Liberi di navigare ma senza porti sicuri: perché il diritto soccombe alla tecnologia. Una proposta di inversione

Emilio Girino
Avvocato in Milano – Managing Partner, Studio Ghidini, Girino & Associati – Docente CUOA Finance – già Membro dell'Arbitro Bancario Finanziario (Collegio di Milano e Collegio di Coordinamento)

Franco Estrangeros
Avvocato in Milano – Partner, Studio Ghidini, Girino & Associati – già Membro dell'Arbitro Bancario Finanziario (Collegio di Milano e Collegio di Coordinamento)

Maurizio Bedarida
Ingegnere, Esperto in digital forensics e Cyber Security. Svolge attività di consulente per diverse Procure della Repubblica, tribunali, primari studi legali e aziende nei settori finanziario e manifatturiero

Il "mezzo di trasporto" più insicuro? Quello virtuale

Nessun mezzo di trasporto può ritenersi totalmente e assolutamente scevro da rischi, sia pur con diversi, sensibili gradienti di rischiosità. Eppure, da quando è entrata in auge la metafora della navigazione per plasticizzare il quotidiano ondeggiare fra i flutti di Internet, si è dovuto prender atto, con una graduale, indesiderata ed oggi pressoché soffocante accelerazione, che la rete è il peggior mezzo in fatto di sicurezza. Un paradosso in odor di nemesi perché la rete ha consegnato a chicchessia un senso di ubiquità, onnipresenza e onnipotenza che sembra aver generato un contrappasso eguale e contrario: i nostri corpi restano fermi, solo dita e occhi scorrono su sfreccianti tastiere o sensuali lamine di silicio, ma è l'intera nostra vita ad essere ogni giorno esposta, manipolata o commerciata per lo più a nostra totale insaputa. Può immaginarsi viaggio più insicuro?
Sennonché, negli ultimi due decenni[1] la natura, la dimensione e la percezione stessa del rischio di navigazione virtuale è radicalmente mutata, sino

[1] Per una più ampia ricostruzione storica si rinvia alla prima parte del par. 3.

ad invertirsi lungo un tracciato di progressiva incoscienza degli utenti. Dal debutto di Internet sin quasi alla fine degli anni Novanta, il pericolo della rete – l'unico in quello che ci sembrava un infinito Eldorado di libertà cognitiva e comunicativa – era identificato con l'attacco, consumato con l'ausilio di spyware, malware, trojan e altri programmi malevoli. Il pericolo coincideva dunque con l'aggressione terza, l'atto di violenza virtuale, quindi un illecito, sia pur difficilmente tratteggiabile, un guasto comunque scaturente da una fonte criminale o, in alternativa, da un morbo involontariamente contratto nell'indesiderato rapporto con untori dolosamente infettanti: e non a caso un altro prestito linguistico, stavolta mutuato dalla scienza medica, indicherà universalmente l'unico vero rischio che il navigare in rete avrebbe comportato: virus.

Dall'inizio degli anni Duemila l'espansione qualitativa e quantitativa della rete, la prepotente affermazione dei social network, l'esplosione del commercio elettronico, il progressivo e crescente dirottamento di servizi in senso lato sociali (assicurativi, bancari, sanitari, tributari, consulenziali) dalla localizzazione fisica alla delocalizzazione virtuale hanno determinato, singolarmente e nella loro interazione, un'esponenziale dilatazione del rischio di attacco ben maggiore di quella provocata dal virus tradizionale. Con tre non trascurabili varianti: in primo luogo, gli attacchi non provengono più soltanto da fonti criminali o da untori vogliosi di rapporti non protetti bensì dalle stesse più che legittime fonti che erogano il servizio; in secondo luogo, mentre è possibile (cercare di) proteggersi contro i virus, assai meno agevole è sottrarsi agli attacchi apparentemente innocui delle fonti lecite; in terzo, ultimo ma più sconcertante luogo, quelle aggressioni diventano discrete e invisibili, indolori e prive di sembiante dannoso, nei fatti tollerate o accettate, comunque non più percepite come un pericolo ma come una naturale evoluzione del sistema.

Restando ancora per qualche riga nei paraggi della cifra linguistica, impietoso ma fedele registro delle mutazioni del sentire collettivo, l'aggettivo virale nel contesto internettiano ha perso il suo connotato epidemico correlato alla sorgente infettiva, trasformandosi nel significante di una condizione positiva: se il video è virale, se la notizia è virale ciò significa che sta avendo enorme risonanza, si diffonde sì come un virus, ma come un virus buono e in qualche modo necessario. Il cambio di passo, rispetto al virus quale fonte di contaminazione o grimaldello banditesco, è eloquentemente illuminante.

Ma come avviene, in concreto, questa progressiva ablazione di dati, questa volpeggiante incetta di informazioni e la loro fitta messa in correlazione finalizzata al tracciamento delle vite individuali e al suo reimpiego per condizionarne le condotte?

Preoccupa, fino ai margini del brivido, quanto emerso da un recente articolo[2] che, nel riportare i risultati di un'indagine dell'agenzia danese Cybot, deputata alla sorveglianza statistica della sicurezza dei dati in rete, rivela come molti siti della Pubblica Amministrazione italiana (fra cui, ancor più inaspettatamente, il sito del Ministero delle Finanze) permettano a 54 compagnie che si occupano di pubblicità on line di ottenere dati dai cittadini che navigano le pagine e utilizzano i servizi dei siti istituzionali. Non per accordo né per dolo ma semplicemente per carenza di controllo. Ma ancor più preoccupa – e qui il brivido diventa agghiacciante –il fatto che la critica sia sostanzialmente nel senso dell'assenza di trasparenza, e non già nel senso della proibizione di tali circolazioni. Parliamo di siti pubblici che un cittadino spesso non può scegliere di schivare ma è anzi, per le più svariate ragioni (necessità di aggiornamento normativo, fruizione di servizi, acquisizione di dati statistici, richiesta o consultazione di pareri e via dicendo), costretto a navigare in lungo e in largo e magari neppure occasionalmente.
La faccenda parte da lontano. Coloro che oggi chiamiamo "signori della rete" nacquero come, o seppero incaricare, demiurghi e artieri tecnicamente scaltri e lungimiranti. Al di là delle poliformi denominazioni e declinazioni, il primo e tuttora più potente (ancorché non unico) tracciatore di dati resta il cookie. Chi inventò il nome non era un burlone ma un visionario. I cookie nacquero con la rete ma chi li concepì già sapeva che prima o poi almeno questi "netturbini-riciclatori" sarebbero caduti nell'occhio dei regolatori. La lungimiranza consistette nel dar loro un nome gradevole e apparentemente innocuo: "biscottino". Che poi fosse e sia lievemente avvelenato, a seconda della fraudolenza o della sbadataggine di chi lo sforni o se ne serva o sia costretto a servirsene, è altra faccenda. È da qui che muove la nostra analisi.

