Come resistere (per quanto possibile) al capitalismo della sorveglianza

Di Marcello Bellini[1]

[1] Marcello Bellini è laureato in Comunicazione Digitale presso l'Università di Pavia e attualmente Data Analyst presso DDB Group Italy.

Introduzione

L'obiettivo di questo report è quello di creare una catalogazione di tutti le pratiche e gli strumenti a disposizione di un utente per proteggere i propri dati personali dalla raccolta sul web.

È infatti noto che esiste un sistema molto pervasivo di raccolta e catalogazione dei dati di navigazione degli utenti, in cui sono convolti a vari livelli le grandi multinazionali high-tech come Meta o Amazon, le istituzioni e buona parte delle aziende e delle organizzazioni che offrono servizi digitali. Il primo obiettivo di questo monitoraggio è quello di poter sfruttare questi dati per affinare i prodotti e servizi offerti.

I dati raccolti tramite internet sono molteplici e molto vari. Possono essere dati demografici come nome, età o sesso, dati di posizione generati dai dispositivi che utilizziamo, dati di contatto, come mail o numeri di telefono, o addirittura dati riguardanti la nostra attività online[2].
L'utilizzo di questi dati ha permesso lo sviluppo del web per come lo conosciamo e l'affinamento degli algoritmi di selezione di contenuti che sul web filtrano gli elementi che appaiono all'utente mentre naviga (Ads) o quando guarda dei contenuti specifici (es: feed di Google News).
L'apertura improvvisa di un mercato così vasto e così innovativo, in cui i dati sono diventati la merce di scambio principale, ha colto impreparata la giurisprudenza di moltissimi paesi che, pur avendo già leggi a tutela della privacy precedenti all'arrivo del web, ha faticato a creare delle normative con degli effetti tangibili e al contempo capaci di rimanere efficaci nonostante i mutamenti quotidiani delle strategie di monitoraggio online. Lo sviluppo tecnologico, infatti, combinato alla crescita esponenziale della quantità e varietà di dati a disposizione sul web, ha permesso in pochissimi anni di sviluppare modelli di raccolta e analisi dati capaci di ricostruire profili utente molto precisi, che arrivano addirittura a predire alcune caratteristiche "complesse" di un utente - come orientamento sessuale, orientamento politico, inclinazioni e desideri - semplicemente partendo dai dati generati dalla navigazione sul web.

Di per sé l'esistenza di queste tecnologie e la disponibilità di questi dati non costituirebbe necessariamente un pericolo, ma l'utilizzo di questi strumenti dovrebbe avere come prerequisiti il coinvolgimento degli individui oggetto

[2] Office of the Privacy Commissioner of Canada, What kind of information is being collected about me online?, Gennaio 2020 (https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/fs-fi/choice-choix/).

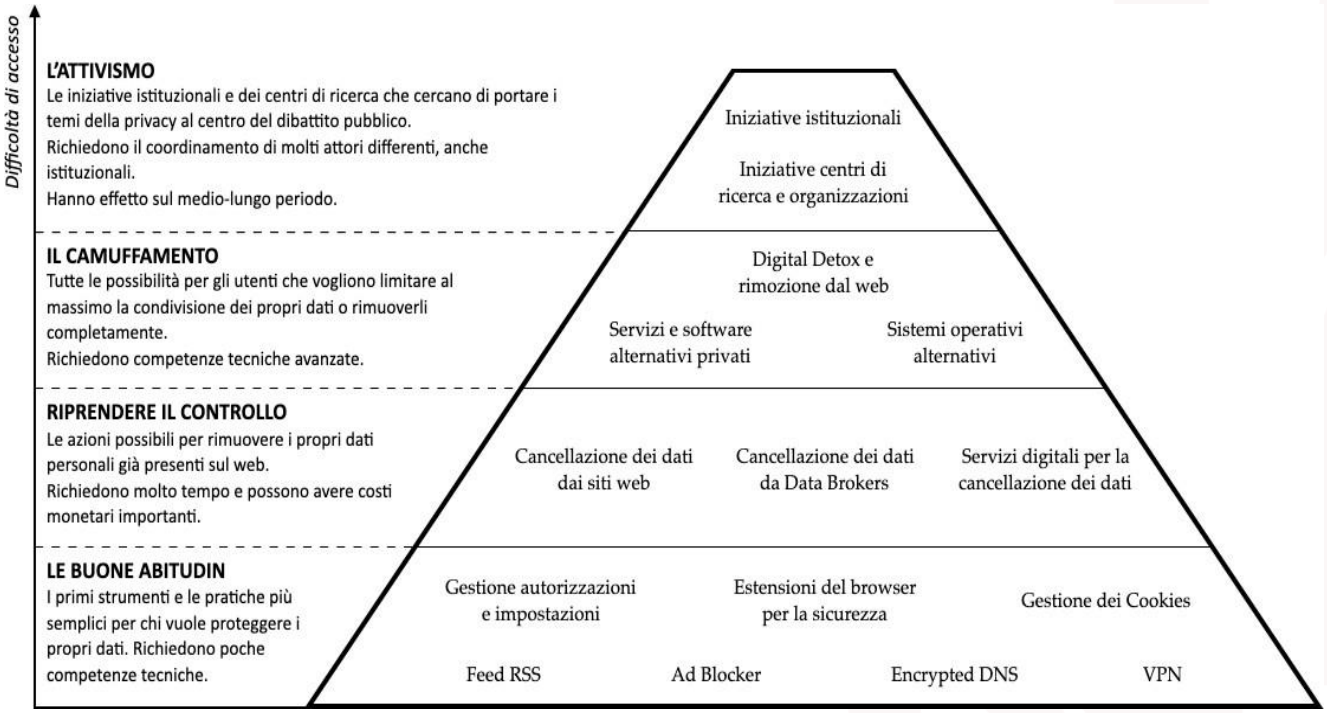
del monitoraggio e la sicurezza dell'ambiente economico e sociale in cui questo monitoraggio viene implementato.

