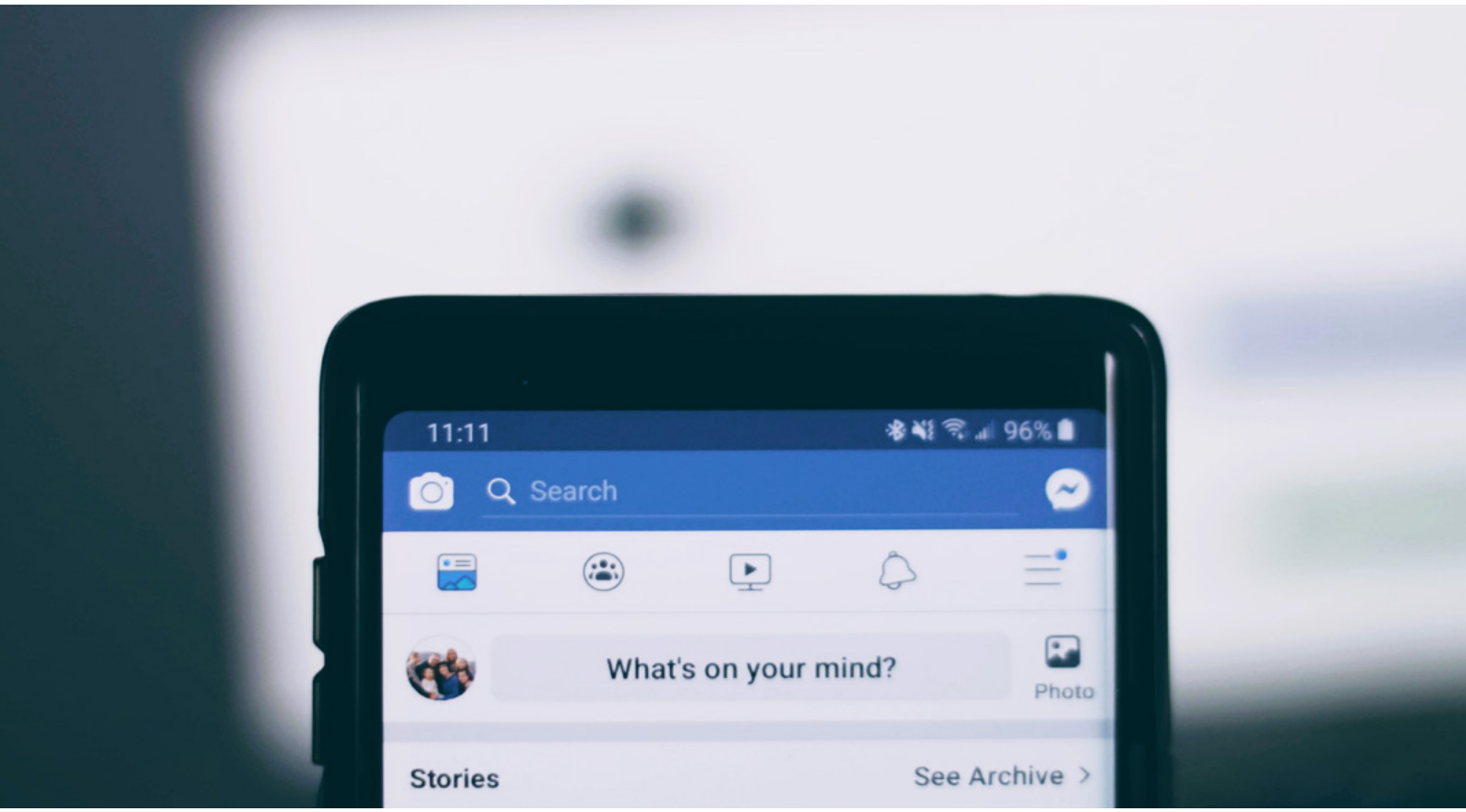
CILD Coalizione Italiana Libertà e Diritti civili



Tutela Dati Personali

COMPRENDERE E PROTEGGERSI DALLA PROFILAZIONE ONLINE A FINI DI MARKETING E PROPAGANDA POLITICA

CILD - COALIZIONE ITALIANA LIBERTÀ E DIRITTI CIVILI
via Monti di Pietralata, 16 – 00157 ROMA - cild.eu - info@cild.eu

CHI SIAMO?

Nata nel 2014, la Coalizione Italiana per le Libertà e i Diritti civili (CILD) è una rete di 35 organizzazioni della società civile che lavora per difendere e promuovere i diritti e le libertà di tutti, unendo attività di advocacy, campagne pubbliche e azione legale. Le aree tematiche di cui CILD si occupa sono soprattutto diritti di migranti e rifugiati, discriminazioni, giustizia penale, libertà di espressione e privacy.

COVER IMAGE

joshua Hoehne on Unsplash

Indice

CILD - COALIZIONE ITALIANA LIBERTÀ E DIRITTI CIVILI
via Monti di Pietralata, 16 – 00157 ROMA - cild.eu - info@cild.eu

COSA SONO I DATI PERSONALI?

Secondo la normativa europea e italiana, comunemente accettata da giurisprudenza e dottrina, sono dati personali le informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue abitudini, caratteristiche fisiche, stile di vita, relazioni personali, stato di salute, situazione economica. Non solo quindi i tradizionali documenti di identità ma più in generale qualsiasi dato riferibile ad un individuo, identificabile anche in un secondo momento.

Particolarmente importanti sono:

- I ***dati identificativi***: che permettono l'identificazione diretta (come i dati anagrafici, i documenti personali, numero telefonico ed indirizzo IP, le immagini);
- I ***dati sensibili***: tutti i dati che qualificano la personalità del soggetto nelle sue scelte più intime. Possono rilevare, anche solo potenzialmente, l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, lo stato di salute e la vita sessuale;
- I ***dati giudiziari***: fanno parte dei dati sensibili e in particolare possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti a iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto o l'obbligo di soggiorno, le misure alternative alla detenzione), o la veste di imputato o di indagato (i c.d. carichi pendenti).

Anche tutte le informazioni che consentono di monitorare gli spostamenti di un individuo, quali forme di geolocalizzazione fornite da smartphone o applicazioni, fornendo informazioni sui luoghi frequentati e sugli spostamenti, sono considerati dati personali e quindi soggetti alle forme di tutela previste dalla legge.

Il diritto alla protezione dei dati personali

Il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo tutelato in Italia dal Codice in materia di protezione dei dati personali (decreto legislativo 20 giugno 2003, n. 196, come novellato dal D.lgs. 101/2018) e in

Europa dal nuovo Regolamento 2017/679, che ha efficacia dal 25 maggio 2018. È, inoltre, un diritto fondamentale dell'individuo riconosciuto a livello europeo e internazionale dalla Carta dei Diritti Fondamentali dell'UE (artt. 7 e 8), dalla Convenzione Europea sui Diritti dell'Uomo (art. 8) e dalla Dichiarazione Universale dei Diritti dell'Uomo (art. 12), oltre che da vari altri atti normativi italiani e internazionali.

In concreto tale diritto consente ad ogni individuo di pretendere che i propri dati personali siano trattati da terzi solo nel rispetto delle regole e dei principi stabiliti dalla legge.

Come si esercita questo diritto?

Ogni persona può tutelare i propri dati personali, in primo luogo, esercitando i diritti previsti dagli articoli da 15 a 22 del Regolamento Europeo.
In particolare, ogni interessato può presentare un'istanza al titolare[5] o al responsabile del trattamento dei dati, senza particolari formalità. L'istanza può essere riferita, a seconda delle esigenze dell'interessato, a specifici dati personali, categorie di dati, ad un particolare trattamento oppure a tutti i dati personali che lo riguardano. Nell'esercizio dei diritti l'interessato può farsi assistere da una persona di fiducia (ad esempio un legale) e può anche conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi.

Il titolare del trattamento è obbligato a fornire una risposta ad ogni richiesta, senza ritardo, entro e non oltre:

- 30 giorni dal suo ricevimento;
- Ulteriori 30 giorni se le operazioni necessarie per un integrale riscontro sono di particolare complessità, ovvero se ricorre altro giustificato motivo. In questo secondo caso, il titolare o il responsabile devono comunque dare riscontro all'interessato entro i primi 30 giorni.