Le attuali regole della web-privacy in materia di tracciamenti e raccolta. La Direttiva e-Privacy e il GDPR

Durante la navigazione in Internet, i siti visitati installano automaticamente cookie, *tracker* e altri ammennicoli nel terminale dell'utente interessato. Non si tratta di una raccolta derivante dalla compilazione di *form*, dall'adesione a newsletter, dall'utilizzo di servizi "*voice*", cioè da condotte che implichino di per sé la sciente e volontaria comunicazione di dati personali al prestatore di servizi, ma di raccolta di dati personali da parte di terzi che interviene per il solo fatto che l'utente si colleghi e navighi in Internet.
Il GDPR non disciplina specificamente la fattispecie ma, al "considerando"

[2] Comparso sul magazine *Sette* del *Corriere della Sera,* 24.5.2019, p. 72 ss.

n. 30, si limita a riconoscere che attraverso gli indirizzi IP e l'acquisizione di identificativi univoci sarebbe possibile risalire alla persona fisica che sia operativa on line monitorandola nei comportamenti e, quindi, profilarla [3]. La fattispecie trova invece disciplina nella norma della Direttiva 12 luglio 2002 n. 2002/58/CE "*relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche*" (in seguito Direttiva e-Privacy). Trattando specificamente il settore delle comunicazioni elettroniche e disciplinando la materia dei cookie, tale disciplina è da considerarsi norma speciale rispetto al GDPR (norma generale) e quindi non superata dalla pubblicazione di quest'ultimo[4]. D'altra parte è l'art. 95 del GDPR ad espressamente precisare che il medesimo non impone obblighi supplementari per quanto riguarda le materie che sono soggette a obblighi specifici fissati dalla Direttiva e-Privacy, mentre il considerando 173 del regolamento conferma l'applicabilità del GDPR a tutti gli aspetti che non rientrano in obblighi specifici di tale direttiva.

A ciò consegue l'immutata sopravvivenza, a tutt'oggi, dell'art. 122 del D.Lgs. 196/2003, che attua in Italia la disciplina promanante dalla Direttiva e-Privacy. L'articolo (i) legittima l'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate subordinandola alla prestazione del consenso dell'interessato; (ii) legittima l'archiviazione tecnica o l'accesso a tali informazioni, senza la prestazione del consenso, qualora ciò sia esclusivamente funzionale all'erogazione del servizio; (iii) legittima l'utilizzo di informative semplificate e di programmi informatici o di dispositivi per raccogliere l'espressione del

[3] Quantunque la profilazione spesso possa rivelarsi anche clamorosamente errata: chi visiti frequentemente il sito di un partito politico, di un'associazione cinofila o di un negozio on line di frutta e ortaggi, non necessariamente è un accolito di quel partito, un appassionato di cani o un convinto vegano; a ciò s'aggiunge il fattore della cosiddetta barriera tecnologica: il cookie sa quale dispositivo ha visitato quel determinato sito ma ignora l'individuo corrispondente al visitatore, come regolarmente accade per i computer domestici che non di rado vengono utilizzati da diversi membri di una stessa famiglia o dal personale al servizio della stessa. Il fenomeno oggi tende ad attutirsi in considerazione dello spadroneggiare di smartphone e tablet dove transita circa il 70% del traffico in rete e l'uso promiscuo dei quali è decisamente molto ridotto. Tuttavia questo è un rischio marginale per gli scopi dei produttori di biscottini. Questi rovistano nelle spazzature dei terminali (da qui la qualifica di "netturbini" di cui sopra) e la probabilità di centrare il bersaglio diminuisce ma non s'annulla se si frughi nel bidone condominiale invece che nella pattumiera della cucina: si può comunque colpire in un mucchio mirato.

[4] In tal senso si è altresì di recente espresso lo *European Data Protection Board* (il nuovo Comitato europeo per la protezione dei dati che, alla luce del GDPR, esprime un potere di indirizzo senz'altro pregnante anche sul legislatore dell'Unione Europea in materia di privacy) con il Parere del 13 marzo 2019 sulla "Interazione tra la direttiva ePrivacy e il Regolamento generale sulla protezione dei dati".

consenso sopra menzionato. Permangono altresì le comunicazioni e le disposizioni regolamentari emanate dal Garante Privacy italiano in esecuzione alla norma sopra richiamata[5].

Tuttavia, la disciplina di cui alla Direttiva e-Privacy e, di conseguenza, quella nazionale dalla medesima promanante, non può, proprio in virtù del rapporto di specialità fra i due corpi normativi, spingersi a regolamentare compiutamente i trattamenti di dati eseguiti per il tramite dei cookie. Mentre cioè l'installazione dei cookie sconta le regole della disciplina speciale, i trattamenti che i titolari eseguono sui dati personali di terzi acquisiti tramite l'installazione dei cookie sono soggetti alla disciplina generale (GDPR).

Per scaricare dunque i cookie nei terminali occorre sempre l'informativa ed il consenso informato e frazionabile dell'interessato per i cookie di profilazione (come previsto dalla disciplina speciale). Occorre l'informativa e la esplicitazione del presupposto di legittimazione del trattamento (come previsto dalla disciplina generale, cioè dal GDPR) per l'esecuzione dei trattamenti sui dati personali acquisiti mediante cookie. In relazione a quest'ultimo stadio va rimarcato come il presupposto possa essere diverso dall'esplicitazione del consenso dell'interessato potendosi il titolare del trattamento avvalere del "legittimo interesse" di cui all'art. 6 del Regolamento [6].

Nella sostanza, la disciplina informativa/autorizzativa dell'utilizzo dei cookie (del loro scaricamento nei terminali degli utenti) è racchiusa nel seguente passaggio del Provvedimento: "*Nel momento in cui l'utente accede a un sito web, deve essergli presentata una prima informativa "breve", contenuta in un banner a comparsa immediata sulla home page (o all'altra pagina tramite il quale l'utente può accedere al sito), integrata da una informativa "estesa" alla quale si accede attraverso un link cliccabile dall'utente. Affinché la semplificazione sia effettiva, si ritiene necessario che la richiesta di consenso all'uso dei cookie sia inserita proprio nel banner contenente l'informativa breve. Gli utenti che desiderano avere maggiori e più dettagliate informazioni e diffe-*

[5] Cfr. Provvedimento del Garante per la Protezione de Dati Personali dell'8 maggio 2014 "*Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookies*." (di seguito, il Provvedimento).