Infatti, se è vero che il monitoraggio online è ormai un fatto accertato e noto ai più, non è altrettanto vero che i singoli utenti sono consapevoli di cosa stanno condividendo, con chi, come vengono utilizzati i dati raccolti e per quanto tempo verranno conservati. Né tantomeno viene sempre garantito il controllo di questi dati, inteso come la capacità dell'utente di rimuovere i propri dati dalla disponibilità di chi li sta raccogliendo. Chiaramente la bassa attenzione al tema della protezione dati non deriva necessariamente dall'attuale impotenza dell'utente in questo mercato, ma potrebbe essere conseguenza della complessità (e tediosità) della materia, della velocità con cui si evolvono le pratiche di monitoraggio o semplicemente da un'ignoranza diffusa su questi temi[3]. Di queste tematiche e del rapporto tra individui, dati personali, economia e sfruttamento si è occupata la sociologa Shoshana Zuboff, che coniando il concetto di surveillance capitalism, ha dato il via ad un filone di ricerche che indaga le caratteristiche di questo fenomeno e le sue ricadute sulla società.

Al fine di provare a colmare le asimmetrie di potere e di informazione tipiche del capitalismo della sorveglianza, il presente report introduce e descrive diverse pratiche tecno-sociali di resistenza al capitalismo della sorveglianza – utili a chiunque, non solo intenda saperne di più circa l'argomento, ma voglia anche provare (per quanto possibile) ad opporvisi. Il report, infatti, descrive una lunga serie di pratiche digitali quotidiane utili a limitare gli effetti del capitalismo della sorveglianza sugli individui e sulla società nel suo complesso. Tali pratiche vengono raggruppate in 4 macrocategorie principali: a) *le buone abitudini*; b) *riprendere il controllo*; c) *il camuffamento*; d) *l'attivismo* (vedi Infografica qui sotto) – (che si distinguono per crescenti gradi di sforzo e competenze richieste all'individuo per poter essere messe in atto[4]).
Al di là dei suoi risvolti pratici, il report si rivela anche utile per mettere in prospettiva alcuni discorsi di marketing, entrati ormai nell'immaginario comune, che vorrebbero *privacy* e *data protection* come concetti dati per 'morti', ormai obsoleti nell'odierna società digitale e di scarso interesse per il grande pubblico. Viceversa, come dimostra il report, non solo gli utenti comuni hanno a disposizioni una vasta pletora di strumenti e strategie per resistere al capitalismo della sorveglianza, ma anche che tali strumenti e

[3] Cigi-IPSOS, Internet Security & Trust, 2019, (https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%206%20Cross-border%20Data%20Flows.pdf).
[4] La logica di tale tassonomia è ispirata da Beraldo, D. & Milan, S. (2019). From data politics to the contentious politics of data. *Big Data & Society*, 6(2), https://journals.sagepub.com/doi/full/10.1177/2053951719885967.

strategie sono largamente praticati da ampie fasce della popolazione (es., si veda il crescente ricorso che gli utenti fatto di AdBlocker e VPN).