[5] Modello esercizio diritti in materia di protezione dei dati personali, Garante per la protezione dei dati personali http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1089924

Cosa fare se la risposta all'esercizio dei diritti garantiti dal GDPR non arriva nei tempi indicati o non è soddisfacente?

L'interessato può far valere i propri diritti davanti all'autorità giudiziaria o rivolgendosi al Garante per la protezione dei dati personali presentando un Reclamo ai sensi dell'art. 77 del Regolamento (vedi sezione successiva).
Il Regolamento europeo non prevede più l'istituto del ricorso per fare valere i diritti di accesso ai dati personali (che pertanto non può più essere presentato al Garante a partire dal 25 maggio 2018). Dall'introduzione del Regolamento reclamo e segnalazione sono gratuiti.

Tutelare il diritto alla protezione dei dati personali in Italia

Il Garante Italiano

Il Garante verifica la correttezza del trattamento dei dati e il rispetto dei diritti delle persone connessi all'utilizzo delle informazioni personali in ambito pubblico e privato. Si occupa, tra le altre cose, di controllare che i trattamenti dei dati personali siano conformi a leggi e regolamenti ed esamina reclami e segnalazioni da parte degli utenti. Inoltre, ha il potere di vietare in tutto o in parte il trattamento di dati personali che per la loro natura, per le modalità o per gli effetti del loro trattamento, possano rappresentare un rilevante pregiudizio per l'interessato, sanzionando eventuali violazioni.
Può adottare i provvedimenti previsti dalla normativa in materia di dati personali, tra cui in particolare le autorizzazioni generali per il trattamento dei dati sensibili, e segnalare al Governo, quando ritenuto opportuno, la necessità di adottare provvedimenti normativi specifici in ambito economico e sociale. A questo fine può partecipare attivamente alla discussione in merito a possibili regolamentazioni normative con audizioni presso il Parlamento; svolgere indagini conoscitive sullo stato di attuazione delle leggi in determinati settori; verifiche d'iniziativa sui trattamenti che, in base a specifici elementi, abbia motivo di ritenere siano effettuati in violazione di legge o di regolamento.
Il Garante, inoltre, prende parte alle attività comunitarie ed internazionali di settore in quanto componente del Gruppo Articolo 29 (oggi ridenominato "EDPB"

European Data Protection Board) e delle Autorità comuni di controllo previste da convenzioni internazionali (Europol, Schengen, Sistema informativo doganale).

Quali tutele e strumenti?

Ogni persona può tutelare i propri dati personali, in primo luogo, esercitando i diritti previsti dagli articoli da 15 a 22 del Regolamento (UE) 2016/679.
Ogni interessato può presentare un'istanza al titolare del trattamento, solitamente indicato nelle informative, senza particolari formalità (ad esempio mediante lettera raccomandata o posta elettronica).
L'istanza può essere riferita a seconda delle esigenze dell'interessato, a specifici dati personali, a categorie di dati o ad un particolare trattamento, oppure a tutti i dati personali che lo riguardano.

IL RECLAMO

Il reclamo al Garante è un atto dettagliato con il quale un cittadino – portatore di un interesse diretto – riporta la lesione del diritto alla protezione dei suoi dati personali, ciò che in giurisprudenza viene definita dalla violazione dell'articolo 77 del Regolamento UE 679/2016 GDPR e degli artt. da 140-bis a 143 del Codice. Al reclamo segue un'istruttoria preliminare e un eventuale successivo procedimento amministrativo formale che può portare all'adozione dei provvedimenti di cui all'articolo 58 del Regolamento. Avverso la decisione del Garante è ammesso il ricorso giurisdizionale ai sensi degli articoli 143 e 152 del Codice e dell'articolo 78 del Regolamento. La presentazione del un reclamo è gratuita. Per approfondimenti si rimanda alla pagina informativa del Garante.

LA SEGNALAZIONE

Chiunque può inoltrare al Garante, ai sensi dell'art. 144 del Codice, una segnalazione per la violazione del diritto alla protezione dei dati personali del pubblico o di un terzo soggetto. Questa può essere valutata dall'Autorità anche ai fini dell'emanazione dei provvedimenti di cui all'art. 58 del Regolamento.

Il Garante Europeo

L'Autorità europea ha il compito principale di controllare che le istituzioni e gli organi dell'Unione rispettino il diritto dei cittadini al trattamento riservato dei dati personali. In aggiunta a questo compito fondamentale, offre consulenza alle istituzioni e agli organi dell'UE su tutti gli aspetti del trattamento dei dati personali e delle relative politiche e legislazione da implementare; gestisce denunce e conduce indagini; collabora con le amministrazioni nazionali dei paesi dell'UE per assicurare la coerenza legislativa nell'ambito della protezione dei dati; controlla le nuove tecnologie che possono influire sulla protezione dei dati.

LA PRIVACY È IMPORTANTE ANCHE SE NON HAI NULLA DA NASCONDERE

Una buona parte della nostra vita si svolge online. Sulla rete lavoriamo, ricerchiamo prodotti da comprare, troviamo il compromesso migliore per le vacanze che pianifichiamo di fare d'estate, guardiamo gli eventi ai quali partecipare con i nostri amici, eseguiamo movimenti bancari e cerchiamo informazioni sulle malattie che ci preoccupano. È chiaro dunque come la dipendenza da queste attività porti ad una grande mole di informazioni e condivisione di dati personali nelle mani di poche ed enormi multinazionali che, ancora oggi, non garantiscono – fra le altre cose – efficiente minimizzazione del rischio di eventuali *data breach*, trasparenza e policy efficaci per la protezione dei dati personali degli utenti. Quanto di più problematico esiste nel nostro rapporto con il dominio digitale è la poca o totale mancanza di coscienza nei confronti dei nostri dati personali: essendo la nostra vita online – con molta probabilità – il riflesso di quella che è la vita al di fuori da siti web e social network, è logico pensare che abbia un grande valore. E se per noi è di natura affettiva o meramente ludica, per i proprietari di piattaforme come Facebook (e dunque Instagram e Whatsapp), Twitter, LinkedIn e in generale di siti web, è di tipo economico. E se forse è ancora difficile comprendere questo aspetto, a mantenerci allerta ci sono i cosiddetti *hacker* malevoli: attraverso i loro attacchi informatici, dimostrano quanto rubare dati e informazioni personali danneggi gravemente gli utenti così come coloro che dovrebbero occuparsi di mantenerli al sicuro, mettendone nero su bianco il loro valore.

Spesso il ragionamento di molti utenti ricomprende una certa inconsapevolezza non solo dei propri dati personali, bensì anche delle molteplici cause per le quali vengono spiati o sorvegliati. In primis un utente – anche se forse sarebbe più corretto dire un individuo – possiede un pensiero: questo può essere distorto o cambiato a favore di un'azienda o di un'ideologia politica. Un individuo ha anche una capacità economica alla quale le compagnie assicurative, le aziende e altri soggetti mirano per la vendita dei loro prodotti. Un cittadino è tale poiché ha un'identità: questa può essere utilizzata da criminali per impersonarlo oppure per risalire ad ulteriori informazioni inerenti alla sua vita. Un utente ha un ruolo nella società e nella comunità più ristretta della quale fa parte – è padre, madre,

figlio/a, sorella, fratello – e può fornire, volontariamente o involontariamente, dati e informazioni su tutti i componenti. Un utente è nodo per altri utenti: per questo motivo la maggior parte delle app chiedono di aver accesso ai contatti presenti sul telefono. Sulla base di quanto detto, è possibile affermare che tutti sono persone importanti. Per vari motivi tutti gli individui sono una fonte di potere. Senza privacy, altri soggetti possono esercitare questo potere contro di te.

Come giustamente sottolineato da Privacy International[6], organizzazione benefica che sensibilizza cittadini e governi sul tema della privacy, in questa circostanza è importante che i singoli siano abili a prendere decisioni informate in merito alla gestione dei loro dati, proteggendo i loro dispositivi e i loro dati personali, senza lasciare che in ciò interferiscano attori pubblici o privati e contrastando quindi possibili squilibri di potere. Oltre a restituire il controllo agli utenti, parallelamente è essenziale anche evitare di imporgli la protezione di sé stessi, un approccio che minimizza di fatto la responsabilità di aziende, governi e altri *stakeholder*.