[6] Al riguardo cfr. E. Girino, F. Estrangeros, *Alla ricerca dei dati perduti,* in questa *Rivista*, n. 1, maggio 2019, par. 6. Ovviamente non vengono in discussione i cookie cc.dd. tecnici, quelli cioè che consentono il corretto funzionamento del sito e, di conseguenza, la corretta navigazione da parte dell'utente, bensì i cookie di profilazione, che spiano gusti e orientamenti dell'utente attraverso le tracce delle visite. Benché la disciplina imponga di enunciare specificamente le funzionalità dei differenti cookie, non sempre nelle informative il distinguo è chiarissimo mentre non di rado ci s'imbatte in messaggi intrasparenti che "avvertono" l'utente che il rifiuto dei cookie, senza specificare quali, potrebbe compromettere il funzionamento del sito. Intrasparenza che la regola del piccolo banner sbrigativo esalta e, paradossalmente, finisce con il "legalizzare".

renziare le proprie scelte in merito ai diversi cookie archiviati tramite il sito visitato, possono accedere ad altre pagine del sito, contenenti, oltre al testo dell'informativa estesa, la possibilità di esprimere scelte più specifiche" (cfr. par. 4 del Provvedimento). La disciplina che invece inerisce il trattamento di dati personali di terzi acquisiti tramite i cookie è da ricercarsi nel GDPR. Tale impianto ha partorito veri e propri "mostri para-informativi".

Da un lato, ogni sito web che utilizzi cookie tecnici e/o di profilazione deve avvisare l'utente e dargli la possibilità di visionare la versione completa dell'informativa e di autorizzare per ogni categoria di cookie la relativa registrazione sul proprio terminale. Dall'altro deve prevedere l'informativa riferita ai trattamenti eseguiti su tali dati personali specificando i presupposti di legittimazione di ciascun trattamento ed, eventualmente, richiedendo la relativa espressione del consenso esplicito. Tutto ciò, che appare normativamente logico e concettualmente ineccepibile rispetto al principio del "consenso informato" che caratterizza la disciplina *privacy*, lascia alquanto perplessi circa la sua effettività.

Da semplici utenti ci siamo messi alla prova: ci siamo impegnati a visitare 3 siti web, uno di e-commerce per l'acquisto di una applique per la camera da letto, un altro di informazione giornalistica per l'aggiornamento sulle ultime notizie del nuovo governo (mentre scriviamo siamo a settembre 2019), un terzo di un operatore di telecomunicazione per valutare l'offerta per la visione di partite della prossima Champions League. Tempo stimato (e disponibile) per scelte e valutazioni: 30 minuti. La prova ci imponeva però di non sottovalutare la tematica cookie, aderendo *sic et simpliciter* alla policy proposta dal titolare del sito web visitato (cliccando "accetto" nel banner semplificato che compare accedendo al sito), ma di esaminare diligentemente l'informativa estesa e procedere, là dove disponibile, ad accettare le categorie di cookie effettivamente necessarie per l'esecuzione delle operazioni previste e prestare selettivamente i consensi.

La prova ha avuto inizio ad una cert'ora di un certo giorno. Dopo i fatidici 30 minuti stimati, ahinoi, eravamo ancora sul primo sito, faticosamente avanzavamo nella lettura della policy senza pienamente comprendere cosa e come avremmo potuto escludere dai nostri consensi. Era passata mezz'ora e la applique non solo non era stata acquistata, ma neppure eravamo arrivati ad una prima selezione di possibili candidate. Insomma, dopo mezz'ora eravamo ancora fermi alle premesse dell'informativa estesa.

Il banco di prova è, giocoforza, esteso a tutti gli utenti Internet che giornalmente accettano, senza cura, le privacy policy degli editori dei siti web visitati. Quanti e quali, fra gli utenti medi della rete, hanno tempo, voglia, pazienza e capacità di leggere, discernere, scegliere? Non esistono – o almeno

non sono disponibili – statistiche ufficiali e attendibili, ma crediamo di non essere distanti dal vero se azzardassimo una percentuale, se non infinitesimale, certamente minima e comunque irrilevante rispetto al disegno di tracciamento su cui s'adagia il *monstre* normativo [7].

E non è tutto, perché, i biscottini trovano un eccellente companatico in molti altri strumenti di tracciamento. Tenteremo una sintetica ricostruzione e per facilitarne la lettura proponiamo un piccolo glossario[8]. Ci si avvedrà di come, al di là delle varianti morfologiche o funzionali, il circuito delle appropriazioni abbia un'empatia coi rosari: aprirsi, sgranarsi, agganciare un grano all'altro per infine tornare, sempre e inevitabilmente, al punto di partenza.

Gli incontri possibili, palesi e segreti, comuni e sporadici, nella navigazione

La materia è marcatamente complessa, non solo per ragioni tecniche, ma anche perché siamo nel pieno di una trasmutazione tecnologica che si celebra su scenari prima sconosciuti. L'avvento del web oltre che accrescere esponenzialmente le potenzialità di raccolta dei dati rende possibile una interazione immediata o quasi immediata con l'utente/consumatore. Interazione che comporta un fenomeno di mutuo condizionamento. I moderni algoritmi sono in grado di automodificarsi in base ai dati che raccolgono per meglio "profilare" i propri target. I nostri stili di vita e finanche i nostri desideri e pensieri sono modificati o comunque condizionati da ciò che il web ci propone o propina.

[7] Cfr. nello stesso l'editoriale di G. Arnò *Ti informo di averti informato,* in questa *Rivista*, n. 2/19.

[8] Nella trattazione si incontreranno alcuni termini tecnici, di alcuni verrà data una spiegazione quando saranno citati, altri "più comuni" sono definiti nel seguito:

- Web Browser: applicazione presente sui *device* che permette la navigazione in internet o meglio la lettura delle pagine presenti sui siti Web;
- Sito Web: aggregazione di contenuti (testi, audio, video, link) secondo un linguaggio (nascosto all'utente) interpretabile dai web browser;
- Web Server: macchina/e (virtuali/fisiche) che ospitano i web server;
- Applicazioni Web: applicazioni usufruibili attraverso un Web Browser;
- Applicazioni: le applicazioni che sono eseguite con un calcolatore o personal computer/portatile;
- Sistema Operativo: funzionalità di base di un dispositivo (PC/*Tablet* Smart Phone) che permettono di eseguire le applicazioni e l'interazione con l'utente;
- App: applicazioni che si scaricano dai negozi virtuali correlati ai diversi sistemi operativi. Sviluppatori di *software house* diverse o operatori di servizi vari creano le App e le pubblicano sui diversi Store (Apple Store, Google Play) dove possono essere acquistate o scaricate liberamente a seconda del modello di business del creatore della App;
- Store: le uniche applicazioni presenti sui *device* mobili (ma ormai anche sui PC) mediante le quali l'utente può comprare e/o scaricare software.