Pratiche tecno-sociali di resistenza a capitalismo della sorveglianza

Per dare un ordine all'insieme di soluzioni possibili per difendere i propri dati online può essere utile utilizzare come parametro principale proprio lo "sforzo" che viene richiesto all'individuo (o a gruppi di individui) per accedervi.
In questo modo possono essere create quattro categorie principali:

- La prima categoria, che ho chiamato "*Le buone abitudini*", raggruppa tutte le soluzioni a disposizione dell'utente per cercare di limitare il più possibile la condivisione dei propri dati durante l'utilizzo quotidiano del web. Sono pratiche facilmente accessibili alla maggior parte degli utenti e con costi limitati.
- Nella seconda categoria, "*Riprendere il controllo*", ci sono le diverse azioni possibili per far sì che i propri dati, per quanto possibile, vengano rimossi dal web o dalla disponibilità di chi li ha raccolti. Queste azioni spesso possono avere dei costi monetari importanti e richiedere tempi di attesa molto lunghi, generalmente sono poco conosciute dall'utente medio.
- La terza categoria è "*Il camuffamento*", in cui si trova l'insieme di pratiche volte a staccarsi definitivamente dal web mainstream attraverso l'utilizzo di sistemi operativi, software e app alternativi e focalizzati sulla privacy dell'utente. Perseguire questo obiettivo è certamente difficile considerando la competenza tecnica richiesta per l'utilizzo di alcuni di questi software e le difficoltà che possono crearsi quando si utilizzano servizi digitali poco diffusi.
- Infine, la categoria "*Attivismo*" contiene le iniziative istituzionali e private che si propongono di influenzare l'opinione pubblica su questi temi attraverso attività di educazione, sensibilizzazione e denuncia. Per loro natura sono delle pratiche che richiedono la partecipazione di molte persone sia per essere introdotte, sia per avere un riscontro effettivo nella società.

1. Le buone abitudini

Data la pervasività della raccolta dati attraverso internet e la molteplicità di canali attraverso cui avviene, le pratiche presentate in questo paragrafo non si riferiscono alla sola navigazione web attraverso il browser, ma riguardano dispositivi molto diversi tra loro, che vanno dal laptop allo smartphone. I dati che vengono protetti possono essere demografici, biometrici, di posizione e comportamentali.

Nonostante comportino alcune accortezze, sono pratiche abbastanza semplici da implementare nella propria vita quotidiana sul web, e spesso la scarsa attenzione che viene loro riservata dipende piuttosto da una scarsa conoscenza delle opzioni sulla privacy presenti nei nostri dispositivi.

1.1 Gestione delle autorizzazioni e controllo delle impostazioni sulla privacy dei dispositivi e servizi digitali

Il primo passo per avere il controllo sui propri dati sul web consiste proprio nel prendere consapevolezza di quali siano i dati che vengono condivisi con il dispositivo o il servizio con cui stiamo interagendo e limitarli in base alla volontà dell'utente. La maggior parte dei servizi e degli strumenti con cui interagiamo attraverso il web consentono agli utenti di decidere tra vari livelli di condivisione di dati durante l'utilizzo di quello specifico servizio o dispositivo, nonostante ciò, spesso queste impostazioni vengono trascurate e lasciate sui valori predefiniti, che chiaramente il più delle volte permettono la più ampia raccolta dati possibile. Chiaramente in base al dispositivo utilizzato, gli utenti possono scegliere tra opzioni diverse riguardanti la loro privacy. Ad esempio, dalle impostazioni di un dispositivo mobile si potrebbe decidere quali permessi rilasciare alle singole app, consentendo o meno l'accesso al microfono o alla fotocamera, dalle impostazioni di un browser web invece si potrebbe decidere come gestire i cookies durante la navigazione.
In sostanza, ogni dispositivo e servizio digitale garantisce alcune possibilità di personalizzazione, ed ognuna di queste diventa importante ai fini della protezione dei dati dell'utente. Non basta preoccuparsi solamente delle impostazioni del proprio dispositivo, ma bisogna acquisire l'abitudine di controllare le impostazioni della privacy ogni qualvolta si accede, si utilizza o ci si iscrive ad un nuovo servizio digitale, sito web o dispositivo.

Il più delle volte questi servizi richiedono all'utente di condividere dati demografici, come la sua età, dati di contatto come mail o numeri di telefono, dati comportamentali riguardanti l'utilizzo del dispositivo o gli interessi dell'utente, ricostruiti attraverso l'accesso ad ulteriori cartelle o app che possono permettere anche la raccolta di dati biometrici.
Per fare un esempio, consentire l'accesso alla fotocamera ad app come TikTok, permette la raccolta di dati biometrici che consentono di associare le reazioni di un utente al contenuto presentato in quel momento in modo da affinare ulteriormente l'algoritmo di presentazione dei contenuti[5].

