioni e le persone su cui facciamo affidamento per le politiche di salvaguardia dei dati sensibili dei cittadini.

Comunque, all'ombra di questo, c'era anche il dettaglio più importante: alcuni giornalisti politici erano ben consapevoli dell'esistenza di queste credenziali di accesso, come uno dei più famosi giornalisti politici svedesi Niklas Svensson, che aveva usato le credenziali come strumento giornalistico per ottenere informazioni sul funzionamento del partito al governo.

È qui che la storia diventa interessante: nel mondo analogico, quel giornalista avrebbe ricevuto quei *leaks* sotto forma di documenti copiati, consegnati fisicamente a lui, e la fuga di notizie in questo modo analogico era (ed è tuttora) estremamente protetta dalla legge, nonché da alcune costituzioni: in Svezia, ad esempio si può persino andare in prigione per speculazioni casuali fatte al lavoro durante la pausa caffè che potrebbero essere state all'origine di una fuga di notizie sulla stampa. È preso molto sul serio.

Tuttavia, in questo caso, al giornalista non sono arrivati i documenti, ma una chiave per l'accesso ai documenti digitali - le credenziali incredibilmente insicure "sigge / sigge" - ed è stato condannato in giudizio per accesso abusivo a un portale elettronico, *nonostante svolgesse un lavoro giornalistico con un chiaro e protetto equivalente analogico.*

È interessante guardare alla storia per vedere quanto eventi di importanza critica non sarebbero mai stati scoperti, se questa accusa di giornalismo digitale fosse stata applicata al giornalismo analogico.

Per esempio, prendiamo la fuga di notizie su [COINTELPRO](#), quando gli attivisti copiarono i file da un ufficio dell'FBI per smascherare un'operazione segreta e altamente illegale da parte delle forze dell'ordine per screditare le organizzazioni politiche basandosi esclusivamente sulla loro opinione politica. (Questo non è ciò che le forze dell'ordine dovrebbero fare, parlando in termini generali). Questa fuga di notizie si è verificata quando gli attivisti misero un biglietto sulla porta dell'FBI l'8 marzo 1971, scrivendo "Per favore non chiudere questa porta stasera"; poi tornarono nel bel mezzo della notte, quando nessuno era lì, e trovarono la porta sbloccata come richiesto, e rubarono circa 1000 file classificati che rivelavano le pratiche illegali.

Questi vennero poi spediti a vari organi di stampa. Il furto portò all'esposizione di alcuni dei documenti più auto-incriminanti dell'FBI, tra cui diversi documenti che descrivono l'uso da parte dell'FBI di impiegati delle poste, centralinisti, ecc., al fine di spiare studenti universitari neri e vari gruppi di attivisti neri nonviolenti, [secondo Wikipedia](#). Ed ecco il kicker nel contesto: mentre le persone che rubavano i documenti potevano e sarebbero stati incriminati per averlo fatto, *era impensabile accusare i giornalisti di riceverli.*

Oggi non è più così.

**I nostri figli digitali hanno perso il diritto di far arrivare informazioni ai reporter. Un'attività che era data per scontata -nonché vista come di cruciale importanza per il bilanciamento dei poteri – nel mondo dei nostri genitori analogici. I nostri figli digitali che lavoreranno come giornalisti non potranno più ricevere *leak* che mostrino gli abusi di potere. È del tutto ragionevole che i nostri figli digitali abbiano almeno le stesse libertà civili di cui godevano i loro genitori nel mondo analogico.**

## 11. I nostri genitori usavano denaro anonimo

**Il denaro anonimo dei nostri genitori analogici sta rapidamente scomparendo, e al suo posto arrivano carte di debito tracciabili e autorizzate per i nostri figli. Ancorché conveniente, è un lupo travestito da pecora.**

Nell'ultimo articolo abbiamo visto come i nostri genitori analogici potessero comprare un giornale in modo anonimo all'angolo della strada con qualche spicciolo, e leggere la loro fonte di notizie preferita senza che nessuno lo sapesse.

Questo discorso si può estendere molto oltre i giornali, ovviamente.

La possibilità dei nostri genitori di portare a termine transazioni decentralizzate e sicure in modo anonimo è stata del tutto persa in un panorama che continua a spingere per i pagamenti con le carte di credito per comodità.

La comodità di non pagare in anticipo, con carte di credito; la comodità di pagare sempre un importo esatto, con carte di debito; la comodità di non dover trasportare e trovare quantità esatte con ogni acquisto. Alcuni potrebbero persino obiettare che avere ogni transazione elencata su un estratto conto è una comodità della contabilità.

Ma con la contabilità arriva il monitoraggio. Con il monitoraggio arriva la prevedibilità e la responsabilità indesiderata.

È stato detto che un dirigente VISA può prevedere un divorzio un anno prima delle parti coinvolte, in base ai cambiamenti nei modelli di acquisto. Tristemente, un negozio [Target](#) si rivolgeva a una *teenager* con pubblicità per maternità, cosa che in un primo momento rese il padre furioso: ma, [come si scoprì in seguito](#), la giovane donna era davvero incinta. Target lo sapeva, suo padre no.

Questo accade perché quando non si usa più denaro anonimo, ogni singolo acquisto è tracciato e registrato, con l'intento esplicito di usarlo contro di noi -che sia per spingerci a fare certe scelte o ad esaurire le nostre risorse (“compra di più”), o magari per punirci per aver comprato qualcosa che non avremmo dovuto comprare, in una vasta gamma di modi concepibili.