Giova un breve excursus storico dell'evoluzione tecnologica manifestatasi in uno spazio temporale relativamente contenuto.
All'inizio dell'era del Web la problematica maggiore era la connettività ed il possesso di apparati idonei (PC) per il grande pubblico. Da un ambito prettamente universitario/professionale il sistema si stava aprendo ai mercati, nascevano i primi motori di ricerca. Da metà degli anni 90 ai primi anni del XXI secolo il problema del digital divide era nei programmi dei governi mondiali. Il digital divide va inteso in una doppia accezione: la prima attiene all'impossibilità per alcune fasce di popolazione di poter accedere alle tecnologie abilitanti alla fruizione dei servizi della Rete (PC e connettività), la seconda attiene alle conoscenze necessarie per poter avvalersene. Dagli inizi del 2000 e per tutto il primo decennio si assiste ad una sempre più capillare diffusione dei PC e alla caduta verticale dei costi di connessione, si comincia a percepire le potenzialità dei motori di ricerca (anche ai fini della profilazione), nascono i primi programmi per convogliare contenuti pubblicitari non voluti durante la consultazione delle pagine Web (Adwarwe). Il primo "salto quantico" si realizzò attraverso un singolare ma micidiale "combinato disposto" tecnologico: l'immissione sul mercato dei primi smartphone e la possibilità di avere connettività dati su tali dispositivi mobili, cui seguirà poco dopo "l'invenzione"(diverrà chiara fra breve la virgolettatura) del cloud. A questo stadio la prima accezione del digital divide scade in secondo piano mentre diventa preponderante e attualissima la seconda (la conoscenza per un uso consapevole di tali strumenti). Ad oggi siamo ancora nel pieno di questo salto.
La premessa si completa richiamando un concetto che si riallaccia alla nozione di cloud, ossia le cosiddette IOT (Internet of Things). Il segreto delle IOT è di portare le tecnologie del cloud sugli oggetti di uso comune: domotica e elettrodomestici, sistemi di allarme, strumenti elettromedicali, orologi etc. Non occorre una profonda conoscenza tecnica per capire la quantità di informazioni ricavabili da questi "oggetti" che ancora scivolano fra i meandri di una normativa spiazzata dalla loro roboante entrata nella quotidianità.
Sempre per gusto metaforico, il cloud non è una indefinita nuvola che sta in un cielo artificiale lontano ma raggiungibile, noi siamo immersi nel cloud, come attraversare una nuvola bassa in montagna dove l'acqua vaporizzata ci circonda ma ci permette di vedere le sagome di chi cose e persone "vicino" a noi ed in un certo senso a loro ci connette.

I cookie

I capostipiti sono tracciatori subdoli (salvo quanto rammentato alla nota 6). Di per sé, l'installazione di un cookie sul terminale (dopo la pressione del

tasto "Accetto") non comporta un ulteriore "avviso" automatico all'utente nel momento in cui essa ha materialmente luogo. Si tratta di un registratore che si attiva silenziosamente e intelligentemente, capace di autonomamente valutare e catalogare i comportamenti del soggetto monitorato. Pensate a un registratore che, potenzialmente, una volta attivato potrebbe funzionare fino al suo deperimento, senza conoscere il tasto "off".

I cookie sono stringhe di byte (caratteri) di piccole dimensioni (dei file) che i siti visitati dall'utente inviano al suo dispositivo (in genere attraverso il browser del dispositivo stesso). Tali file vengono memorizzati sui dispositivi in specifiche posizioni per poter essere poi letti o dagli stessi siti visitati successivamente o anche da siti di terzi abilitati o in grado di leggere tali file. Durante la navigazione di un sito, l'utente può ricevere anche cookie da siti diversi (di terze parti ma in qualche modo collegati alla pagina che si sta visitando). Nei cookie possono essere salvate informazioni di vario genere (dati personali, coordinate di posizionamento, link, dati di sessione, etc.) presenti sul browser/sito o sul dispositivo utilizzato.

Le attività di navigazione producono centinaia di cookie diversi. Possono essere crittografati o non intellegibili o contenere del testo intellegibile [9].

Quali degni capostipiti della progenie dei predatori di dati perduti, i biscottini hanno un'altra virtù: sono vendicativi. Spendendo qualche ora per (forse) neutralizzarli, essi potrebbero indispettirsi e precluderci una navigazione completa del sito. Incarnano il sogno del guidatore anarchico: tutor e autovelox non si rispettano né si violano. Basta eluderli.

I banner

Fra le prime e ancora più diffuse forme di pubblicità i banner consistono in strisce dinamiche o immagini che compaiono nella pagina web che l'utente sta visitando. Generalmente il contenuto del banner è frutto delle informazioni di profilazione fatte sull'utente. A tutti è capitato di fare un acquisto su un dato sito e trovarsi per un certo lasso di tempo informazioni pubblicitarie del prodotto acquistato o affini su pagine che (apparentemente) nulla abbiano a che vedere con l'acquisto fatto o il negozio elettronico utilizzato. Ad esempio, si acquista un trapano online e per un certo periodo compaiono, sul sito del giornale online che si è usi consultare, articoli di ferramenteria.

[9] Un cookie, si è detto, è un file contenente delle stringe di byte ossia anche del testo. Un utente capace può aprire questi file con normale editor di testo (es. *Notepad*) e tentare di acquisirne il contenuto. Generalmente i cookie tecnici che contengono informazioni utili per accedere a pagine ad accesso riservato sono cifrati. Di contro se il sito che crea il cookie non vuole far capire le informazioni che raccoglie attraverso questo meccanismo, può cifrare o rendere non intellegibile il contenuto degli stessi.

I banner possono essere anche utilizzati per notificare all'utente qualcosa, possono essere utilizzati ad esempio per far consultare le regole sulla privacy adottate dal sito stesso.
Software (non sempre ma spesso) malevoli, i banner sono veri e propri spazi pubblicitari generalmente gestiti da terzi rispetto al proprietario e/o gestore del sito che si sta visitando. Un click su un banner può comportare (e ci risiamo) la scrittura di cookie di profilazione e/o l'acquisizione di informazioni sull'utente.

I Pop-up

I pop-up sono elementi utilizzati dai Web Server (ed anche da alcune applicazioni) che compaiono automaticamente in forma di riquadri o finestrelle. Lo scopo originario dei pop-up era benigno: mirava a separare la pubblicità dalla pagina web che si stava visitando. In seguito la tecnologia è stata utilizzata per fornire ulteriori informazioni agli utenti, anche di ausilio (help online), per raccogliere dati dell'utente senza cambiare la pagina di navigazione, per inviare notifiche non richieste. L'uso piuttosto invasivo dei pop-up dal punto di vista sia della frequenza sia dell'occupazione dello spazio della pagina Web non ha mancato di ulteriormente degenerare: i pop-up possono tramutarsi in vettori di attacchi ai dispositivi degli utenti (al pari dei banner pubblicitari).