[5] N. Wouters, J. Paterson, TikTok captures your face, in "Pursuit", 26 Luglio 2021, University of Melbourne (https://pursuit.unimelb.edu.au/articles/tiktok-captures-your-face).

All'interno di questo gruppo, come detto in precedenza, non rientrano soltanto i dispostivi e le app che vengono utilizzate dall'utente ma anche e soprattutto le impostazioni dei servizi digitali a cui siamo iscritti (es: Google, Amazon, Facebook). Le grandi aziende tech sono infatti gli attori più forti nel campo della profilazione degli utenti e limitare la quantità di dati condivisi con queste multinazionali è sicuramente il primo passo per opporsi all'attuale sistema di sfruttamento dei dati personali degli utenti.

1.2 Navigare sul web, il browser

La navigazione tramite browser genera una moltitudine di dati sull'utente e numerose occasioni per raccoglierli, per questo proteggere i propri dati mentre si naviga sul web diventa fondamentale tanto quanto l'attenzione alle impostazioni sulla privacy dei dispositivi. Utilizzando un browser senza le dovute precauzioni, alcuni dati personali come l'indirizzo IP o la cronologia di ricerca, possono facilmente essere raccolti da proprietari dei siti web che visitiamo, dai provider Internet, dai browser stessi e a volte anche da terze parti, se previsto dalle condizioni d'uso del software che stiamo utilizzando.

Data la complessità delle modalità di raccolta, per proteggere i propri dati gli utenti devono attuare strategie diverse tra loro. Tralasciando browser "speciali" come Tor, che verranno descritti successivamente, tutti quanti i browser più diffusi (Chrome, Safari, Firefox, ecc.) hanno una sezione in cui è possibile impostare le proprie preferenze in fatto di privacy. Ma non tutti trattano i dati dei propri utenti allo stesso modo ne permettono la stessa profondità di personalizzazione.

Figura 1 - Market share dei browser (Febbraio 2023).

Fonte: SimilarWeb

I browser, infatti, possono differire enormemente dal punto di vista delle limitazioni al tracciamento che implementano. Per comprendere meglio queste differenze esistono diverse possibilità online che si occupano di valutare la sicurezza dei browser registrando per ciascuno quali elementi traccianti vengono fermati e quali invece sono liberi di raccogliere i dati degli utenti. Alcuni presentano la comparazione tra i browser più diffusi, altri

strumenti permettono invece di eseguire un test sul proprio browser per valutarne la sicurezza[6].

Sul sito privacytests.org, l'importanza della scelta del browser in relazione di protezione dati è spiegata molto chiaramente: "*Your web browser is a likely route: browsers commonly leak data to third parties, revealing what web pages you have visited. This information lets tracking companies know what you read, what you write, where you are located, what you search for, and what you buy. And this highly personal information is assembled by those companies into detailed individual profiles of every person on the internet, containing data on your ethnicity, religious views, political views, sexual orientation, gender, family, friends, colleagues, health history, habits, relationships, educational records, income, and so on. These companies often retain your data for years or decades, and sometimes share it with third parties, including other companies or governments. Fortunately, most browser makers have acknowledged their responsibility to stop users' private information from leaking out. But the default behavior for browsers used by billions of people remains highly leaky*" (Fonte: privacytest.org).

Osservando i risultati del test sui quattro browser più diffusi (Chrome, Safari, Edge e Firefox) effettuato da questo sito, si nota facilmente che differiscono moltissimo per grado di protezione dei dati dell'utente e anche come il browser più diffuso sia anche quello meno rispettoso della privacy dell'utente. Diventa quindi chiaro come sia fondamentale essere consapevoli delle dinamiche di tracciamento già dal momento della scelta del browser. Oltre a questa scelta, le soluzioni a disposizione dell'utente per aumentare il grado di protezione dei propri dati personali sono diverse: la navigazione in incognito, il rifiuto o la gestione dei cookies di tracciamento, l'utilizzo di estensioni dedicate alla privacy come "Ad blocker" e altri strumenti più specifici, come l'utilizzo di RSS Feed focalizzati sulla privacy.

Un primo passo verso una maggiore protezione dei propri dati è l'utilizzo della modalità "Navigazione in incognito", un'impostazione presente in ogni browser. Questa modalità però, nonostante il nome evocativo, si limita a bloccare solamente alcuni degli elementi traccianti che si incontrano durante la navigazione web e, di per sé, non è molto efficace contro i metodi di monitoraggio più sofisticati.