La Cina sta già spingendo il concetto oltre, e potrebbe aver ispirato [un episodio di Black Mirror](#): sta ponderando i punteggi di obbedienza dei suoi cittadini in base al fatto che comprino oggetti utili o generosi - utili nelle opinioni del regime, naturalmente.

Non è solo il fatto che le transazioni dei nostri figli digitali vengono registrate per un uso futuro contro di loro, in un modo in cui i nostri genitori analogici non potrebbero mai concepire.

È anche il fatto che le transazioni dei nostri figli digitali siano *autorizzate*. Quando i nostri figli digitali comprano una bottiglia d'acqua con una carta di debito, una transazione viene autorizzata da qualche parte in background. Ma ciò significa anche che qualcuno può decidere di *non autorizzare* la transazione; qualcuno ha il diritto di decidere arbitrariamente ciò che le persone comprano e non comprano, se questa tendenza continua per i nostri figli digitali. Questo è un pensiero orribile.

I nostri genitori utilizzavano transazioni decentralizzate, resistenti alla censura e anonime usando denaro normale. Non c'è ragione per cui i nostri figli digitali dovrebbero avere qualcosa di meno. È una questione di libertà e autodeterminazione.



## 12. I nostri genitori compravano senza essere tracciati. I loro movimenti nei negozi non erano registrati

Nell'ultimo articolo abbiamo visto come oggi le persone siano tracciate quando usano carte di credito al posto dei contanti. Tuttavia, ad un'occhiata più attenta, possiamo renderci conto che vengono tracciati *anche* quando usano i contanti.

Poche persone prestano attenzione al piccolo cartello sulle porte girevoli dell'aeroporto Schiphol, ad Amsterdam. Dice che il Wi-fi e il bluetooth tracciano ogni singolo individuo si trovi nell'aeroporto.

Ciò che rende unico l'aeroporto di Schiphol è che non tracciano i movimenti delle persone nelle zone commerciali. (È per scopi commerciali, non di sicurezza). No, ciò che lo rende unico che oltretutto *lo dicono* alle persone. (L'Olanda di solito prende la privacy sul serio, come la Germania, e per le stesse ragioni).

I [locator beacons](#) sono praticamente uno standard nelle aree commerciali più grandi ora. Eseguono il ping del telefono tramite wi-fi e bluetooth e, utilizzando la triangolazione dell'intensità del segnale, una griglia di locator beacon è in grado di mostrare come ogni singolo individuo si muove in tempo reale a livello di singoli passi. Questa prassi viene usata per "ottimizzare il marketing" - in altre parole, trovare il modo di ingannare il cervello delle persone per spendere risorse che altrimenti non avrebbero. La nostra stessa perdita di privacy è contro di noi, come sempre.

Dove si fermano le persone per un po', cosa attira la loro attenzione e cosa no, qual è un buon posto per vendere di più?

Queste sono domande legittime. Quello che non è legittimo è trovare le risposte togliendo la privacy alle persone.

Questo tipo di tracciamento individuale di massa è stato persino utilizzato a livello cittadino, cosa che è avvenuta in completo silenzio fino a quando l'Osservatorio di vigilanza sulla privacy di un governo remoto ha lanciato l'allarme. La città di Västerås ha ottenuto il via libera per continuare a tracciare, una volta soddisfatti alcuni criteri formali.

Sì, è provato che questo tipo di tracciamento delle persone è già stato implementato a livello cittadino in almeno una piccola città in una parte remota del mondo (Västerås, Svezia). Con l'Organo di supervisione della privacy del governo che ha fatto spallucce e ha detto "ok, qualunque cosa sia", non aspettatevi che questo rimanga nella piccola città di Västerås. Anzi, mi correggo, ho usato il tempo sbagliato: non aspettatevi che **sia rimasto** solo Västerås, dove ha ricevuto il via libera tre anni fa.

I nostri genitori analogici avevano la possibilità di camminare in città e nella strada di loro scelta senza essere tracciati, e senza che ciò venisse usato o contro di loro. Non è irragionevole pretendere che i nostri figli digitali abbiano lo stesso diritto.

C'è un altro modo per comprare cose in contanti che evita questo tipo di tracciamento, ed è il pagamento in contassegno quando ordini qualcosa online o per telefono alla tua porta - nel qual

caso il tuo acquisto è anche autenticato e registrato, solo in un altro tipo di sistema.

Questo non è solo usato contro il comune cittadino per scopi di marketing, ovviamente. È usato contro il cittadino comune per ogni scopo immaginabile. Ma torneremo su questo in un articolo successivo della serie.

## 13. I nostri figli digitali sono tracciati non solo in tutto ciò che comprano, ma anche in ciò che *non* comprano

Abbiamo visto come la privacy dei nostri figli digitali venga violata in tutto ciò che acquistano in contanti o a credito, in un modo a cui i nostri genitori analogici si sarebbero ribellati. Ma c'è di peggio: la privacy dei nostri figli digitali è violata anche dal monitoraggio di ciò che *non* comprano, sia che declinino attivamente sia che ignorino semplicemente un'offerta.

Amazon ha appena aperto il suo primo negozio "Amazon Go", dove si raccolgono le cose in una borsa e si va via, senza mai passare attraverso un processo di checkout. Come parte dell'introduzione di questo concetto, Amazon sottolinea che è possibile raccogliere qualcosa dagli scaffali – in tal caso il negozio registrerà il vostro acquisto - e cambiare idea e rimmetterlo sullo scaffale – e in quel caso sarete registrati e annotati come clienti che non hanno acquistato l'articolo.