Nella pratica, vi sono alcuni esempi calzanti rispetto al tema appena sollevato e, in generale, per quanto riguarda la propria privacy online. La navigazione sul web, infatti, è oggetto di *screening* e di attenzione da parte sia di istituzioni pubbliche sia di privati. Per quanto riguarda le prime è bene sapere che in Italia la c.d. riforma Orlando (legge 103/2017)[7] ha esteso la possibilità di utilizzare software di tipo ***trojan*** per monitorare navigazione e conversazioni degli utenti. Si tratta di un tema che pur non suscitando vasto dibattito pubblico, ha raccolto molte critiche tra gli addetti ai lavori[8]. Al riguardo segnaliamo in particolare la dettagliata analisi di Privacy International, tradotta e condivisa da CILD[9].

---

[6] https://privacyinternational.org/topics/cyber-security

[7] https://www.gazzettaufficiale.it/eli/id/2017/07/4/17G00116/sg

[8] Ddl Orlando, ecco le conseguenze giudiziarie delle intercettazioni con i trojan, Agenda Digitale, 13 giugno 2017 https://www.agendadigitale.eu/documenti/ddl-orlando-ecco-le-conseguenze-giudiziarie-delle-intercettazioni-con-trojan/

[9] Trojan di stato e i rischi della legge Orlando: serve dibattito pubblico, CILD, 20 giugno 2017: https://cild.eu/blog/2017/06/20/trojan-di-stato-rischi-della-legge-orlando-sulla-sorveglianza/ Il testo originale dell'analisi di Privacy International è disponibile qui: https://www.documentcloud.org/documents/3728074-Privacy-International-s-Analysis-of-the-Italian.html

Tuttavia, stati e governi non hanno la possibilità di intercettare comunicazioni – telefoniche o via email – senza l'intervento di un magistrato che garantisca il rispetto delle forme e dei requisiti di legge.
Un'altra questione che resta aperta – e che questa guida non tratterà – è invece quella relativa alle nuove metodologie e tecniche di riconoscimento facciale utilizzate dalle Forze dell'Ordine, anch'essa oggetto di acceso dibattito fra gli esperti in materia.

Anonimato come strumento di esercizio della libertà di espressione

Sulla base di queste premesse, è lecito che l'utente si domandi quali azioni intraprendere al fine di difendersi dall'intrusione di terzi nella sua vita digitale.

Ancora oggi persiste una sorta di stigma nei confronti dell'anonimato online, come se essere anonimi durante la navigazione internet comportasse, di per sé, una volontà criminale o una presunzione di non punibilità in caso di commissione di reati o illeciti civili. In realtà, la necessità di anonimato in rete non è – fortunatamente – esclusiva del cybercriminale, ma è spesso un bisogno che deriva dalla semplice esigenza di evitare attività di monitoraggio delle proprie abitudini di navigazione da parte di intrusioni governative o private.

Sin dagli albori la rete internet, utilizzata inizialmente e principalmente quale metodo di rapido scambio accademico di idee e pensieri, ha assunto una connotazione di intrinseca democraticità con l'obiettivo di incentivare uno scambio quanto più autonomo, libero e decentrato di idee e informazioni, permettendo la costruzione di rapporti sociali su base volontaria. L'anonimato — ivi compreso il ricorso a network anonimi come Tor — rappresenta uno dei più importanti strumenti di salvaguardia di tali caratteristiche. Esso consente la libera manifestazione del pensiero e la libera esplicazione della personalità di ciascun individuo (art. 2 Cost.), ponendolo al riparo dai rischi di intimidazione e stigmatizzazione propri del mondo reale. Non si tratta di un'esigenza limitata alla posizione dei singoli individui. L'anonimato sembrerebbe offrire benefici non irrilevanti anche dal punto di vista dell'autonomia dei gruppi, difatti consentendo

alle minoranze – di genere, di ceto, di etnia, di orientamento sessuale - di esprimere critiche, rivendicare pretese e organizzare forme di mobilitazione a un grado di intensità altrimenti impossibile. Tutto ciò specialmente in quei paesi a scarso tasso di democraticità, dove il suo effetto può essere ampiamente positivo sul piano della partecipazione alla vita politica e, dunque, della redistribuzione del potere sociale.

Anonimato come diritto tutelato dalle normative in materia di protezione dati personali

Il nuovo Regolamento Europeo 679/2016 (GDPR) pone una grandissima enfasi su anonimizzazione, tecniche di pseudonimia dei dati personali e possibilità di fruizione anonima dell'ambiente online. Infatti, poiché è la natura stessa della fruizione dei servizi telematici che implica una cospicua raccolta di informazioni personali dell'utente e una sistematica attività di monitoraggio delle modalità di utilizzazione dal lato del fornitore del servizio, in linea di principio il ricorso a tecniche che favoriscano dei gradi di anonimizzazione è non soltanto lecito ma persino incoraggiato sul piano normativo, in quanto strumentale rispetto all'esigenza di salvaguardare l'utente dalle forme più invasive di sorveglianza elettronica. Come detto, la possibilità di essere anonimi online risponde sia a esigenze legate alla libertà espressiva del singolo (e di un gruppo di individui), sia alla possibilità degli utenti di cercare di esercitare un controllo sulla diffusione dei propri dati personali. Con i prossimi paragrafi capiamo dunque perché è diventato oggi indispensabile essere consapevoli di come esercitare tali prerogative.

Privacy by Default

È importante sapere che attualmente, in compliance con la normativa Europea, i grandi player del mercato dei dati personali sono obbligati a consentire ai propri utenti di ridurre la propria "traccia digitale" (*digital fingerprint*) senza dover passare per espedienti tecnici. Tuttavia, tali opzioni sono raramente attive di default, come previsto dalla normativa e l'utente alla ricerca di maggiore privacy rischia di perdersi fra le pagine del sito web.
E' pertanto necessario conoscere le metodologie e gli accorgimenti finalizzati a

ridurre la propria impronta digitale durante le attività di navigazione in internet. Ma cosa significa privacy per l'utente?

Privacy nella vita quotidiana

Per un utente è necessario – prima di conoscere gli strumenti per proteggerla – avere una giusta comprensione in merito alla valenza e al significato della privacy quotidiana. Un paragone calzante è il seguente: la privacy è come una chiave che, se usata, fornisce accesso agli aspetti più intimi di un individuo, quelli che lo rendono sé stesso e vulnerabile agli occhi degli altri. Racconta la sua storia passata presente e futura, corredata di paure, perdite e fallimenti; fa luce sulle cose peggiori che ha fatto, detto o pensato. Nella vita offline le persone forniscono questa chiave a coloro che amano, condividendo le loro vulnerabilità in cambio di sicurezza e intimità. Per questo esistono diversi livelli di apertura nei confronti degli altri: gli amici e conoscenti conoscono la data del tuo compleanno così da poter organizzare una festa a sorpresa; e i tuoi gusti per trovare il regalo perfetto per questa ricorrenza. Non tutti, però, utilizzano queste informazioni nell'interesse della persona alla quale appartengono: i truffatori possono avvalersi dei tuoi dati personali per impersonarti, le aziende creare pubblicità sui tuoi gusti e indurti dunque a comprare un prodotto, e via dicendo.

Su Internet tutta la navigazione effettuata è da sempre utilizzata a fini statistici e di profilazione utenti sia lato client (browser utilizzato) che lato server (siti web visitati e, in particolare, motori di ricerca). E' possibile affermare che siamo un riflesso di tutto ciò che abbiamo ricercato e ricerchiamo online.
Attraverso tecnologie più o meno raffinate come *Cookies, Flash Cookies, Evercookie, Etags, HTML5 Web Storage e Device Fingerprinting*, sia i siti web che i produttori di browser possono tracciare con un alto grado di precisione le attività e quindi i gusti degli utenti, al fine di comunicare pubblicità sempre più mirata ed ottenere un alto livello di personalizzazione del profilo utente.

Di seguito le definizioni di alcune tecnologie che l'utente può facilmente ritrovare durante la navigazione online.

Cookies: file di piccole dimensioni contenenti dati e informazioni. Un cookie può essere creato per mantenere i contenuti all'interno del carrello di Amazon, o per confermare che l'utente è loggato all'interno del suo profilo Facebook. In questi casi i cookie sono utili alla nostra navigazione online. Diversi sono invece i cookie di terze parti, ovvero quelli utilizzati per la profilazione dettagliata e duratura dell'utente a fini di marketing.