Inoltre, la navigazione in incognito porta con sé i primi disagi per l'utente, ad esempio togliendo l'accesso automatico ai servizi digitali o l'auto

[6] Vedi https://privacytests.org & https://coveryourtracks.eff.org/

compilazione dei modelli, piccoli "fastidi" che, seppur a volte necessari, certamente possono scoraggiare e disincentivare un utente poco consapevole o interessato al tema della protezione dati.

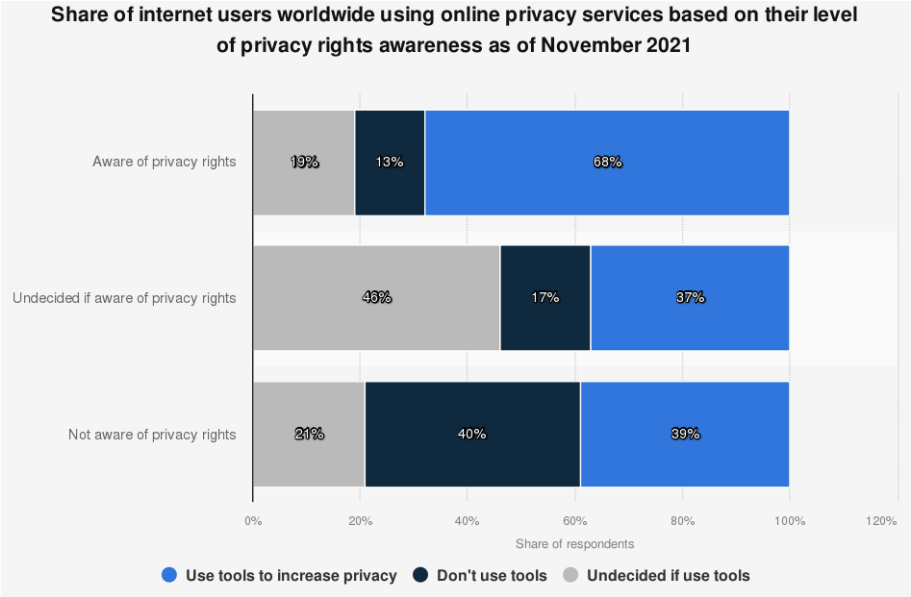


Grafico 2 - Statista, https://www.statista.com/statistics/1302406/security-tools-usage-based-on-privacy-rights-awareness-worldwide/

Tra gli elementi traccianti che incontriamo sul web ci sono i Cookies, ben noti a tutti gli utenti europei dopo che l'introduzione del GDPR[7] ha imposto a tutti i siti che utilizzano questi elementi traccianti di segnalarne la presenza all'utente e di permettere anche di rifiutare il tracciamento.
I cookies sono dei file di testo che vengono memorizzati sul dispositivo che si sta utilizzando quando si visita un sito web. Ne esistono di vari tipi e svolgono diverse funzioni, come ad esempio memorizzare gli accessi ad un sito web, ricordare qual è la lingua del sito preferita dall'utente o l'impostazione grafica che aveva scelto durante la sua ultima visita.

Ci sono però anche dei cookies che riescono a raccogliere altre informazioni e a ricostruire le abitudini che si ha sul web, fino a creare un profilo dettagliato contenente le sue abitudini, i suoi desideri e le sue inclinazioni. Questo set di informazioni viene poi utilizzato incrociandolo con altri dati come la geolocalizzazione per mostrare messaggi pubblicitari e contenuti che sono in linea con gli interessi degli utenti.

[7] Regolamento UE n. 2016/679 (GDPR).

Grazie ai vantaggi che garantiscono, i cookies sono stati certamente tra gli elementi più sfruttati per la raccolta di dati significativi su interessi e abitudini degli utenti.

Per difendere la propria navigazione da questo tipo di tracciamento è possibile proseguire in vari modi: molti browser, soprattutto se sviluppati con un focus sulla privacy, permettono di bloccare questo tipo di tracciamento o di cancellare periodicamente tutti i cookies dal proprio dispositivo, direttamente dalle impostazioni. A tutela dell'utente contro questo tipo di monitoraggio è intervenuta anche l'Unione Europea: dopo l'introduzione del GDPR, infatti, l'utilizzo dei cookies è stato finalmente regolamentato. Oggi ogni sito web che utilizza questo tipo di tracciamento su territorio europeo deve segnalare all'utente chi sta raccogliendo i dati, che tipo di dati sta raccogliendo e con quale scopo. Inoltre, all'utente deve essere garantita la scelta di rifiutare questo trattamento dei dati, negando l'utilizzo dei cookies non strettamente necessari al funzionamento del sito o servizio. Nella realtà dei fatti però, anche in UE operano ancora diversi siti che non rispettano queste indicazioni, sfruttando la vaghezza delle norme e la difficoltà d'implementazione di un sistema di controllo sul rispetto di questo regolamento.