Certo, non si sta pagando per qualcosa su cui si è cambiato idea, che è il punto della presentazione video. Ma non si tratta solo della deduzione dall'importo totale da pagare: Amazon sa anche che hai preso in considerazione l'acquisto e alla fine non lo hai fatto, e utilizzerà questi dati.

I nostri figli digitali sono seguiti in questo modo su base giornaliera, se non oraria. I nostri genitori analogici non lo sono mai stati.

Quando facciamo acquisti online, ci sono anche [semplici plugin](#) per le più comuni soluzioni commerciali con i termini commerciali "funnel analysis" - dove nel cosiddetto "purchase funnel" i nostri figli digitali scelgono di lasciare il processo di acquisto di qualcosa - o "cart abandonment analysis".

Non possiamo nemmeno più semplicemente allontanarci da qualcosa senza che venga registrato, registrato e catalogato per un successivo utilizzo contro di noi.

Ma il cosiddetto "abbandono del carrello" è solo una parte della più grande questione del monitoraggio di ciò che ci interessa nell'era dei nostri figli digitali, ma che non abbiamo comprato. Molte persone oggi giurerebbero di aver parlato di uno specifico prodotto con il loro telefono presente (ad esempio, "gonne di pelle nera") e, all'improvviso, la pubblicità per quel tipo di prodotto specifico sarebbe apparsa su Facebook e/o gli annunci di Amazon. E' davvero dovuto a qualche azienda che ascolta le parole chiave attraverso il telefono? Forse sì, forse no. Tutto quello che sappiamo dalle rivelazioni di Snowden è che se è *tecnicamente possibile* invadere la privacy, ciò sta già accadendo.

(Dobbiamo presumere che queste persone devono ancora imparare a installare un semplice adblocker.)

Nei luoghi più affollati, come (ma non solo) gli aeroporti, ci sono degli eyeball tracker per scoprire quali annunci si guardano. Non cambiano ancora per soddisfare i tuoi interessi, come nel film

Minority Report, ma questa funzione è già presente sul tuo telefono e sul tuo desktop, e quindi non sarebbe sorprendente vedere in pubblico presto.

Nel mondo dei nostri genitori analogici, non siamo stati registrati e monitorati quando abbiamo comprato qualcosa.

Nel mondo dei nostri figli digitali, siamo registrati e monitorati anche quando *non* compriamo qualcosa.

## 14. Le preferenze dei nostri genitori analogici in materia di appuntamenti non venivano monitorate, registrate e catalogate

Le preferenze dei nostri genitori analogici in materia di appuntamenti erano considerate la questione più privata di tutte. Per i nostri figli digitali, le loro preferenze in materia di incontri sono un'opportunità di raccolta all'ingrosso a fini di marketing. Come è avvenuto questo terrificante cambiamento?

Credo che il primo grande raccoglitore di preferenze di incontri sia stato l'innocente hotornot.com 18 anni fa, un sito che sembrava più un lavoro secondario di un liceale frustrato che una manovra di marketing intelligente. Permetteva semplicemente alle persone di valutare l'attrattiva soggettiva percepita di una fotografia e di caricare le fotografie per tale valutazione. (I due fondatori di questo presunto progetto collaterale del liceo hanno guadagnato 10 milioni di dollari ciascuno per il sito quando è stato venduto).

Poi la scena è esplosa, con siti di incontri finanziati sia dagli utenti che dalla pubblicità, che hanno catalogato le preferenze di incontri delle persone nei minimi dettagli.

Siti pornografici su larga scala, come Pornhub, hanno anche iniziato a catalogare le preferenze pornografiche della gente, e a produrre [interessanti infografiche](#) sulle differenze geografiche delle preferenze. E' particolarmente interessante, in quanto Pornhub è in grado di suddividere le preferenze in modo specifico per età, posizione, sesso, fasce di reddito, e così via.

Conoscete qualcuno che ha detto a Pornhub qualcuno di questi dati? No, nemmeno io. E ancora, sono in grado di individuare a chi piace cosa che con una certa precisione, precisione che viene da qualche parte.

E poi, naturalmente, abbiamo i Social Network (che possono o meno essere responsabili di questo monitoraggio, tra l'altro).

E' stato riferito che [Facebook può dire se sei gay o meno con un minimo di tre like](#). Tre. E non devono essere correlati a preferenze di incontri o preferenze di stile di vita - possono essere selezioni casuali che si limitano a mappare bene con modelli più grandi.

Questo è già abbastanza brutto di per sé, sulla base del fatto che si tratta di dati privati. Come minimo, le preferenze dei nostri figli digitali dovrebbero essere le loro, proprio come il loro gelato preferito.

Ma le preferenze di incontri non sono solo una preferenza come scegliere il tuo gusto di gelato, vero? Dovrebbe esserlo, ma non lo è in questo momento. Potrebbe anche essere qualcosa con cui sei nato. Qualcosa per cui le persone vengono uccise anche se *nascono* con la preferenza sbagliata.

E' ancora illegale nascere omosessuale in 73 paesi su 192, e su questi 73, undici prescrivono la pena di morte per essere nati in questo modo. Solo 23 paesi su 192 hanno piena parità di matrimonio.

Inoltre, anche se la direzione politica è a senso unico verso una maggiore tolleranza, accettazione e inclusione in questo momento, ciò non significa che la tendenza politica non può invertire per una serie di ragioni, la maggior parte delle quali molto negative. Le persone che si sentivano a proprio agio nell'esprimersi possono essere nuovamente perseguitate.