Flash Cookies: raccolta di dati simili a cookie, per tracciamento e impostazioni, che un sito web contenente Adobe Flash può utilizzare durante la navigazione di un utente. Ciò che rende questi cookie differenti da quelli normali è il fatto che Adobe può installarli di default senza l'autorizzazione del fruitore.

Evercookie: è un'applicazione che produce, all'interno del browser web, cookie "zombie" intenzionalmente difficili da eliminare. Questi vengono ricreati da backup archiviati all'esterno della memoria dedicata dal browser web oppure memorizzati direttamente sul computer del visitatore (potendo di fatto violare la privacy e tracciare l'utente attraverso tutti i browser che ha installati). Sono tipicamente utilizzati per ricerche di marketing.

Storia

Edward Snowden, ex NSA, parla di Evercookie utilizzati come metodo per rintracciare gli utenti sul browser anonimo Tor
https://www.theguardian.com/us-news/the-nsa-files

Navigazione in rete e motori di ricerca sicuri

Ad oggi esistono numerose estensioni per browser che consentono all'utente un maggior controllo sui propri dati di navigazione. Tuttavia, l'implementazione cumulativa di molte estensioni incide sulla qualità della navigazione stessa, rallentando il caricamento delle pagine web, inibendo o riducendo la riproduzione di video o la visualizzazione di immagini.

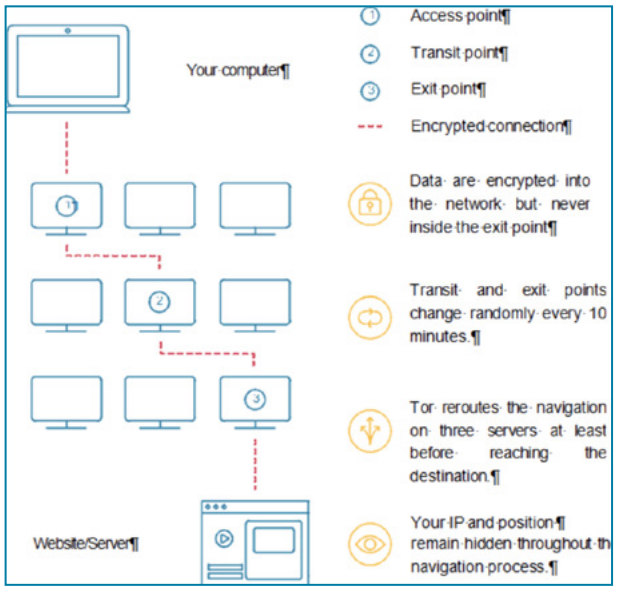
Le estensioni più conosciute, tutte gratuite, sono:

- ***AdBlock***: serve a bloccare noiosi pop-up, banners e alcuni trackers;
- ***AdNauseam***: strumento che automaticamente clicca su ogni pubblicità presente nel sito, rendendo il tracciamento, la profilazione e il monitoraggio degli utenti inutile a scopi di marketing;
- ***Disconnect***: disponibile in versione gratuita (base) e a pagamento, è un'estensione per browser Firefox e Chromium che consente di bloccare numerose "richieste" da parte di *trackers* presenti sui siti web;
- ***Ghostery***: individua e consente all'utente il blocco o lo sblocco selettivo di numerosi tipi di *trackers*;
- ***Lightbeam***: non blocca i tracciatori ma ne consente il controllo attraverso la mappatura degli stessi. Crea inoltre una visualizzazione interattiva che mostra i siti con cui, direttamente o indirettamente, l'utente interagisce mentre naviga;
- ***NoScript***: (per utenti più esperti) consente all'utente il diretto controllo sull'esecuzione di JavaScript, Java, Flash e altri plug-in su determinati siti ed il blocco su altri. Può seriamente inficiare la qualità della navigazione;
- ***Privacy Badger***: controlla che non ci siano attività di *tracking* da parte di tracciatori di terze parti (cioè non direttamente collegati al sito che si sta visitando) bloccando automaticamente il caricamento dei contenuti collegati ai questi ultimi;
- ***Https Everywhere***: è un'estensione per Chrome, Opera e Firefox che, se installata, rende impossibile visualizzare siti che non siano disponibili con sistema di protocollo https. Quest'ultimo permette l'autenticazione del sito web visitato sul server associato con il quale si sta comunicando, proteggendo in questo modo dai cosiddetti *man-in-the-middle attacks*;

- ***Ublock Origin***: è un'estensione anti *tracker* Open Source per Chrome, Firefox, Safari e Microsoft Edge che ha il merito di essere poco incisiva sulle risorse di sistema anche di computer poco performanti. Inoltre il suo codice è costantemente migliorato e tenuto aggiornato da una dedicata *community* che si occupa anche di segnalare la scoperta di nuovi tracciatori.

  L'utilizzo di tali estensioni rende meno incontrollata la diffusione delle proprie informazioni di navigazione a scopo di profilazione. L'utilizzo quotidiano può essere utile per evitare la creazione di un preciso profilo di mercato dell'utente e per evitare casi di discriminazione dei prezzi in base alle proprie abitudini di navigazione e acquisto. Tuttavia non protegge da attività di sorveglianza e controllo in senso stretto. Per proteggere la propria navigazione e comunicazione da questo tipo di intrusioni è invece possibile utilizzare:

- ***Tor*** (The Onion Router): è un browser che permette la navigazione anonima dell'utente. Come spiegato nella figura, le attività dell'utente sono crittate e transitano su una rete di router presenti ovunque nel mondo. La connessione viene "rimbalzata" almeno tre volte prima di arrivare a destinazione. L'unica controindicazione nell'utilizzo di TOR è esattamente la possibilità che il gestore di uno di questi nodi router sia un hacker malintenzionato o un ente di governo preposto al monitoraggio;



- ***Brave Browser*** è un software di derivazione "Chromium" che ha ottenuto particolare attenzione sia perché è stato programmato da un co-fondatore di Mozilla Firefox (Brendan Eich), sia perché è stato al centro di un reclamo formale all'autorità Garante per la Protezione dei Dati Personali Irlandese contro la IAB[10], la più importante organizzazione di lobbying in materia di cookie traccianti sui siti web[11]. È un browser che si distingue da tutti gli altri disponibili sul mercato poiché integra (senza dover quindi installare ulteriori e diverse estensioni) una serie di "anti-tracciatori" il cui scopo è di rendere la navigazione online meno profilabile possibile. Infatti, la filosofia di questo software si basa sulla gestione dei banner pubblicitari, rimossi nei siti web visitati e sostituiti forzatamente con quelli del proprio network (che non tracciano l'utente). Recentemente, anche se solo in versione beta, Brave fornisce agli utenti la possibilità di essere pagati in cambio della visione di alcuni annunci pubblicitari.
- ***PGP*** (Pretty Good Privacy) per quanto riguarda le comunicazioni: è un software di crittografia gratuito ma particolarmente avanzato che consente di cifrare comunicazioni tra utenti. Ad oggi, è comunemente considerato uno dei mezzi più sicuri per la trasmissione di informazioni confidenziali su internet. Numerosi giornalisti e attivisti ne fanno uso per comunicare con fonti o soggetti in pericolo.

[10] Formal GDPR complaint against IAB Europe's "cookie wall" and GDPR consent guidance. Il reclamo è stato successivamente esteso anche alle Autorità Garanti di altre nazioni europee tra cui l'Italia. Per l'Italia, CILD si è occupata di presentare un dettagliato reclamo.

[11] Brave requests European Commission antitrust examination of online ad market; Brave: January Update on GDPR complaint (RTB ad auctions); Brave: February Update on GDPR complaint (RTB ad auctions).

Una connessione privata per tutti: cos'è e come scegliere la giusta VPN

Uno dei migliori modi per proteggere la propria privacy online è utilizzare una VPN (Virtual Private Network): questa permette ad un utente di collegarsi da remoto ad una rete informatica attraverso un "tunnel" virtuale e protetto. È molto comune in ambito aziendale e universitario ma può essere utilizzata da chiunque, per esempio in stati nei quali esiste un Internet censurato o insicuro, dove la navigazione online combinata con l'attivismo sociale, può comportare determinate ripercussioni anche fisiche. Attraverso l'utilizzo di una VPN i dati di navigazione dell'utente come ad esempio indirizzo IP, indirizzi IP dei siti visitati e i servizi utilizzati durante la navigazione possono essere canalizzati attraverso la rete virtuale, schermando in questo modo il dispositivo in uso da possibili hacker malevoli, firewall o dalla sorveglianza governativa. Tuttavia è da notare che, anche in questo caso, non tutti i provider di reti VPN sono trasparenti per quanto riguarda i dati dell'utente che vi transitano. Generalmente i servizi a pagamento non conservano e non trattano questi dati se non quando indispensabile a garantire il servizio. È consigliabile invece diffidare di quelli gratuiti perché nella maggior parte dei casi il contributo mensile è esiguo, ma soprattutto perché la ragione per la quale sono gratuiti è che si avvalgono di alcune preferenze dell'utente.