Capita spesso così che l'utente si trovi di fronte richieste per la gestione dei cookies con grafiche poco chiare e confusionarie, che non permettono all'utente di compiere una scelta libera e consapevole rispetto al tracciamento che il sito vuole attuare. Per difendersi dai cookies e da altri tipi di tracciamento, la soluzione migliore potrebbe essere associare delle impostazioni del browser restrittive sul tracciamento ad estensioni dei browser stessi che siano focalizzate sulla privacy. Tutti i browser più diffusi infatti danno la possibilità di aggiungere estensioni di terze parti che svolgono le funzioni più varie, come per esempio salvare il testo di un articolo o gestire le proprie password di accesso ai servizi digitali. Tra queste, molte estensioni sono dedicate alla protezione dei dati di navigazione.
Un primo esempio sono gli ad-blocker e le altre estensioni contro il monitoraggio che limitano l'attività di profilazione bloccando i tracker e le pubblicità indesiderate. Pur essendo molto facili da installare sul proprio browser, esistono moltissime estensioni diverse che spesso promettono di fare cose simili. Per questo motivo, può capitare di scegliere un'estensione che teoricamente garantisce la protezione dei dati dell'utente durante la

navigazione ma che poi, nei fatti, potrebbe non funzionare come dovrebbe o addirittura essere dannoso[8].
Gli utenti meno esperti o attenti al momento della scelta dell'estensione, sicuri di aver aggiunto un layer di sicurezza alla propria navigazione, potrebbero facilmente ritrovarsi a navigare sul web senza essere al sicuro dal monitoraggio e la profilazione.

Come ultima cosa, quando si naviga sul web attraverso un browser si possono anche utilizzare strumenti e pratiche più avanzate e specifiche per garantire un maggior controllo sui propri dati.
Un esempio sono gli RSS feed, dei servizi digitali che mandano una notifica quando dei siti web scelti dall'utente vengono aggiornati, un servizio molto utile, ad esempio, per raggruppare in un unico posto gli aggiornamenti di siti web che trattano argomenti simili. L'utilizzo consapevole dei feed RSS è un buon esempio di come anche un servizio che non ha come scopo primario la protezione dei dati di un utente possa diventare uno strumento efficace anche in questo campo.
L'utilizzo di un RSS feed, infatti, può aiutare a contrastare il monitoraggio attraverso il riassunto dei contenuti di un sito web facendo si che l'utente non debba collegarsi ad ogni singolo sito web per verificare se sono stati pubblicati novi contenuti.
Avendo a disposizione un'anteprima dei nuovi contenuti, l'utente diminuisce il numero e la frequenza delle visite ai singoli siti web, concedendo così meno occasioni a questi ultimi per raccogliere dati sull'attività online dell'utente o dati personali.

Chiaramente anche l'utilizzo dei feed RSS può nascondere dei pericoli e delle difficoltà di cui bisogna sempre essere consapevoli quando si valuta un servizio digitale. Per prima cosa, non essendo servizi molto diffusi o trasversalmente utili, può capitare che l'utente abbia qualche difficoltà in più a conoscere, impostare ed utilizzare questo tipo di servizi.
Inoltre, come per tutti gli altri servizi digitali in questo ambito, pur limitando le possibilità di raccolta delle informazioni, alcuni RSS feed assieme ai servizi digitali a cui sono associati potrebbero a loro volta avere delle condizioni di utilizzo che prevedono la raccolta dei dati dell'utente, di fatto vanificandone gli sforzi. È quindi sempre buona norma, come nel caso degli ad-blocker, valutare attentamente le condizioni di utilizzo di questi servizi e quali dati richiedono per funzionare.

[8] H. Domanski, Google has kicked five malicious ad blockers off the Chrome Store, in "Tech Radar" 19 Aprile 2018 (https://www.techradar.com/news/google-has-kicked-five-malicious-ad-blockers-off-the-%20chrome-store).

1.3 Navigare sul web, gli strumenti avanzati
In questo paragrafo vengono analizzate brevemente le Encrypted DNS, le VPN, e gli altri strumenti che non hanno difficoltà di utilizzo rilevanti ma che è possibile utilizzare quotidianamente per proteggersi dalla raccolta dei dati online. Infatti, pur richiedendo qualche competenza in più rispetto alla scelta delle impostazioni sulla privacy o l'utilizzo della navigazione in incognito, utilizzare questi strumenti non richiede particolari competenze tecniche. D'altra parte, in alcuni casi questi strumenti possono avere un costo monetario che può trasformarsi in una barriera all'ingresso molto difficile da superare, soprattutto per gli utenti meno motivati.