Il genocidio si basa quasi sempre su dati pubblici raccolti con intento benevolo.

Ecco perché la privacy è l'ultima linea di difesa, non la prima. E quest'ultima linea di difesa, che ha tenuto duro per i nostri genitori analogici, è stata violata per i nostri figli digitali. La questione non è presa abbastanza sul serio.

## 15. Le conversazioni digitali dei nostri figli sono silenziate a seconda dell'argomento

Nel peggiore dei casi, ai nostri genitori analogici potrebbe essere stato impedito di incontrarsi. Ai nostri figli digitali viene impedito di parlare di argomenti specifici, una volta che la conversazione è già in corso. Si tratta di uno sviluppo spaventoso.

Quando i nostri figli digitali pubblicano un link a The Pirate Bay da qualche parte su Facebook, a volte si apre una piccola finestra che dice "avete pubblicato un link con contenuti potenzialmente dannosi. Si prega di astenersi dal pubblicare tali link".

Sì, anche in conversazioni private. *Soprattutto* nelle conversazioni private.

Questo può sembrare una piccola cosa, ma è davvero enorme. Ai nostri figli digitali non viene impedito di avere una conversazione, di per sé, ma sono sorvegliati sugli argomenti negativi che il regime non ama siano discussi, e viene impedito loro di discutere di *quegli argomenti*. Questo è molto peggio che impedire ad alcune persone di incontrarsi.

L'equivalente analogico sarebbe stato se i nostri genitori, durante una conversazione telefonica, a un certo punto avessero sentito una terza voce minacciosa e lenta che parlava abbastanza dolcemente da essere percepita come minacciosa: "Lei ha parlato di un argomento proibito. Vi preghiamo di astenervi dal parlare di argomenti proibiti in futuro".

I nostri genitori sarebbero rimasti inorriditi se ciò fosse accaduto - e giustamente!

Ma nel mondo digitale dei nostri figli, lo stesso fenomeno viene invece incoraggiato dalle stesse persone che lo aborrissero se accadesse nel loro mondo, a sé stessi.

In questo caso, naturalmente, sono tutti i link a The Pirate Bay che sono considerati argomenti proibiti, sotto il presupposto - *presupposto!* - che portino alla produzione di copie che violerebbero il monopolio del diritto d'autore.

Quando ho visto per la prima volta la finestra di Facebook sopra che mi diceva di non discutere argomenti proibiti, stavo cercando di distribuire materiale politico che avevo creato io stesso, e ho usato The Pirate Bay per distribuire. Si dà il caso che sia un modo molto efficiente per distribuire file di grandi dimensioni, ed è proprio per questo motivo che viene usato da molte persone (eeh, chi l'avrebbe mai pensato?), comprese persone come me che volevano distribuire grandi collezioni di materiale politico.

Ci sono canali di comunicazione privati, ma troppi pochi li usano, e i politici in generale (sì, questo include i nostri genitori analogici) continuano a sostenere questo andazzo, a causa del "terrorismo" e altri spauracchi.

## 16. La sorveglianza retroattiva di tutti i nostri figli

Nel mondo analogico dei nostri genitori, era assolutamente impensabile che il governo chiedesse di conoscere ogni passo che hai fatto, ogni telefonata che hai fatto e ogni messaggio che hai scritto, proprio come una questione di routine. Per i nostri figli digitali, i funzionari governativi continuano ad insistere su questo come se fosse perfettamente ragionevole, perché c'è da combattere il terrorismo, e anche i nostri figli digitali possono ascoltare musica o guardare la TV insieme, il che è illegale nel modo in cui amano farlo, a causa della legislazione sulle vendite per corrispondenza di Hollywood. A peggiorare ulteriormente le cose, la sorveglianza è retroattiva: viene registrata, registrata e conservata fino a quando qualcuno la vuole tutta.

Circa dieci anni fa, un mio collega si è trasferito dall'Europa in Cina. Egli ha osservato che, tra le tante differenze, il servizio postale è molto più controllato, in quanto ogni lettera inviata viene annotata a mano su una riga di un giornale di bordo, tenuto dal postino di ogni ufficio postale. Mittente, destinatario e data.

All'epoca, tre cose mi colpirono: *primo*, quanto ciò sembrasse naturale alla popolazione cinese, non conoscendo davvero nessun altro sistema al mondo; *secondo*, quanto i nostri genitori analogici si sarebbero scandalizzati dinanzi a questo concetto; *terzo*, il fatto che, nonostante il punto 2, questo è esattamente ciò che i nostri legislatori analogici stanno facendo a tutti i nostri figli digitali in questo momento.

O almeno cercano di farlo; i tribunali si stanno opponendo duramente.

Sì, sto parlando della conservazione della [Telecommunications Data Retention](#).

C'è un detto, che rispecchia abbastanza bene il sentimento cinese di normalità in proposito: "Le stronzate che questa generazione sopporta come un fastidio temporaneo da parte di politici squilibrati sembreranno perfettamente ordinarie per la prossima generazione".

Ogni pezzo di sorveglianza finora in questa serie è amplificato da diversi ordini di grandezza dalla nozione che non solo sei guardato, ma che tutto ciò che fai è registrato per un uso successivo contro di te.

Questo è un concetto così brutto, che nemmeno Orwell in 1984 l'ha pensato: se il teleschermo di Winston l'avesse mancato mentre faceva qualcosa di sgradito al regime, Winston sarebbe stato al sicuro, perché non c'era nessuna registrazione in corso, ma solo sorveglianza *in quel momento*.