Idealmente la scelta della VPN dovrebbe basarsi sulle leggi a tutela della privacy esistenti nel paese di provenienza. Quando si discute di giurisdizione si fa di solito riferimento ai cosiddetti *5 Eyes, 9 Eyes and 14 Eyes*[12], ovvero alleanze internazionali nate durante la Guerra Fredda[13] e rappresentanti i vari stati che lavorano insieme per raccogliere e condividere una grande mole di dati basati sulla sorveglianza. Scegliere una VPN di un'azienda operante in un paese al di fuori di queste alleanze internazionali è dunque una scelta saggia, soprattutto dopo che il PRISM *program*[14] ha portato alla luce prove di una collaborazione fra aziende tecnologiche e agenzie

[12] https://restoreprivacy.com/5-eyes-9-eyes-14-eyes/

[13] https://en.wikipedia.org/wiki/Five_Eyes

[14] https://en.wikipedia.org/wiki/PRISM_(surveillance_program)

governative statunitensi con l'obiettivo di fornire diretto accesso ai dati degli utenti. Certamente la scelta di una VPN dipende anche dal proprio ***threat model***, ovvero, in termini semplici, dal soggetto o dai soggetti da cui l'utente deve difendersi[15].

I migliori servizi di VPN disponibili sono[16]:

- ***ExpressVPN***: azienda sotto giurisdizione delle Isole Vergini britanniche, offre all'utente 94 paesi nel mondo fra i quali scegliere per connettersi, nascondendo il luogo dal quale realmente avviene la connessione. Permette la navigazione online e il download in modo anonimo di una grande quantità di contenuti che possono essere censurati o presenti all'interno di siti bloccati, senza tracciare l'utente o le sue attività.
- ***IPVanish***: anche in questo caso non vi è nessun tracciamento dell'utente e i server sono di proprietà dell'azienda stessa. Inoltre, si possono avere fino a 10 connessioni private su molteplici dispositivi e il servizio è accessibile su Android, iOS, Windows, macOS. L'azienda che la produce è situata negli Stati Uniti.
- ***NordVPN***: creata da un'azienda situata a Panama, offre i servizi già precedentemente citati (server disponibili, connessioni) ma in numeri minori. Fornisce delle estensioni proxy per Chrome e Firefox.

Appartenente al mondo open source è invece OpenVPN, rilasciato sotto licenza GNU GPL[17] e basato su librerie di cifratura OpenSSL[18]. Come tutti i programmi open source la sua sicurezza, gli aggiornamenti, i miglioramenti e la trasparenza del progetto sono supportati da una comunità di utenti ed esperti del settore che ne garantisce la qualità. Anche in questo caso i costi del servizio sono contenuti.

---

[15] Possibili soggetti attaccanti possono essere: le forze di polizia, le agenzie di sorveglianza statali, hacker malevoli, criminalità organizzata, soggetti che non perseguono specificatamente uno scopo ma agiscono "just for fun".

[16] https://www.techradar.com/vpn/best-vpn

[17] https://opensource.org/licenses/GPL-3.0

[18] È un'implementazione open source dei protocolli SSL e TLS, che permettono una connessione sicura, end-to-end, con autenticazione e confidenzialità, https://www.openssl.org

Da non dimenticare è anche OperaVPN, servizio disponibile direttamente sull'omonimo browser Opera: con la sua attivazione viene garantita la connessione ai siti web direttamente via server VPN e quindi facendo figurare quest'ultima in un luogo diverso, attribuendo un IP virtuale.

Dimmi cosa cerchi e ti dirò chi sei: privacy e motori di ricerca

Infine, per quanto riguarda i motori di ricerca, è necessario ricordare che il *core business* di un fornitore di servizio di ricerca è esattamente quello di raccogliere le cosiddette "*queries*", ovvero le ricerche effettuate dall'utente, così da avere un'idea sempre più precisa di cosa cerchi il pubblico collegandolo al *quando*, *come e perchè*, ossia a determinati momenti storici, luoghi geografici e alle motivazioni. Tutto ciò per ottenere un alto livello di profilazione dell'utente volto alla creazione di pubblicità mirate e, quindi, all'ottenimento di un ritorno economico.

In alternativa, e per ovviare al problema, è possibile utilizzare dei motori di ricerca differenti. Alcuni di questi sono, ad oggi, ancora poco conosciuti (e quindi potenzialmente meno efficienti nel ritorno dei risultati di ricerca rispetto ai concorrenti più accreditati). Alcuni di questi sono *DuckDuckGo*, *Startpage Search*, *Search Encrypt*, *Qwant*, *Gibiru* e *Swisscows*. La maggior parte si basa su motore di ricerca Google o Yahoo (e dunque alta qualità nei risultati) garantendo però all'utente che la sua attività online non sia tracciata, memorizzata e profilata, così da non poter fattivamente vendere nessun dato di navigazione ad aziende terze. Questi motori di ricerca permettono inoltre di eludere la cosiddetta *filter bubble* che di fatto isola l'utente da potenziali risultati che "confliggono" con le sue ricerche o interessi abituali. Nello specifico:

- ***DuckDuckGo*** è probabilmente il browser e motore di ricerca più conosciuto fra quelli citati: i risultati che ritornano all'utente derivano da molte fonti come Yahoo, Bing, Index, Wikipedia e il DuckDuckBot[19]. Non memorizza indirizzo IP e informazioni

[19] Il DDGbot è un web crawler, ovvero un internet bot che sistematicamente naviga all'interno del World Wide Web con lo scopo di ricercare pagine web. Alcuni motori di ricerca utilizzano questi bot per aggiornare i loro contenuti web o indicizzare pagine internet in modo tale da renderle più facilmente ricercabili ai propri utenti.

di navigazione cosicché l'utente non sia destinatario di pubblicità mirata con la quale si ritroverebbe invece a fare i conti su un motore di ricerca tradizionale come Google.

- ***Startpage Search*** è un motore di ricerca molto simile al primo per quanto riguarda l'attenzione alla privacy, ma fornisce risultati molto più precisi poiché pescati all'interno di Google.

- ***Search Encrypt***: un motore di ricerca che, come gli altri, non permette la profilazione dell'utente e dunque la pubblicità mirata, cancella la cronologia di ricerca una volta terminato il suo utilizzo ed è dotato di SSL Encryption, ovvero richiede al sito al quale ci si sta connettendo una connessione sicura alla quale inoltrare dati criptati. Senza questo tipo di certificazione SSL, le informazioni sono trasmesse in chiaro compromettendo la sicurezza dell'utente. È possibile scaricare un'estensione di Search Encrypt per Chrome.

- ***Qwant***: nato nel 2013 e, a differenza degli altri motori di ricerca, europeo (per la precisione francese). Non utilizza cookies o strumenti di tracciamento per profilazione pubblicitaria, dissocia l'indirizzo IP dalle ricerche dell'utente così da renderle anonime e crea una "memoria locale" sul dispositivo utilizzato per memorizzare alcune informazioni utili alla navigazione (lingua, filtro dei contenuti). Esiste anche in versione dedicata ai bambini e ragazzi tra i 6 e i 13 anni, Qwant Junior. Quest'ultimo favorisce contenuti di tipo formativo ed educativo, nascondendo i risultati pornografici, violenti, contenenti discorsi d'odio o relativi al consumo di droga.

- ***Gibiru***: simile ai precedenti motori di ricerca, aggiunge, fra le opzioni, la funzione "uncensored" (non censurato). Gibiru infatti offre un servizio VPN e la possibilità di svelare siti, immagini, video o notizie che sono nascosti dai motori di ricerca mainstream, solitamente per questioni legate alla censura imposta dallo stato in cui l'utente risiede ovvero a contenuti potenzialmente pericolosi.