Inoltre, è bene sottolineare che entrambi i servizi si basano sul coinvolgimento di terze parti che si frappongono tra l'utente ed il resto del web camuffandone alcuni elementi della navigazione, le VPN e i provider di DNS appunto. Risulta quindi fondamentale trovare delle aziende che garantiscano la più ampia privacy possibile nel trattamento dei dati dell'utente, per non rischiare che il servizio che dovrebbe proteggere dal tracciamento finisca semplicemente per sostituirsi agli attori da cui dovrebbe proteggere.

I due strumenti si differenziano moltissimo tra loro, ad esempio mentre l'utilizzo di una VPN potrebbe rallentare la navigazione, l'utilizzo di DNS crittografate influenza meno la velocità della connessione. Al contempo però il grado di protezione garantito dalle VPN è maggiore rispetto al solo utilizzo di DNS crittografate.

Le DNS, infatti, sono dei protocolli che traducono i nomi dei domini con cui gli utenti possono raggiungere un sito (es: microsoft.com) in indirizzi IP numerici che servono al computer per trovare il sito web. I provider di DNS crittografate garantiscono di proteggere i dettagli sulla navigazione dell'utente crittografando i nomi dei domini web che l'utente vuole raggiungere e promettendo di non utilizzarli per costruire dei profili digitali sulle abitudini e gli interessi dell'utente stesso. Alcuni provider DNS che non garantiscono ciò possono infatti facilmente costruire il profilo delle abitudini una persona attraverso la sua posizione geografica, i siti visitati e i time-stamps delle richieste web effettuate.

Per modificare le DNS, un utente può affidarsi sia alle impostazioni del WiFi sul dispositivo utilizzato, sia direttamente dalle impostazioni del router utilizzato. In alternativa o nel caso di reti mobili si può ricorrere a software che forniscono questo servizio senza doverlo impostare manualmente, facendo attenzione

alle condizioni di utilizzo. Infine, alcuni browser hanno la possibilità di utilizzare dei protocolli DNS crittografati già integrata nelle impostazioni.

Le VPN (Virtual Private Networks) invece consistono in un insieme di server su cui far passare il traffico di un utente prima di inoltrarlo sul web. Sono uno strumento molto efficace per camuffare il traffico di un utente, proteggerlo e renderlo anonimo.
Oltre a proteggere i dati dell'utente da potenziali attacchi crittografandoli, le VPN sono un valido strumento contro il monitoraggio online sia perché non permettono agli inserzionisti o agli ISP (Internet Service Provider) di accedere alla cronologia dell'utente sia perché sostituiscono l'indirizzo IP dell'utente con quello del server VPN, rendendo impossibile risalire alla posizione geografica del dispositivo che ha inviato la richiesta.
Le VPN pur essendo uno strumento molto efficace possono presentare degli svantaggi. Per prima cosa instradare il traffico attraverso i server delle VPN appesantisce la navigazione rendendola più lenta, soprattutto nel caso in cui non si disponga di una buona connessione. In secondo luogo, le VPN che garantiscono la protezione dei dati senza poi sfruttarli a loro volta nella compravendita con gli inserzionisti pubblicitari, nella quasi totalità dei casi sono a pagamento.

Infine, è interessante notare come le VPN siano tra gli strumenti più utilizzati da chi vuole proteggere la propria attività online[9], ma, nonostante ciò, spesso questi servizi vengono sponsorizzati come mezzi per poter accedere a servizi digitali di altri paesi e non come uno strumento per proteggere il proprio traffico online. Un segnale che probabilmente sia ancora vantaggioso a livello di marketing investire sulla loro voglia di consumo piuttosto che sulla volontà di tutelare i propri dati.

[9] Vedi Grafico 3.