Programmi o App che raccolgono dati in modo più o meno occulto. I Trojan

Oltre ai cookie, scaricati nei terminali degli utenti che navigano on line, PC e smartphone subiscono l'aggressione di codici che raccolgono dati immessi dall'utente trasferendoli a terzi. La tecnica ha origini remote e si basa sull'inserimento all'interno di applicazioni con apparente scopo utile e/o innocuo d'un codice a tutt'altro proteso. Nel mondo dei PC si tratta di software classificato come *Trojan Horse* (a ricordo del mitologico, ligneo cavallo guidato da Neottolemo), nel mondo dei *device* mobili non v'è ancora una definizione così precisa. Ma l'insidia non varia: il più benevola forza pubblicità non volute, il più perfido inocula virus. Nel mondo del *mobile* possono essere utilizzati per carpire agevolmente informazioni personali in maniera più puntuale (a volte per accorgersene basta scrutare le autorizzazioni che chiedono: può senz'altro destare sospetti una applicazione finalizzata ad utilizzare la luce led del *device* come torcia che chiede l'autorizzazione per accedere ai contatti personali e alle foto).
A differenza dei Pc, dove si deve prestare attenzione ai siti da dove si scaricano *software*, nel mondo del *mobile* le App vengono prelevate dagli Store: uniche

location abilitate a scaricare software. Senza volersi far censori degli altrui vizi, per quanto esistano protocolli di controllo per pubblicare le App nei vari Store, è un dato di fatto che molte App adottino tecniche per eludere le sorveglianze. Il controllo da parte dei gestori dello Store è continuo e spesso le App vengono rimosse perché non conformi alle politiche di sicurezza e di privacy imposte dallo Store medesimo.
È ormai qualche anno che anche sui Pc il software è scaricabile attraverso gli Store di riferimento. La politica non è così vincolante sui Pc come invece lo è sugli apparati mobili. Ma anche sui Pc le interazioni tra le diverse applicazioni per ottenere i dati dell'utente (pur chiedendo il consenso – si è dianzi notato a quale prezzo) stanno guadagnando terreno.

Altre "occasioni" di raccolta

I cookie hanno altri alleati. Sempre più i siti *web*, i motori di ricerca, le applicazioni e i programmi chiedono all'utente di poter inviare informazioni, in gergo "notifiche". Spesso è l'utente stesso che abilita la richiesta di notifica: ad esempio, per tenersi aggiornati su un certo argomento si richiede al motore di ricerca di notificare (di norma via mail) la presenza sul web di novità circa l'argomento d'interesse. Il veicolo "Notifiche" è una sorta di pop-up gestito dal browser o da alcune app attraverso le nuove funzionalità del sistema operativo. La notifica non solo può veicolare messaggi pubblicitari non richiesti ma ben può raccogliere dati sulle nostre preferenze. L'impostazione su un browser di ricerca che attiva la segnalazione di novità su argomenti che l'utente ha richiesto permette chiaramente una più puntuale profilazione dell'utente stesso [10].
Nei gironi infernali del peregrinare in rete ci si imbatte nei Blog: chiusi, ovverosia limitati ad un gruppo di utenti ristretto a cui si può partecipare solo su (blanda) cooptazione, o aperti, dove una semplice registrazione con un profilo falso è sufficiente. I dati acquisiti da tali piattaforme (spesso di non facile localizzazione) vengono rivenduti a società di ricerca e possono essere anche utilizzati per azioni di marketing mirato. Anche l'eventuale falsa identità spesa iscrivendosi al blog (l'avatar) non salva. A sbugiardare l'ingenuo tentativo intervengono sentinelle algoritmiche, simili alle multitentacolari piovre di Matrix, in grado di individuare interventi di uno stesso soggetto (specie se particolarmente attivo) in base allo stile di scrittura, alla

[10] Pensiamo alle applicazioni di "cerco casa". Da una parte il servizio è comodo perché permette di proporci in tempo quasi reale opportunità di acquisto/affitto secondo i parametri che abbiamo immesso risparmiando all'utente la perdita di tempo nel fare ricerche manuali, di contro vengono salvate informazioni circa il nostro budget e lo stile di vita che conduciamo (la scelta di particolari zone della città contribuiscono a indicare il tenore di vita dell'utente).

struttura grammaticale ed ai costrutti semantici che utilizza e di correlare queste informazioni con altre presenti nel web pervenendo ad identificare il possessore di uno o più avatar con differenti gradi d'approssimazione quando non di certezza.

Che dire degli intoccabili social network, nati per permettere a quante più persone possibile di interagire, scambiarsi dati, foto, lodi, insulti, auspici di disgrazia e altro (ivi inclusa l'organizzazione di atti terroristici)? Nelle prime versioni di Facebook, per esempio, l'adesione al servizio comportava la cessione dei dati che vi si immettevano. Al di là delle considerazioni più immediate su stolidi eccessi di fiducia e configurazioni errate che possono diffondere sul web informazioni personali, due i tratti rilevanti ai nostri fini. Primo: Cina a parte, la maggior parte di questi strumenti sono gestiti da un numero esiguo di società: *multa paucis*, recita il motto d'un celebre editore giuridico. Con la differenza che qui non si discute dell'ampiezza culturale riservata ai pochi che l'apprezzino, bensì dell'oligopolio mondiale dei dati. Secondo: i dati degli utenti, residenti su questi database, aggregati in varie forme o meno sono in vendita e costituiscono uno dei maggiori *core business* di queste società. Se un mercante ci regala qualcosa, il prezzo siamo noi.

La quantità di informazioni ricavabili da queste basi dati è impressionante e, insieme al *cloud* ed oggi anche all'*Internet of Things*, costituiscono uno dei più robusti strumenti di raccolta massiva per le bramose canne dei cosiddetti Big Data.

Dulcis in fundo, *cloud* e *Internet of Things*. Il primo è un luogo virtuale dove vengono memorizzate (più o meno trasparentemente) tutte le informazioni che ci riguardano ricavabili dalle fonti ormai note. Basti pensare ai servizi *cloud* gratuiti per caricare o trasferire dati voluminosi o salvare backup del telefono, delle chat, dei contatti, degli SMS, o di quant'altro. Il *cloud* inoltre offre i servizi di connessione che permettono di condividere le informazioni personali tra gruppi di persone, di interagire con gli IOT, di ritrovare le proprie preferenze di navigazione e altro su tutti i *device* collegati ad un nostro profilo che per l'appunto è memorizzato nella nuvola. Lo stesso accade, ad esempio, per le applicazioni gratuite di spostamento reale: è grazie al *cloud* che tali strumenti, "geolocalizzandoci", ci dicono in base alla posizione ed il tragitto se ci sono code, lavori, incidenti sul nostro percorso, ci consigliano soste in locali magari profilati mediante altre applicazioni da dove estraggono le nostre propensioni culinarie. *L'Internet of Things* è una altrettanto lata nozione che accomuna tutti quei dispositivi, d'uso comune, controllabili attraverso la rete o più tipicamente una App. Nella famiglia degli IOT rientrano gli apparati di domotica comprensivi di elettrodomestici, alcuni tipi di sistema di allarme per la casa, per l'auto o la moto, gli *smartwatch*, gli strumenti

elettromedicali, le smartTV. Sia il *cloud* che gli IOT consentono l'acquisizione e la conservazione dei dati legati ai profili (foto, contatti, documenti, etc.), che diventano dei comodissimi punti unici di raccolta di informazioni che prima potevano essere sparsi su dispositivi diversi. Sono l'espressione più nitida del fenomeno di "dispersione concentrativa" che caratterizza l'uso, anche non smodato, delle nuove opportunità di connessione[11].