Se Winston Smith avesse avuto il regime di sorveglianza di oggi, con la registrazione e la conservazione dei dati, il regime avrebbe potuto tornare indietro e avrebbe riesaminato ogni azione precedente a quella che poteva essere sfuggita.



Questo orrore è realtà *ora*, e si applica ad ogni pezzo di questa serie. I nostri figli digitali non sono solo senza privacy *in questo momento*, ma anche in passato sono stati retroattivamente senza privacy.

(Beh, questo orrore è una realtà che va e viene, come i legislatori e i tribunali sono in un tiro alla fune di guerra. Nell'Unione Europea, la conservazione dei dati è stata autorizzata nel 2005 dal Parlamento Europeo, non è stata autorizzata nel 2014 dalla Corte di Giustizia Europea, e proibita nel 2016 dalla stessa Corte. Altre giurisdizioni stanno giocando a giochi simili; un tribunale britannico ha appena sferrato un colpo alla Data Retention, per esempio.)

## 17. C'era una volta l'inviolabilità dei diari

**Per i nostri genitori analogici, un diario o una lettera personale potrebbero raramente essere toccati dalle autorità, nemmeno dalle forze dell'ordine che cercano prove di un crimine. Oggetti come questi avevano una protezione che va al di là delle garanzie costituzionali sulla privacy. Per i nostri figli digitali, tuttavia, i diari e le lettere equivalenti non sono nemmeno considerati degni della privacy costituzionale di base.**

Nella maggior parte delle giurisdizioni, esiste un diritto costituzionale alla privacy. Le forze dell'ordine in questi paesi non possono semplicemente entrare e leggere la posta di qualcuno, intercettare le chiamate telefoniche o rintracciare i loro indirizzi IP. Hanno bisogno di un'ordinanza del tribunale per farlo, che a sua volta si basa su un sospetto concreto di un reato grave: il caso generale è che si ha diritto alla privacy, e le violazioni di questo diritto sono l'eccezione, non la norma.

Tuttavia, di solito c'è un livello di protezione supplementare a questo: anche se e quando le forze dell'ordine ottengono il permesso da un giudice di violare la privacy di qualcuno sotto forma di un mandato di perquisizione della propria abitazione, ci sono alcune cose che non possono essere toccate a meno che non vengano concessi permessi specifici e aggiuntivi dallo stesso tipo di giudice. Questa classe di oggetti include gli oggetti più intimi: lettere private, diari e così via.

Naturalmente, questo è vero solo nel mondo analogico dei nostri genitori. Anche se la lettera della legge è la stessa, questa protezione non si applica affatto al mondo digitale dei nostri figli, ai loro diari e alle loro lettere.

Perché il diario moderno è tenuto su un computer. Se non su un computer desktop, allora certamente su un computer portatile mobile - quello che per ragioni storiche chiamiamo "telefonino", ma che è in realtà un computer portatile a tutti gli effetti.

E il computer era solo uno strumento di lavoro, nel mondo analogico dei nostri genitori. Ci molti precedenti giuridici che stabiliscono che qualsiasi dispositivo elettronico è uno strumento di lavoro, e questo poteva essere vero nel vecchio mondo analogico; e le forze dell'ordine sono ben liete di aggrapparsi a questi precedenti giuridici, anche ora che i nostri dispositivi digitali contengono i nostri diari, le nostre lettere personali e altri oggetti molto più privati di quanto un diario analogico sia mai stato in grado di fare.

Proprio così: mentre i diari dei tuoi genitori erano estremamente protetti dalla legge, i diari dei tuoi figli - non meno privati di quelli dei tuoi genitori - sono protetti dalle perquisizioni e dai sequestri come una normale chiave in acciaio in un laboratorio casuale.

Quindi la domanda è: come siamo arrivati dal punto A al punto B qui? Perché la Polizia, che sa di non poter toccare un diario analogico durante una perquisizione domiciliare, afferra istantaneamente telefoni cellulari che servono allo stesso scopo per i nostri figli?

"Perché possono", è la risposta breve. "Anche perché nessuno punta più i piedi" per i punti avanzati del corso di educazione civica. E anche perché alcune persone hanno visto politici di assai corte vedute affermare di voler usare "il pugno duro col crimine", anche a patto di cancellare completamente i diritti conquistati duramente nel processo.

Crittografate tutto.

## 18. I nostri genitori analogici avevano conversazioni private, sia in pubblico che a casa

I nostri genitori, almeno nel mondo occidentale, avevano il diritto di tenere conversazioni private faccia a faccia, sia in pubblico che nella santità della loro casa. Per i nostri figli digitali non c'è più niente di tutto ciò.

Non molto tempo fa, la cosa dei libri e dei film dell'orrore era che ci sarebbe stata in realtà una sorveglianza diffusa di ciò che lei ha detto all'interno della sua stessa casa. I nostri genitori analogici hanno letteralmente avuto questo come storie spaventose degne di Halloween, mescolando l'orrore con l'assoluta incredulità.

*Naturalmente, non c'era modo di sapere se in un dato momento si era sotto osservazione. Quante volte o su quale sistema la Psicopolizia avesse collegato ogni singolo dispositivo, era una cosa su cui si poteva solo tirare a indovinare. Era persino concepibile che ascoltassero sempre tutti. Ma in ogni caso potevano ascoltarti quando volevano. Dovevi vivere – e lo facevi, dopo che l'abitudine era diventata istinto - nell'assunto che ogni suono che producevi fosse ascoltato.*

(G. Orwell, 1984)

In Occidente, eravamo orgogliosi di non essere l'Oriente - in particolare l'Oriente comunista - che considerava i propri cittadini come sospetti: sospetti che avevano bisogno di essere purificati dai cattivi pensieri e dalle cattive conversazioni, al punto che le case comuni venivano intercettate per le conversazioni ordinarie.