- ***Swisscows*** è invece un motore di ricerca posizionato al di fuori dell'Unione Europea e degli Stati Uniti, in Svizzera. Oltre ad avere un server dedicato, non lavora

con fornitori terzi ed è un motore di ricerca semantico: utilizza un'intelligenza artificiale e il *machine learning*[20] per valutare il contesto di una ricerca impartita dall'utente. In questo modo, il risultato è trovato più facilmente e viene messo in risalto rispetto agli altri.

È consigliabile utilizzare questi browser quando si effettuano ricerche in merito ad informazioni sensibili, come, ad esempio, lo stato di salute relativo ad un utente o a sé stessi. "Meglio essere sicuri che dispiaciuti" quando si parla di protezione delle proprie informazioni durante la navigazione online.

[20] In italiano, apprendimento automatico. Esplora lo studio e la costruzione di algoritmi che apprendano da insiemi di dati e dunque predire su questi ultimi costruendo in modo induttivo un modello basato su dei campioni. Per approfondire, http://ai.stanford.edu/people/nilsson/MLBOOK.pdf

UTILIZZO CONSAPEVOLE DEI SOCIAL NETWORK

I social network sono una diversa e più evoluta forma di quella che in sociologia e antropologia viene chiamata rete sociale. Mentre quest'ultima consiste in un gruppo di individui connessi fra loro da diversi legami sociali – sia in qualità che quantità – come i colleghi di lavoro, la famiglia, i conoscenti; quella online non prevede invece limiti nel numero di individui appartenenti alla stessa rete, né alle relazioni attuabili. Per quanto vi siano studi che quantificano quello che potrebbe essere il limite massimo di persone con le quali mantenere relazioni sociali[21], possiamo affermare che i social network hanno evoluto fortemente la comunicazione fra individui anche molto lontani fra loro, e non solo per distanza. Social network come Facebook, Twitter, Instagram, WhatsApp, VK, LinkedIn, Pinterest, sono lo strumento di condivisione e informazione per eccellenza e rappresentano straordinarie forme di comunicazione, anche se comportano dei rischi per la sfera personale degli individui coinvolti. I social network sono strumenti che danno l'impressione di uno spazio personale o di piccola comunità.


Facebook Unveils Redesign as It Tries to Move Past Privacy Scandals

Facebook future is anonimity

https://www.nytimes.com/2019/04/30/technology/facebook-private-communication-groups.html

Si tratta di un falso senso di intimità che può spingere gli utenti a esporre troppo la propria vita privata, a rivelare informazioni strettamente personali provocando effetti collaterali anche a distanza di anni: tutte questioni che non dovrebbero essere sottovalutate. I dati e le informazioni caricate online nel corso dell'utilizzo delle varie piattaforme social sono comunque conservati nei server e negli archivi informatici dell'azienda che offre il servizio.

[21] https://it.wikipedia.org/wiki/Numero_di_Dunbar

Tutti i dati volontariamente condivisi dall'utente vengono analizzati unitamente alla quantità e qualità dei contenuti visualizzati, preferiti e "mi piace", così come il tempo trascorso sulle pagine, le reti di relazioni con altri utenti, la localizzazione geografica, la tipologia di dispositivo utilizzato per la fruizione e molto altro.

I social network, al contrario di quanto si creda comunemente, non offrono servizi a titolo gratuito agli utenti, non sono un'entità pubblica, svolgono un'attività a scopo di lucro e dunque non necessariamente a favore dell'utente. I social network trovano la controprestazione economica nel rapporto con quest'ultimo attraverso l'appropriazione e il trattamento dei suoi dati personali e delle informazioni che condivide.
Queste ultime, una volta rese pubbliche su una piattaforma di questo tipo, non sono più sotto il controllo dell'utente. I dati possono essere salvati e conservati da tutti i contatti e dai componenti dei gruppi dei quali si fa parte. Possono essere conservati, rielaborati, diffusi, anche a distanza di anni.
Quasi sempre infatti, accettando di iscriversi ad un social network, si concede all'impresa che gestisce il servizio la licenza di utilizzare senza limiti di tempo il materiale caricato online: foto, chat, pensieri e, eventualmente, anche materiale protetto da copyright, quali ad esempio opere intellettuali prodotte dall'utente.
Questi dati vengono utilizzati per creare profili molto precisi che saranno bersaglio di pubblicità commerciale o politica mirata anche al di fuori dalla piattaforma. La vendita di annunci pubblicitari sui social è la fonte di maggior introito economico per questo tipo di attività[22] e, dunque, il modello di business. Le nuove norme europee in materia di trattamento dati stanno cercando di obbligare i fornitori di servizi ad offrire delle informative semplici da comprendere ai propri fruitori. È bene abituarsi a leggere cosa esattamente prevedono termini, le condizioni d'uso e le garanzie di privacy offerte nel contratto che si accetta al momento dell'iscrizione ad un social network. Tuttavia, questi oneri informativi non sono sempre rispettati dalle compagnie e già oggi alcune autorità garanti europee sono intervenute sanzionando i grandi collettori di dati come Google e Facebook.

[22] How You're Making Facebook a Money Machine, The New York Times, 2016
https://www.nytimes.com/2016/04/30/upshot/how-youre-making-facebook-a-money-machine.html

Facebook Tracking Exposed

FbTREX[23] è un'estensione open source per browser che ha lo scopo di raccogliere i contenuti visibili nel proprio feed di Facebook, e un sito web che aggrega tutti i dati che gli utenti dell'estensione hanno raccolto durante la loro navigazione online. Creato con lo scopo di rendere gli utilizzatori delle piattaforme social, dunque i cittadini, i giornalisti interessati alla pluralità di informazione e i ricercatori nell'ambito della *data analysis*, coscienti di come siano tracciate le loro attività online, FbTREX è uno strumento utile. Ciò che vediamo online e, specificatamente, su una piattaforma come Facebook, è frutto di una selezione dei contenuti condivisi dai nostri amici. Ma in quale modo il social network decide di farci visualizzare il nostro feed? L'algoritmo di Facebook non è trasparente e in continuo cambiamento. In questo senso è possibile dunque che ciò che vediamo durante la nostra navigazione all'interno della piattaforma possa essere "ritagliato su misura" per noi e favorisca la cosiddetta *filter bubble*. Il pericolo è che gli utenti siano influenzati nella visualizzazione di contenuti e, di conseguenza, incapaci di operare scelte che rispecchino fattivamente la loro volontà.

Inoltre, sulle piattaforme social, è spesso possibile attivare/collegare alcune "app" che, in maniera più o meno trasparente, raccolgono anch'esse la medesima mole di dati senza che l'utente ne sia consapevole. È precisamente così che Cambridge Analytica ha incrociato la sua base dati con la raccolta proveniente da Facebook: attraverso una app collegata.


Vox

The Facebook and Cambridge Analytica scandal, explained with a simple diagram

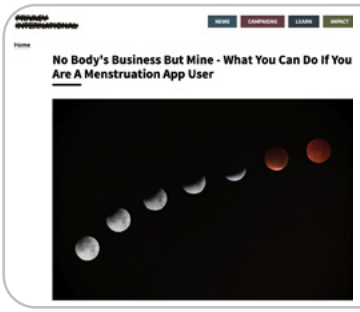
A visual of how it all fits together. They're now shutting down.

Cambridge Analytica spiegato in modo semplice

https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

[23] https://facebook.tracking.exposed/privacy-statement

Per questo motivo il *social login*, ovvero la pratica di utilizzare il proprio account social per accedere ad altri servizi, dovrebbe essere evitato o quantomeno limitato e utilizzato solo in casi in cui la tradizionale creazione di un account attraverso email e password sia, per qualche motivo, inutilizzabile. Inoltre, in molti social network è permessa la sola disattivazione del proprio profilo personale senza possibilità di cancellarlo, anche in caso di terminazione del servizio. In questo caso è possibile – anche se per soli utenti mediamente esperti – fare affidamento ad uno *script*[24] che ripetutamente rimpiazza i contenuti condivisi dall'utente ad esempio su Facebook, con dati e informazioni randomici e senza senso. Si chiama CasperJS e, dopo alcuni mesi di utilizzo, rende i dati dell'account insensati[25] per l'algoritmo del social network, non più in grado di costruire una profilazione utile dell'utente. Utilizzare script come questi, potenziale base per la creazione di applicazioni più facilmente utilizzabili, significa potersi proteggere in quei paesi – ancora molti – nei quali non è presente il cosiddetto *right to be forgotten* (in italiano, diritto all'oblio).