Le contromisure tecniche

Esistono rimedi tecnici per aiutarci a consapevolmente disporre dei nostri dati? Se l'evoluzione tecnologica ha portato ad introdurre sempre più sofisticati algoritmi e sistemi di captazione dei dati personali, equivalente (o quasi) evoluzione si è avuta anche dal punto di vista dei presidi a salvaguardia della sicurezza e della privacy. Gli stessi costruttori di dispositivi e di sistemi applicativi, ad ogni versione, inseriscono nuove possibilità di personalizzazione del sistema volte a preservare dati e privacy. Tutto ciò, tuttavia, a scapito della semplicità di configurazione e di fruizione dei servizi.

Gli antivirus

Li conosciamo da tempo. Nascono poco dopo la nascita del PC e li abbiamo sempre creduti il più potente antidoto contro i virus. Di base il loro funzionamento non è diverso a seconda che li si installi su un PC e uno smartphone ma ci sono delle differenze che impongono delle riflessioni. Ormai potenza di calcolo e memoria non costituiscono più un problema per un antivirus per smartphone o tablet. Ciò che incide è il consumo di risorse e quindi di batteria. Smartphone di fascia medio bassa, pur essendo esposti agli stessi pericoli, non sono in grado di supportare alcuni antivirus perché il loro utilizzo comporterebbe un consumo eccessivo della batteria. In commercio cominciano ad esserci antivirus che lavorano in background e che svolgono le analisi più impegnative sul *device* quando il dispositivo è connesso alla rete elettrica. Altro requisito indispensabile, per un efficace utilizzo del software, è la presenza di connettività che assicuri il costante aggiornamento dei programmi.
Gli antivirus possono presidiare la navigazione in Internet ma anche questa attività consuma risorse. Sono in commercio antivirus che controllano in tempo reale un determinato indirizzo con una banca dati on line per verificare se esso sia nella *black list* dei siti potenzialmente dannosi. Questa metodologia, pur aumentando il traffico di rete, diminuisce la potenza di

[11] Sul punto cfr. ancora E. Girino, F. Estrangeros, *Alla ricerca dei dati perduti*, *cit.*, par. 8

calcolo richiesta. Le pagine segnalate sono come tali comunicate all'utente che decide come proseguire. Altro compito di questi "antivirus portatili" è verificare che le App non contengano codici per forzare banner o notifiche pubblicitarie non volute.
Un'ultima funzionalità da menzionare è quella che ricade sotto il nome di *Early Warning*: si tratta del monitoraggio di varie vulnerabilità scoperte dagli hacker e non ancora pubblicate, indicando le contromisure da adottare, ovvero la evidenziazione di *data-breach* non ancora formalmente noti, in modo che l'utente provveda a prendere le contromisure del caso (es. cambio delle password).

Sistemi per preservare l'anonimato della navigazione

Tutti i browser, smartphone e tablet inclusi, permettono ormai di impostare la navigazione in formato "anonimo". La navigazione anonima è idonea a proteggere dai cookie e dalle informazioni fornite dai browser, ma non preserva dalla rilevazione del IP pubblico che si sta usando per la navigazione. Un *bug* di non secondario rilievo posto che l'IP pubblico permette di associare alle attività di navigazione il provider telefonico che si sta utilizzando e risalire all'utente autore di una navigazione anonima, anche utilizzando algoritmi specifici di raffronto. Il settaggio in formato "anonimo" della navigazione può essere abbinato all'utilizzo di un "*proxy* di anonimizzazione", cioè di un servizio che incanala la navigazione dell'utente mascherando il reale indirizzo IP con IP di vari paesi sparsi nel mondo. Sono utilizzati per evitare il tracciamento dell'IP del proprio provider telefonico e unitamente alla navigazione anonima possono preservare da alcune forme di profilazione. Esistono App che permettono di utilizzare questi proxy di anonimizzazione anche da smartphone e tablet (quelli gratuiti in genere rallentano molto la velocità di navigazione, quelli a pagamento garantiscono, in genere, una buona velocità).

Junk mailbox

È un vecchio trucco utilizzato per evitare pubblicità moleste e spam. Il metodo è semplice e senza costi. Si crea una casella free su un qualsiasi provider con un nome di fantasia ed un avatar (i dati reali possono o devono essere inseriti nel profilo, ma ci sono servizi, specialmente non europei, che non prevedono il riconoscimento dell'utente effettivo della casella). Alla richiesta di informazioni tramite form si possono utilizzare i dati della Junkmail evitando profilazioni puntuali. Occorre tuttavia non incrociare mai le informazioni della Junk mail con informazioni reali (i motori dei Big Data potrebbero correlare e attribuire all'utente vero la casella di junk mail).

Sistemi di blocco pubblicitario

Ne esistono svariati, con differenti opzioni non complicatissime da adottare. Il loro funzionamento è piuttosto soddisfacente perché paralizzano la più parte delle pubblicità e dei banner, quindi riducono il "fastidio di navigazione" e allontanano dalla tentazione di cliccare su finestre sconosciute. Il loro limite è duplice: per un verso non impediscono la profilazione da navigazione, per altro verso rendono impossibile l'accesso a taluni siti che sbarrano l'ingresso rilevando la presenza del blocco e richiedendone la disattivazione. Se l'utente può rinunciare al sito bene, ma se non può è costretto ad aprire l'uscio rimuovendo la protezione.

Limiti dei rimedi tecnici

L'intramontato paradigma della sicurezza è che il punto più debole nella catena di protezione non è la tecnologia ma il fattore umano: verità che smartphone e tablet confermano in modo granitico. I *device* portatili sono spesso i più vulnerabili e i più negletti. Gli utenti non hanno ancora realizzato che quello che portano in tasca o in borsa non è un telefono ma un computer: paradossalmente molti proteggono con costosi e aggiornatissimi antivirus i loro pc fissi ma eguale accortezza non viene dispiegata per gli smartphone. Tre le ragioni di questo bipolarismo d'autoprotezione.

La prima è la convinzione (molto ingenua per non dire sciocca) che il pc fisso sia più difficilmente proteggibile perché si deve spesso lasciarlo incustodito, mentre lo smartphone ci accompagna persino in toilette. Niente di più falso e di più tristemente comico.