C'erano microfoni sotto ogni tavolo del bar e in ogni residenza. E anche se non ci fossero in senso letterale, proprio lì e poi, potrebbero essere ancora ovunque, quindi bisognava vivere - ha vissuto - ha vissuto, da abitudine che è diventata istinto - nell'assunto che ogni suono che hai fatto è stato ascoltato.

*Per favore, parla forte e chiaro nel vaso di fiori.*

*(Un comune non-scherzo sulle società comuniste durante la Guerra Fredda)*

Tralasciamo per un momento le chiamate telefoniche e altre conversazioni a distanza, dato che sappiamo già che vengono intercettate sulle piattaforme più comuni. Guardiamo le conversazioni in una casa privata.

Ora abbiamo Siri e Alexa. E mentre essi potrebbero aver voluto mantenere le vostre conversazioni per se stessi, fuori dalla portata delle autorità, Amazon [ha già consegnato le registrazioni del soggiorno alle autorità](#). In questo caso, il permesso è diventato un punto controverso perché il sospetto ha dato il permesso. Nel prossimo caso, il permesso potrebbe non esserci, e potrebbe accadere comunque.

I telefoni cellulari sono già in ascolto, in continuazione. Lo sappiamo perché quando diciamo "Ok Google" a un telefono Android, questo si sveglia e ascolta più intensamente. Questo, come minimo,

significa che è sempre in ascolto delle parole "Ok Google". Gli iPhone hanno un meccanismo simile per ascoltare "Hey Siri". Anche se è nominalmente possibile spegnerli, è una di quelle cose di cui non si può mai essere sicuri. E portiamo con noi questi microfoni di sorveglianza governativi ovunque andiamo.

Se i documenti di Snowden ci hanno mostrato una “regola” generale, questa è che se una certa forma di sorveglianza è tecnicamente possibile, sta già accadendo.

E anche se Google e Apple non stanno già ascoltando, la polizia tedesca ha avuto il via libera per entrare nei telefoni e piantarci dei malware, l'equivalente dei microfoni nascosti nel vaso di fiori. Si potrebbe pensare che la Germania di tutti i paesi ha nella memoria recente che cattiva idea sia questa. Si potrebbe - forse addirittura si dovrebbe - si potrebbe supporre che le forze di polizia di altri paesi hanno e stanno già utilizzando strumenti simili.

Per i nostri genitori analogici, il concetto di conversazione privata era evidente quanto l'ossigeno nell'aria. I nostri figli digitali potrebbero non sapere come ci si sente.

E così viviamo oggi - da quella che è iniziata come un'abitudine che è già diventata istinto - nell'assunto che ogni suono che facciamo è ascoltato dalle autorità.

## 19. I teleschermi in soggiorno

Le storie distopiche degli anni '50 dicevano che il governo avrebbe installato telecamere nelle nostre case, con il governo che ci ascoltava e ci osservava in ogni momento. Queste storie erano tutte sbagliate, perché le telecamere le abbiamo installate noi stessi.

Nel mondo analogico dei nostri genitori, è stato dato per scontato che il governo non ci avrebbe guardato nelle nostre case. È un'idea così importante, è scritta nelle costituzioni stesse degli stati di tutto il mondo.

Eppure, per i nostri figli digitali, questa regola, questa pietra miliare, questo principio è semplicemente..... ignorato. Solo perché la loro tecnologia è digitale, anziché quella analogica dei nostri genitori.

Ci sono molti esempi di come ciò sia avvenuto, nonostante sia assolutamente *verboten*. Forse il più importante è il programma [OPTIC NERVE](#) dell'agenzia di sorveglianza britannica GCHQ, che intercetta le videocchiamate senza che le persone interessate ne siano a conoscenza.

Sì, questo significa che il governo stava effettivamente indagando a distanza nei salotti della gente. Sì, questo significa che a volte hanno visto persone nude. Un bel po' di "a volte", anche.

Secondo i riassunti in The Guardian, [oltre il dieci per cento](#) delle conversazioni viste può essere stato sessualmente esplicito, e il 7,1% conteneva [nudo indesiderato](#).

Assaggiate questo termine. Dillo ad alta voce, per sentire di persona quanto sia realmente opprimente. "Nudità indesiderabile". Il modo in cui sei descritto dal governo, in un file su di te, quando guarda nella tua casa privata senza il tuo permesso.

**Quando il governo ti scrive che hai "nudità indesiderata" in casa tua.**

Ci sono molti altri esempi, come [le scuole statali che attivano le webcam emesse dalle scuole](#), o anche il governo degli Stati Uniti che ammette candidamente che [tutti i vostri dispositivi domestici saranno usati contro di voi](#).

E' troppo difficile non pensare alla citazione da 1984:

*Il Teleschermo ha ricevuto e trasmesso simultaneamente. Ogni suono che Winston faceva, al di sopra del livello di un sussurro molto basso, sarebbe stato da lui ripreso, inoltre, fintanto che egli rimaneva nel campo visivo che la placca metallica gli comandava, poteva essere visto e sentito.*

E, naturalmente, questo è già successo. Le cosiddette "Smart TV" di LG, Vizio, Samsung, Sony e sicuramente altri [sono stati sorpresi a fare proprio questo](#) - spiare i suoi proprietari. Si può sostenere che i dati raccolti sono stati raccolti solo dal produttore televisivo. E' ugualmente discutibile che i poliziotti che bussano alla porta di quel produttore che non hanno il diritto di tenere tali dati per sé stessi, ma che il governo vuole partecipare anche all'azione.