Come dati medici sono condivisi con Facebook

Una ricerca di Privacy International sulle app per il controllo delle mestruazioni.
https://www.privacyinternational.org/news-analysis/3199/no-bodys-business-mine-what-you-can-do-if-you-are-menstruation-app-user

Solo molto recentemente le Autorità Garanti per la protezione dei dati personali di vari paesi europei hanno comminato alcune sanzioni elevate nei confronti di colossi del web quali Google e Facebook. Le motivazioni dei provvedimenti sono relative a circostanze da tempo note in campo giuridico ma dalle quali l'utente medio è

[24] In termini informatici, un particolare tipo di programma scritto attraverso uno dei linguaggi di programmazione esistenti (detti linguaggio di scripting).

[25] https://motherboard.vice.com/en_us/article/qvxv4x/how-to-delete-facebook-data

spesso tuttora all'oscuro. In sostanza le autorità hanno rilevato come la maggior parte degli utenti dei servizi forniti da Google e Facebook utilizzi le piattaforme da anni senza realmente conoscere l'accordo che hanno stipulato al momento dell'iscrizione "gratuita" al servizio. Il costo reale, ovvero la "causa" del contratto tra utente e piattaforma, è nei dati personali che vengono forniti quotidianamente tramite le attività online. La raccolta di queste informazioni avviene attraverso svariate metodologie informatiche e anche qualora si utilizzi un *nickname* non direttamente riconducibile alla nostra identità. Questo perché le tecniche di *device fingerprinting*[26] identificano in maniera univoca gli apparati elettronici utilizzati per connettersi online e, allo stesso tempo, le informazioni connesse al contratto di fornitura del servizio di connessione alla rete, localizzazione geografica e molto altro. Nel noto caso Cambridge Analytica è stato scoperto come la società era riuscita ad ottenere profili individuali su oltre 200 milioni di cittadini USA: i profili psicografici ottenuti sono stati poi utilizzati durante la campagna politica presidenziale statunitense. La campagna Trump è stata in grado di indirizzare gli elettori a livello individuale, creando messaggi e contenuti su misura per orientare il voto, ovvero per invogliare elettori non ancora schierati.


Facebook Answers Mozilla's Call to Deliver Open Ad API Ahead of EU Election

After calls for increased transparency and accountability from Mozilla and partners in civil society, Facebook announced it would open its Ad Archive API next month. While the details are still limited, this is an important first step to increase transparency of political advertising and help prevent abuse during upcoming elections.

Elezioni EU su Facebook

https://blog.mozilla.org/blog/2019/02/13/facebook-answers-mozillas-call-to-deliver-open-ad-api-ahead-of-eu-election/

[26] In terminologia informatica, l'impronta digitale di un dispositivo è univoca e consiste nelle informazioni raccolte su un dispositivo remoto a scopo identificativo. Più specificatamente, alcune tra le informazioni ottenibili sono la dimensione dello schermo, il software installato, la font.

Il tracciamento dell'utente va oltre le piattaforme social

Mentre guarda la sua bacheca di Facebook, la home di Twitter o il feed di Instagram la probabilità che l'utente venga a contatto con contenuti pubblicizzati o esterni è molto alta. Nel primo caso, visto un prodotto o un servizio che ci interessa siamo indotti a cliccare sull'annuncio per approfondirne i dettagli; allo stesso modo l'utente è curioso di aprire i link condivisi dalla stampa o da siti web di qualsiasi altro genere. Nel momento in cui clicca su un contenuto esterno alla piattaforma in uso e viene reindirizzato al sito web in questione, porta con sé una serie di informazioni alle quali i servizi social hanno accesso. Nella pratica, anche se l'utente non è più attivo sulla piattaforma di provenienza, questa riesce a carpire l'attività online che ne sussegue.

Allo scopo di evitare che gli utenti siano tracciati al di fuori di Facebook, Instagram o Facebook Messenger, è stata creata un'estensione per browser Mozilla Firefox. Questa è un componente aggiuntivo per Firefox desktop con lo scopo di impedire il tracciamento delle attività dell'utente da parte di Facebook confinando il social e altri siti ad esso collegati in un "contenitore" separato.
Facebook Container fa sì che la pagina web venga aperta in un apposito contenitore che separa l'attività svolta sui social da quella di navigazione di altri siti web, di fatto impedendo alla piattaforma Facebook (Messenger o Instagram) di effettuare una correlazione fra i dati raccolti su quest'ultima e quelli derivanti dalla navigazione al di fuori. I contenitori sono semplici schede Firefox che permettono la creazione di sezioni separate: le preferenze del sito, le sessioni registrate e i dati di tracciamento delle pubblicità che si incontrano sulle piattaforme citate non sono trasferiti in altri contenitori. Le schede contenitore impostate di default sono "Personale", "Lavoro", "Banca", "Shopping" ma si possono modificare o anche crearne di nuove. L'estensione permette fattivamente di rendere più facile e veloce la buona pratica della differenziazione di dispositivi: utilizzare a lavoro uno strumento che non viene utilizzato nella vita privata o durante lo shopping online è importante non solo per limitare determinate attività ad alcune schede browser, ma anche per proteggere l'utente da eventuali sviste e impedirgli di visitare accidentalmente un sito di shopping nel contenitore dedicato alle operazioni

bancarie (da mantenere maggiormente più sicuro).
Nel momento in cui l'utente naviga utilizzando la modalità in incognito (concetto molto diverso da quello di anonimato in rete) questa estensione è disattivata.

È comunque circostanza nota che la piattaforma social di Facebook riesca a tracciare utenti anche non iscritti al suo servizio grazie ai pulsanti (presenti in app Android) creati allo scopo di condividere una reazione nei confronti di un contenuto (i cosiddetti "mi piace") presenti su altri siti al di fuori della piattaforma[27]. Secondo Privacy International quasi il 61% delle app Android testate nella ricerca *How Apps on Android Share Data with Facebook*[28], presentata durante la 35esima edizione del Chaos computer Congress (35C3) in Germania, trasferiscono dati e informazioni (talvolta periodicamente) a Facebook nel momento in cui gli utenti le utilizzano. Ciò accade, come detto anche se gli utenti non possiedono un account sul social network e a prescindere che vi siano loggati o meno. Nell'ultimo aggiornamento della ricerca, risalente al marzo 2019, Privacy International ha potuto constatare che alcune delle app investigate[29] non condividono più, ad oggi, dati o informazioni con Facebook.

[27] https://privacyinternational.org/blog/2758/guess-what-facebook-still-tracks-you-android-apps-even-if-you-dont-have-facebook-account

[28] https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report

[29] Tra quelle più popolari: Dropbox, Spotify, Shazam, candy Crush, Duolinguo, TripAdvisor, Indeed Job Search, Yelp, WeChat, VK.

THERE'S NO CLOUD, JUST OTHER PEOPLE'S COMPUTER. I DATI NEL CLOUD

Con il termine *cloud computing*, o semplicemente cloud, ci si riferisce a un insieme di servizi offerti da un fornitore agli utenti attraverso Internet (archiviazione, elaborazione o trasmissione di dati) a partire da risorse presenti in remoto. Un computer possiede infatti una serie di componenti che permettono di elaborare, archiviare o recuperare programmi e dati inseriti al suo interno e visibili all'utente che lo possiede: il cloud rende possibile al proprio computer, collegato ad una rete locale, di estendere queste capacità ad altri computer e dispositivi remoti sulla rete stessa, permettendo ad altri utenti collegati al *cloud provider* (fornitore di servizi) di svolgere le mansioni tramite un semplice browser Internet.

Il cloud, quindi, consente di usufruire di servizi complessi senza doversi necessariamente dotare né di computer e altri hardware avanzati, né di personale in grado di programmare o gestire un sistema di archiviazione dati. Milioni di persone condividono dati personali e informazioni "delicate" come email, fotografie e, sempre di più il loro lavoro, online, su servizi di cloud di proprietà di grandi compagnie come Google. Le problematiche maggiormente sollevate nei confronti dei servizi di *cloud computing* sono quelle relative alla sicurezza informatica e alla privacy degli utenti che utilizzano questa tecnologia. Solitamente il fornitore di servizi cloud dispone di sistemi di protezione contro virus, attacchi hacker o altri pericoli informatici più efficaci (e costosi) rispetto a quelli che potrebbe permettersi il singolo utente o la piccola azienda: ciò fa sì che il cloud computing sia una scelta decisamente più semplice, conveniente ed economica per lo svolgimento di attività di business dell'utente, che può esternalizzare alcuni servizi.