La seconda corrisponde alle oggettive difficoltà di configurare gli apparati (il vecchio *plug & play* è una specie orami estinta) che finiscono con il frustrare l'utente e spazientirlo.

Ma la terza ragione è che, fissi o mobili, i device non possono essere autenticamente immunizzati attraverso le contromisure descritte. Le quali, oltre ad essere, come si è notato, assai imperfette, non semplici da attuare e talora ai limiti della legalità (v. junkmail false o mascheramenti degli IP dirottati), possono forse e parzialmente proteggere contro gli attacchi apertamente malevoli (virus) ma non anche contro l'apparentemente innocuo prelievo di dati ai quali, più o meno involontariamente, l'utente si espone o è nei fatti costretto a esporsi. Possiamo decidere, con ormai grande scomodità, di rinunciare alla domotica o ai mezzi a comando vocale, più difficile è evitare l'uso del satellitare in auto (il cui segnale continua a tracciarci anche se non impostiamo un percorso), impossibile non navigare nei siti web, sia pur solo ad uno stretto fine professionale (quantunque ormai anche la nostra quotidiana esistenza extralavorativa non possa prescinderne per scegliere una

vacanza o un regalo o più semplicemente per leggere notiziari, quotazioni di titoli o previsioni meteo in tempo reale).

Il fallimento attuale della tutela della riservatezza in ordine alla navigazione on line. La (debole) speranza del nuovo Regolamento e-Privacy

Ricapitolando, i cookie sono onnipresenti e invasivi, i banner contengono a loro volta cookie di profilazione, i pop-up eseguono tracciamenti similari, alcune App, pur soggette a rigorosi protocolli, sono non raramente provviste di congegni volti ad eluderli, gli IOT tracciano per definizione con il consenso implicito dell'utente che se ne serva, il *cloud* raccoglie dati nelle forme più disparate e finanche senza specifico acquisto del servizio, le contromisure sono difficili da impiegare, spesso risultano inefficienti, talora comportano accorgimenti non propriamente banali e ai limiti del legale. Già, la legge, a fronte di tutto questo, che fa?

L'analisi del quadro normativo e fattuale della protezione della riservatezza in rete restituisce un risultato sconfortante.

La normativa di riferimento, anche in questo ambito (cookie, loro derivati e affini), applica, come si è detto, il principio generale del "consenso informato". Sostanzialmente obbliga gli editori di siti alla pubblicazione di pagine di informazioni sui cookie medesimi, consentendo quindi agli utenti di selezionare le tipologie di cookie di cui si accetta l'installazione ed i trattamenti sui dati così raccolti. Tuttavia il sistema così creato non raggiunge in realtà alcuno degli obbiettivi di protezione effettiva delle informazioni degli utenti (e della loro privacy). In pochi secondi di navigazione l'utente medio di Internet accede a una pletora di siti web suggeriti dal motore di ricerca o da link potenzialmente infiniti, peggio delle vecchie e, al confronto, patetiche "catene di Sant'Antonio". L'utente non è disponibile a utilizzare il proprio tempo su Internet per porre in essere una interminabile serie di atti preparatori rispetto al fine per cui si è connesso (comperare un libro, controllare un indirizzo, cercare il titolo di una canzone, leggere una notizia, scaricare un documento scientifico, fare un bonifico o pagare le tasse) e ciò è più che comprensibile. Alla fin fine Internet non è altro che un acceleratore della ricerca e di informazioni, uno strumento per definizione incompatibile con l'inesigibile comportamento che il regolatore vorrebbe imporre all'utente. Sarebbe come chiedere a un viaggiatore di scegliere, per una stessa destinazione, fra un volo diretto di 4 ore e uno di 16 con 6 scali tecnici intermedi. Chi mai opterebbe per il secondo?

Che il consenso raccolto dall'utente di Internet su cookie e affini possa dirsi

"informato" si risolve quindi in una mera e ipocrita utopia. Utopia che peraltro trascura che il mondo del web non è popolato esclusivamente da editori scrupolosi e attenti alle regole sulla privacy. Il *World Wide Web* è, e continua ad essere, per sua natura, in larga parte incontrollato e incontrollabile e la facilità con la quale la diffusione, la sottrazione, l'elaborazione, il raffronto di dati personali degli utenti possono essere svolti, richiederebbe una politica di approccio diametralmente opposta a quella che risulterebbe oggi praticata. D'altra parte è lo stesso regolatore che – "in alternativa" – attribuisce agli utenti la facoltà di accettare con un solo click, e in un'unica soluzione, la policy sui cookie degli editori, cioè di fatto stimolandoli all'abdicazione del diritto. Con che lo pseudo-consenso dell'utente apre le dighe ad una comunicazione di dati incontrollata[12].

Un'occasione di revisione della disciplina attuale è data dalla prossima pubblicazione del Regolamento e-Privacy. Come il GDPR ha sostituito le Direttive in tema di privacy che avevano avuto attuazione negli Stati aderenti, così il Regolamento e-Privacy andrà a sostituire la Direttiva n. 2002/58/CE menzionata al § 1, risultando direttamente applicabile negli Stati Membri e determinando il superamento del cit. art. 122 del D.Lgs. 196/2003. L'iter legislativo del nuovo Regolamento e-Privacy è in ritardo sulla tabella di marcia. La bozza di regolamento è stata presentata dalla Commissione nel gennaio 2017[13]. Le posizioni sono ancora distanti, alla ricerca del bilanciamento tra interessi delle imprese e tutela degli utenti e già in due occasioni si è registrata la sollecitazione dell'*European Data Protection Board* rivolta ai legislatori dell'UE a intensificare gli sforzi per l'adozione del regolamento[14].

La bozza originaria del Regolamento e-Privacy si proponeva di risolvere il tema dei consensi parzializzati alla installazione dei cookie mediante la previsione di impostazioni generali nel browser utilizzato, che potessero essere ritenute valide per tutte le attività di navigazione. Tale proposta risultava apprezzabile per il fatto che la scelta sarebbe stata compiuta dall'utente una tantum e avrebbe consentito, quantomeno, l'eliminazione dello stillicidio rappresentato dalle richieste di accettazione delle policy sui cookie, che attualmente si ripetono ogniqualvolta si acceda a un sito web. Tale soluzione tuttavia risulta attualmente osteggiata da posizioni presentate da diversi Stati Membri che hanno allagato il tavolo di lavoro con molteplici richieste di

[12] Cfr. par. 1.