Non c'è assolutamente nessuna ragione per cui i nostri figli digitali non dovrebbero godere dei diritti analogici equivalenti di avere una casa propria per se stessi, un diritto che i nostri genitori analogici hanno dato per scontato.

## 20. Il tuo boss analogico non poteva leggere la tua posta. Mai.

Slack ha aggiornato i suoi Termini di servizio per permettere al tuo manager di leggere le tue conversazioni private in canali privati. I nostri genitori analogici sarebbero rimasti scioccati e inorriditi dall'idea stessa che i loro capi avrebbero aperto i pacchetti e letto i messaggi personali che erano loro indirizzati. Per i nostri figli digitali, è un'altra parte della vita di tutti i giorni.

Il vecchio sistema telefonico analogico, a volte abbreviato POTS, è un buon modello per come le cose dovrebbero essere anche nel mondo digitale. Questo è qualcosa che i legislatori hanno ottenuto soprattutto nel vecchio mondo analogico.

Quando qualcuno è su una telefonata - una vecchia telefonata analogica - sappiamo che la conversazione è privata per impostazione predefinita. Non importa chi è il proprietario del telefono. È la persona che usa il telefono, proprio in questo momento, che ha tutti i diritti sulle sue capacità di comunicazione, proprio in questo momento.

L'utente ha tutti i diritti d'uso. Il proprietario non ha il diritto di intercettare o interferire con l'utilizzo delle comunicazioni, solo in base al solo diritto di proprietà.

In altre parole: solo perché possiedi un apparecchio di comunicazione, ciò non ti dà alcun tipo di diritto automatico di ascoltare le conversazioni private di coloro a cui capita di imbattersi in questo apparecchio.

Purtroppo, questo vale solo per la rete telefonica. Inoltre, solo la parte analogica della rete telefonica. Se c'è qualcosa di digitale anche a distanza, il proprietario può fondamentalmente intercettare qualsiasi cosa che gli piaccia, per qualsiasi motivo.

Questo vale in particolare per il posto di lavoro. Si può sostenere che non ci si aspetta la privacy per quello che si fa sulle apparecchiature del proprio datore di lavoro; questo è proprio dimenticare che tale privacy era di primaria importanza per i POTS, meno di due decenni fa, indipendentemente da chi possedeva le apparecchiature.

Alcuni datori di lavoro installano persino certificati digitali con caratteri jolly sui loro computer sul posto di lavoro con lo scopo specifico di negare qualsiasi sicurezza end-to-end tra il computer del dipendente e il mondo esterno, eseguendo di fatto un cosiddetto "attacco man-in-the-middle". In un termine imbiancato, questa pratica si chiama Intercettazione HTTPS invece di "Man-in-the-middle attack" quando viene eseguita dal vostro datore di lavoro invece di un altro avversario.

Poiché stiamo esaminando la differenza tra analogico e digitale, e come i diritti alla privacy sono scomparsi nel passaggio al digitale, vale la pena di esaminare il codice di legge per la più antica delle corrispondenze analogiche: la lettera analogica, e se il vostro capo poteva aprirla e leggerla solo perché era indirizzato a voi sul posto di lavoro.

La legge analogica differisce leggermente da un paese all'altro su questo tema, ma in generale, anche se il tuo manager o il tuo datore di lavoro sono stati autorizzati ad *aprire* la tua posta (come è



il caso negli Stati Uniti ma non in Gran Bretagna), di solito non sono mai autorizzati a leggerla (anche negli Stati Uniti).

Al contrario, con la posta elettronica, i vostri manager non si limitano a leggere l'intera e-mail, ma in genere ha assunto un intero dipartimento per leggerla per loro. In Europa, questo è arrivato fino alla Corte Europea dei Diritti dell'Uomo, che ha stabilito che va benissimo per un datore di lavoro leggere la corrispondenza più privata, a patto che il datore di lavoro informi di questo fatto (negando così l'aspettativa di privacy).

Naturalmente, questo principio della posta elettronica un po' antiquata si applica ora a tutte le comunicazioni elettroniche, come Slack.

Quindi, per i nostri figli digitali, il concetto di "la posta è privata e vostra, indipendentemente dal fatto che la riceviate sul posto di lavoro" sembra essere stato irrevocabilmente perso. Questo era un concetto che i nostri genitori analogici davano per scontato, non vedevano la necessità di lottare per esso.

## 21. Conclusione, la privacy è stata quasi completamente eliminata dall'ambiente digitale

In una serie di post su questo blog, abbiamo mostrato come praticamente tutto ciò che i nostri genitori hanno dato per scontato in materia di privacy è stato completamente eliminato per i nostri figli, solo perché usano strumenti digitali invece che analogici, e le persone che interpretano le leggi dicono che la privacy si applica solo al vecchio ambiente analogico dei nostri genitori.

Una volta che si è d'accordo con l'osservazione che la privacy sembra semplicemente non valere per i nostri figli, solo per il fatto di vivere in un ambiente digitale invece di quello analogico dei nostri genitori, la sorpresa si trasforma in uno shock di rabbia, ed è facile voler attribuire la colpa a qualcuno per aver sostanzialmente cancellato la lotta per le libertà civili di cinque generazioni mentre la gente guardava dall'altra parte.