È comunque sempre necessario informarsi bene su quali siano le condizioni applicate dal *cloud provider*. Innanzitutto, i servizi offerti "gratuitamente" quasi sempre prevedono attività di monitoraggio e controllo sui contenuti degli utenti. Inoltre, si deve sempre considerare che, affidandosi a un fornitore remoto, esiste il rischio concreto di perdere il controllo diretto ed esclusivo sui propri dati.

Ad esempio, per quanto riguarda i dati condivisi, è rilevante comprendere se il provider al quale li affidiamo, una volta sciolto il contratto con l'utente, cancelli o meno tutti dati e le informazioni che abbiamo archiviato sul cloud. Per ora è pressoché impossibile verificare né escludere questa dinamica poiché potenzialmente i backup di ogni utente sono mischiati fra loro, rendendo particolarmente difficoltosa una cancellazione selettiva. Ad esempio, proprio per questo motivo quando accediamo a Gmail da un nuovo dispositivo o computer ritroviamo tutte le email ricevute fino a quel momento e i servizi a Google associati. Inoltre, risulta ancora non troppo chiara l'attribuzione di responsabilità in materia di sicurezza: questa è ora divisa tra provider e cliente (a seconda del modello di *cloud computing* utilizzato, IaaS[30] o SaaS[31]) con il potenziale rischio che alcuni dati possano risultare scoperti da qualsiasi garanzia.
I più importanti e noti servizi di cloud computing sono Google Drive, Microsoft Azure, Dropbox, Amazon Web Services.

Proteggere la propria corrispondenza online: posta elettronica

Anche se si utilizza un client locale su PC per scaricare la posta elettronica, esattamente come accade nei Cloud, sono i server dei fornitori di servizi di posta elettronica (Gmail, Yahoo, Microsoft, Apple, Hotmail) che gestiscono tecnicamente ricezione, invio e archiviazione della posta. La propria corrispondenza digitale non è quindi nota solo al mittente e al destinatario come accade con la posta tradizionale, a meno di transitare in forma crittografata. Come dovrebbe essere ormai chiaro, ogni servizio online fornito gratuitamente utilizza, come modello di business, lo sfruttamento dei dati degli utenti del servizio stesso. Anche i fornitori di servizi di casella di posta elettronica come quelli citati non fanno eccezione.
In alcuni casi e per alcuni periodi le attività di raccolta, trattamento e analisi dei dati degli utenti sono sfociati nella vera e propria violazione del segreto e della riservatezza della corrispondenza personale sul presupposto che il servizio viene

[30] Acronimo di *Infrastructure as a Service*, ovvero "infrastruttura come servizio".

[31] Acronimo di *Software as a Service*, ovvero "software come servizio".

fornito gratuitamente o con la scusa di dover necessariamente fornire servizi tecnici (antivirus e anti-spam). Anche se con l'avvento del GDPR la situazione è sicuramente migliorata, quantomeno sotto il profilo formale sarebbe opportuno spostare la propria corrispondenza personale o più "delicata" su servizi che garantiscono una effettiva tutela della privacy dell'utente. In questo modo l'utente può iniziare a svincolarsi dagli ecosistemi di raccolta creati dai grandi accumulatori di dati, che incrociano risultati sui motori di ricerca, attività di navigazione e anche utilizzo della posta elettronica, ottenendo dei profili precisi degli utenti.

Di seguito forniamo, senza pretesa di esaustività, un elenco dei più rinomati servizi di posta elettronica online attenti alla privacy degli utenti. Quasi tutti possono essere utilizzati gratuitamente in forma limitata.

- ***Tutanota***: è un servizio di email crittografate nato in Germania nel 2017. Tutanota rende disponibile un piano gratuito ed ha una app per Android e iOS. La cifratura funziona in modo intuitivo;
- ***Posteo.de***: come il precedente è basato in Germania e certifica che il proprio servizio funziona solo sfruttando energie rinnovabili e offre due gigabyte di storage gratuitamente, è usufruibile anche tramite app dedicate;
- ***Protonmail***: è un servizio basato in Svizzera con i server situati "Sotto 1000 metri di solida roccia", come assicurato dall'azienda. La crittografia end-to-end garantisce che solo mittente e destinatario possano leggere la corrispondenza. Esistono le app per iOS e Android ma il piano gratuito prevede solo 500 megabyte di storage e 150 messaggi al giorno;
- ***CounterMail***: è basato in Svezia. La peculiarità di questo servizio è che per funzionare necessita di una chiave hardware tramite dispositivo USB per poter accedere. Tale circostanza, oltre a renderlo particolarmente sicuro, ne impedisce la fruizione gratuita se non per un breve periodo di prova di una settimana.

RACCOMANDAZIONI

Quando si parla dell'importanza di tutelare i propri dati personali, l'obiezione più comune che capita di sentire suona più o meno così: "ormai i nostri dati sono già nelle mani delle grandi corporation e dei politici, è inutile difenderli".Un'affermazione parzialmente falsa e, soprattutto, viziata da una scarsa conoscenza dei meccanismi sottesi al funzionamento dei mercati sui dati. In primo luogo è necessario pensare alla tutela dei dati personali dei minori di oggi, che saranno i consumatori ed elettori di domani. Inoltre, tutti i dati sono utili ai *data broker* così come sono risorsa essenziale per le aziende che utilizzano big data e il valore che hanno aumenta in modo direttamente proporzionale alla loro "attualità" e pertinenza all'individuo.
Le aziende che fanno business con i dati degli utenti hanno bisogno di conoscere in tempo reale opinioni, preferenze di consumo, cambiamenti di pensiero e idee degli utenti poiché solo in questo modo è possibile fornire un'offerta di prodotti – e come abbiamo visto anche politica – che sia sempre in sintonia con i destinatari, fino a condizionare le stesse scelte finali dell'utente, consumatore, elettore. Pertanto è necessario comprendere come non sia mai tardi per iniziare una seria, consapevole e diffusa difesa dei nostri dati, che nel tempo perdono la loro importanza e il loro "peso specifico" per le aziende che li utilizzano. Proprio sulla base di queste considerazioni, CILD ha aderito alla campagna #StopSpyingOnUs, promossa da Liberties.eu, per sollecitare l'attenzione delle autorità Garanti europee sulle violazioni della normativa perpetrate in modo massivo dai fornitori di pubblicità comportamentale in tempo reale (Real Time Bidding, RTB) sui siti web visitati da utenti spesso inconsapevoli. Grazie al reclamo predisposto dai legali di CILD, dall'8 agosto 2019, anche il Garante italiano si è dichiarato "Autorità interessata" nei procedimenti contro Google e IAB, le due piattaforme che gestiscono la pubblicità comportamentale in tempo reale.
Risulta quindi più che mai importante essere consapevoli che la "battaglia" per una maggior tutela dei dati si sta già combattendo oggi nelle aule di giustizia e presso le Autorità garanti in tutta Europa. Ognuno utente può contribuire semplicemente tenendo alto il livello di guardia e protezione sulle proprie informazioni ed abitudini di navigazione, senza mai dimenticare che – come più volte chiarito da Stefano Rodotà – una efficace tutela dei nostri dati protegge, in ultima istanza, la nostra libertà di scelta.

Laura Carrer
Tommaso Scannicchio

FONTI NORMATIVE

Carta dei Diritti Fondamentali della UE
http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=LEGISSUM:l33501

Convenzione Europea sui Diritti dell'Uomo
http://eur-lex.europa.eu/summary/glossary/eu_human_rights_convention.html?locale=it

Dichiarazione Universale dei Diritti dell'Uomo
http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/itn.pdf

Regolamento Generale sulla Protezione dei Dati 2016/679 (UE)
http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679

Nuovo Codice in Materia di Protezione dei Dati Personali (novella D.lgs. 101/2018)
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9042678

Tutela Dati Personali

COMPRENDERE E PROTEGGERSI DALLA PROFILAZIONE ONLINE AI FINI DI MARKETING E PROPAGANDA POLITICA

PRODUCED BY

CILD

CILD - COALIZIONE ITALIANA LIBERTÀ E DIRITTI CIVILI
via Monti di Pietralata, 16 – 00157 roma - cild.eu - info@cild.eu