[13] Cfr. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017PC0010&qid=1528296773144&from=EN

[14] Cfr., da ultimo, il Comunicato 13 marzo 2019 dell'EDPB su www.edpb.europa.eu.

modifica introduttive di eccezioni che toglierebbero ogni effetto positivo al rimedio. Senza contare che l'attuale struttura del regolamento ruota ancora fortemente sulla regola del consenso preventivo (alla raccolta) o successivo (alla conservazione) (cfr. artt. 6-10 della bozza) con pronunciato rischio di ritorno al punto di partenza.
Gli interessi in gioco sono evidenti e chi fornisce servizi vorrebbe normativamente consolidare e pietrificare l'assunto attuale per cui "se usi il web, i tuoi dati sono miei". Appare piuttosto lontana l'individuazione di una soluzione capace di contemperare le esigenze di vari player. Eppure sta sotto i nostri occhi.

Una proposta di inversione: dallo pseudo-consenso informato al rifiuto presunto

La soluzione proponibile si fonda su una decisamente coraggiosa inversione di marcia. All'assunto attuale dovrebbe sostituirsi il principio per cui "se usi il web i tuoi dati restano tuoi", seguito dal corollario: "a meno che tu decida di scientemente condividerli".
Come osservato al par. 3, i rimedi tecnici per evitare la funzionalità, quantomeno dei cookie, ci sono e si concretizzano nella possibilità, già resa disponibile da oramai tutti i browser sul mercato, di rendere anonima la navigazione. In più, organizzando e rendendo parte del sistema i proxy di anonimizzazione, la navigazione "in incognito" risulterebbe ancora più efficace.
Il punto di partenza consiste dunque nel rovesciamento dell'impostazione tecnica attuale. La navigazione dovrebbe aver luogo in totale anonimato legalmente garantito (con la sola esclusione, s'intende, della possibilità di accesso, attraverso canali controllabili *ex post*, da parte di forze dell'ordine e magistratura per la prevenzione o la repressione di attività criminose, come già accade a fronte di quella degenerante aberrazione che prende il nome di *dark web*). Sarebbe sufficiente rendere quindi obbligatoria di *default* questa impostazione per proteggere gli utenti da tracciamenti indesiderati. In altre parole, in luogo della farsesca richiesta di un consenso inevitabile, occorre introdurre tecnicamente e legalmente la "presunzione di rifiuto" alla raccolta e alla profilazione. Qualora viceversa l'utente intendesse usufruire di tutti i servizi garantiti da cookie di profilazione, avrebbe comunque la facoltà di palesarsi, ma a quel punto lo *switch* (la dazione del consenso), interverrebbe (potrebbe intervenire) in termini di consapevolezza e di effettiva informazione. Così come la revocabilità del consenso dovrebbe essere garantita in ogni momento.
Il secondo e fondamentale passo consiste nell'obbligo dei provider di impedire,

nell'impostazione di default o in caso di revoca del consenso, che parti terze (inserzionisti o fornitori di beni e servizi) possano effettuare tracciamenti o siano tenuti a cancellare quelli pregressi, così come di eliminare ogni traccia di comandi vocali, registrazioni, geolocalizzazioni, documenti o immagini (soprattutto nei servizi a pagamento, dove per pagamento deve intendersi anche il prezzo, normalmente non modesto, dei mezzi e dei dispositivi che incorporano IOT o altri similari metodi di fruizione di servizi: pagati, appunto, con l'acquisto del *device*[15]).

Il terzo e ultimo passo consiste nel potenziare gli strumenti a disposizione delle Autorità di controllo e rendere obbligatori e periodicamente regolari accessi e ispezioni presso provider e imprese al fine di sorvegliare l'effettivo rispetto della presunzione di rifiuto di profilazione. Accessi e ispezioni che dovrebbero attivarsi in automatico in presenza di fondati reclami dei proprietari dei dati. Il tutto assistito da salatissime sanzioni pecuniarie il cui ricavato vada, in parte, a compensare i costi degli operatori scrupolosi e corretti e a beneficio degli utenti danneggiati.

A chi obiettasse che in tal modo il business di Internet sarebbe compromesso è agevole replicare che la rete non può essere uno spazio senza regole o governato da regole fittizie e facilmente eludibili. Ma occorre aggiungere che il paventato pregiudizio sarebbe estremamente contenuto. Il navigatore medio, compreso nel suo narcisistico esibizionismo, volentieri accetterebbe come già accetta le profilazioni, specie se accompagnate da qualche vantaggio economico o di mera accresciuta visibilità. L'uso dei social network, concepito per la deliberata esposizione dei sé, degli ego e degli *es*, ne è la migliore e inconfutabile prova.

Quest'ultima considerazione, tuttavia, ci restituisce la vera chiave di lettura del problema, con cui concludiamo la trattazione.

Se è innegabile che la lobby internettiana remi con forza contro ogni seria riforma dei principi e delle regole, è altrettanto indiscutibile che il problema della privacy sia avvertito, nei fatti, solo da una minoranza di utenti, di coloro cioè che ancora aggiungono alla riservatezza quel fondamentale valore d'intimità che le masse oggi disdegnano. Nel *trade-off* legislativo non è difficile immaginare lo sguardo benevolo o tollerante del regolatore verso i colossi del sistema piuttosto che verso la massa degli utenti. Trattandosi di un problema che coinvolge una minoranza, lo si può in fondo trascurare. Peccato si tratti dello stesso sistema che altrove professa, celebra e (assai

[15] Ad esempio, il sistema GPS incorporato in un'automobile o il dettatore vocale di messaggi o mail incluso in uno smartphone non è un servizio aggiuntivo gratuito, bensì una funzionalità specifica del bene, compresa nel suo prezzo e come tale reclamizzata.

meno) pratica la protezione degli individui, dei deboli e degli svantaggiati. L'ipocrisia normativa, più che nel tragicomico consenso informato, risiede in questa cosciente trascuratezza di protezione di coloro che non accettano di piegarsi alla regola della cessione gratuita della propria intimità, forse – e la faccenda si farebbe assai più grave – con l'obiettivo di indurre quei coloro a capitolare e ad unirsi, beati e belanti, all'incoscienza di massa. Come in parte già sta accadendo.

P.S. Mentre scriviamo sopravviene una novità dirompente. Il 1° ottobre scorso una pronuncia della Corte di Giustizia UE nella causa C-673/17 segna l'inizio di quel percorso di inversione qui suggerito. La causa era stata promossa dalla federazione delle organizzazioni e associazioni di consumatori tedesche nei confronti di una società di giochi online e riguardava il consenso, da parte dei partecipanti a un gioco a premi organizzato dalla società, al trasferimento dei loro dati personali agli sponsor e ai partner della stessa, nonché all'archiviazione di informazioni e all'accesso a informazioni archiviate nell'apparecchiatura terminale degli utenti. La Corte ha osservato come l'autorizzazione alla archiviazione di informazioni, o l'accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente di un sito Internet attraverso cookie, debba esprimersi con un "consenso attivo degli utenti", negando quindi validità al consenso espresso mediante deselezione di una casella di spunta che all'apertura della pagina appariva selezionata di default. *Stay tuned, game is not over*.