E allora di chi è la colpa?

È più di un attore al lavoro qui, ma parte della colpa deve essere attribuita all'illusione che nulla sia cambiato, solo perché i nostri figli digitali possono usare tecnologie antiquate e obsolete per ottenere i diritti che dovrebbero sempre avere per legge e costituzione, indipendentemente dal metodo che usano per parlare con gli amici ed esercitare i loro diritti alla privacy.

Tutti abbiamo sentito queste scuse.

"Avete ancora la privacy della corrispondenza, basta usare la vecchia lettera analogica". Come se lo facesse la generazione di Internet. Tanto vale dire ai nostri genitori analogici che dovrebbero inviare un telegramma via cavo per godere di alcuni diritti fondamentali.

"Puoi ancora usare una biblioteca liberamente". Beh, solo una biblioteca analogica, non digitale come The Pirate Bay, che si differenzia da una biblioteca analogica solo per efficienza, e non in qualsiasi altra cosa.

"Puoi ancora discutere di tutto quello che ti piace". Sì, ma solo nelle strade e piazze analogiche, non nelle strade e piazze digitali.

"Puoi ancora uscire con qualcuno senza che il governo conosca le tue preferenze di incontri". Solo se preferisco gli appuntamenti vecchia maniera, come hanno fatto i nostri genitori, nel mondo analogico "non sicuro"; perché in quello digitale "sicuro" i predatori scompaiono con un clic di un pulsante "blocco", un'opzione che i nostri genitori analogici non avevano nei loro bar.

Le leggi non sono diverse per l'analogico e il digitale. La legge non fa differenza tra analogico e digitale. Ma nessuna legge è al di sopra delle persone che la interpretano in tribunale, e il modo in cui le persone interpretano queste leggi significa che il diritto alla privacy si applica sempre al mondo analogico, ma mai al mondo digitale.

Non è una fantascienza pretendere che le stesse leggi si applichino offline e online. Questo include il diritto d'autore, così come il fatto che la privacy della corrispondenza ha la precedenza sul diritto d'autore (in altre parole, non è consentito aprire ed esaminare la corrispondenza privata per violazioni nel mondo analogico, non senza precedenti e singoli mandati - i nostri libri di legge sono pieni di questi controlli ed equilibri; dovrebbero applicarsi anche nel mondo digitale, ma non oggi non accade).

Tornando alla colpa, c'è un attore proprio lì: l'industria del copyright. Hanno sostenuto con successo che le loro leggi sul monopolio dovrebbero applicarsi online proprio come succede offline, e, così facendo, hanno completamente ignorato tutti i controlli e gli equilibri che si applicano alle leggi sul monopolio del copyright nel mondo analogico. E poiché la copia di film e musica si è spostata sugli stessi canali di comunicazione che utilizziamo per la corrispondenza privata, il monopolio del copyright in quanto tale è diventato fundamentalmente incompatibile con la corrispondenza privata a livello concettuale.

L'industria del diritto d'autore è stata consapevole di questo conflitto e ha continuato a spingere per l'erosione e l'eliminazione della privacy per sostenere i loro monopoli obsoleti e fatiscenti, come ad esempio l'odiata (e ora in tribunale) direttiva sulla conservazione dei dati in Europa. Userebbero questa legge federale (o un suo equivalente europeo) per ottenere letteralmente più poteri della polizia stessa nel perseguire singoli individui che semplicemente condividono musica e film, condividendo nel modo in cui tutti lo fanno.

Ci sono altri due fattori importanti al lavoro. Il secondo fattore è il marketing. La ragione per cui siamo rintracciati a livello inferiore a quello degli aeroporti e di altri centri commerciali affollati è semplicemente per venderci più merda di cui non abbiamo bisogno. Ciò avviene a scapito della privacy che i nostri genitori analogici hanno dato per scontata. Non iniziare nemmeno su Facebook e Google.

Ultimo ma non meno importante sono i falchi della sorveglianza - i politici che vogliono sembrare "Con gli occhi aperti sul crimine", o "con gli occhi aperti sul terrorismo", o qualunque sia la parola d'ordine questa settimana. Sono stati questi a spingere la direttiva sulla conservazione dei dati nella legge. L'industria del diritto d'autore è stata quella che l'ha scritta per loro.

Questi tre fattori hanno lavorato insieme e sono stati molto impegnati.

Sarà una lunga battaglia in salita per riconquistare le libertà che sono state lentamente conquistate dai nostri antenati per circa sei generazioni, e che sono state abolite in un decennio.

Non è scienza missilistica che i nostri figli dovrebbero avere almeno lo stesso insieme di libertà civili nel loro ambiente digitale, come i nostri genitori avevano nel loro ambiente analogico. Eppure, questo non sta accadendo.

I nostri figli hanno ragione a chiedere i diritti alla privacy equivalente analogico - le libertà civili che i nostri genitori non solo godevano, ma che davano per scontate.

Temo che il mancato trasferimento delle libertà civili dai nostri genitori ai nostri figli sarà visto come il più grande fallimento di questa particolare generazione attuale, indipendentemente da tutto

il bene che realizziamo. Le società di sorveglianza possono essere erette in soli dieci anni, ma possono impiegare secoli per ritirarsi.

La privacy rimane oggi una vostra responsabilità. Tutti noi dobbiamo riprenderla semplicemente esercitando il nostro diritto alla privacy, con tutti gli strumenti a nostra disposizione.