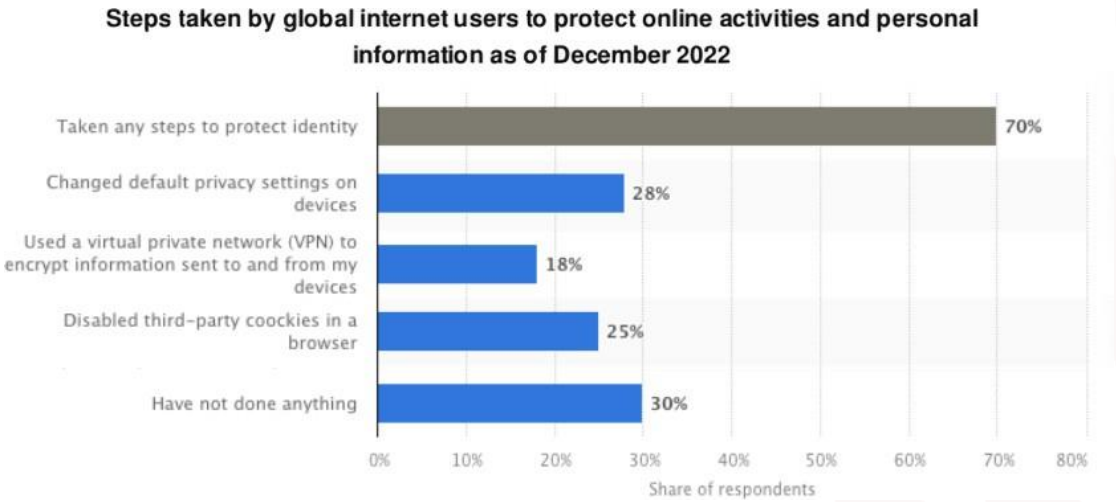


Grafico 3 - Statista, https://www.statista.com/statistics/617422/online-privacy-measures-worldwide/

1.4 Le difese "analogiche"

In quest'ultima categoria rientrano invece tutte quelle pratiche che piuttosto di limitare la condivisione dei dati mirano ad "inquinarli" in modo da generare profili di consumo poco precisi.
L'esempio principale è l'utilizzo di uno stesso account per più persone differenti. Le differenze di utilizzo di due o più persone che hanno uno stesso profilo, generano infatti delle incongruenze nei dati raccolti che potrebbe rendere la profilazione molto più complessa e imprecisa.

Riassumendo, tutti gli strumenti fin qui descritti possono contribuire a proteggere i dati degli utenti, ma devono essere utilizzati congiuntamente per garantire all'utente comune un buon grado di protezione sul web. Tutti questi strumenti concorrono infatti affinché le impostazioni sulla privacy di dispositivi e servizi online utilizzati siano state scelte dall'utente il browser web attraverso cui si accede ad internet sia sicuro e disponga delle estensioni necessarie a bloccare il monitoraggio.
la connessione alla rete internet sia protetta e sicura.

Per un utente standard le pratiche e gli strumenti riassunti in questa sezione potrebbero quindi essere più che sufficienti per limitare la dispersione dei propri dati personali senza richiedergli particolari risorse o competenze tecniche.

2. Riprendere il controllo

In questa sezione sono invece raggruppate tutte le azioni che è possibile fare per richiedere la rimozione dei i propri dati personali dal web.
Prima di elencare le possibilità a disposizione dell'utente in questo senso è importante ricordare che questo processo non ha garanzia di successo per svariati motivi.
Per prima cosa, seppure sia possibile richiedere che i propri dati vengano rimossi da un sito web o un servizio, non esiste garanzia che questi dati non siano stati copiati e archiviati in altri server o database, condivisi tramite Social Network o siano ancora presenti nelle copie dei siti web che vengono conservate dai motori di ricerca. Inoltre, nonostante questo limite sia già difficile da superare di per sé, il vero ostacolo per chi volesse eliminare la sua presenza dal web sarebbe quello di mappare e ricordare tutti quanti i servizi digitali, siti, social network a cui è stato iscritto, contattarli e richiedere l'eliminazione dei propri dati personali tramite le modalità specifiche stabilite da ognuno di questi attori.
Infine, va anche tenuto in considerazione che oltre all'Unione Europea non ci sono paesi o federazioni che abbiano creato leggi a tutela della privacy dell'utente che siano paragonabili al GDPR per quanto riguarda il diritto di cancellazione. Negli USA, ad esempio, la cancellazione dei propri dati online è garantita solamente in casi specifici grazie a leggi statali e sentenze, e non esistono regolamentazioni federali.
Gli strumenti a disposizione dell'utente descritti in questa categoria sono quindi possibili all'interno dell'Unione Europea grazie al GDPR, ma non sono probabilmente garantite in altre parti del mondo. Infine, va anche ricordato che esistono dei casi specifici in cui chi possiede i dati non è tenuto a dare seguito alla richiesta dell'utente[10].

Gli attori che vengono coinvolti da una richiesta di cancellazione dei dati possono essere divisi in due macro-gruppi, in base il primo contiene i siti web e servizi digitali che conosciamo tutti, compresi e-commerce, social network, blog, e via dicendo. Il secondo è invece il gruppo dei data brokers, delle aziende che si occupano di aggregare i dati degli utenti da svariate fonti pubbliche per poi metterli sul mercato.

2.1 Siti Web, social network e servizi digitali

Per prima cosa gli utenti possono richiedere ai siti web e ai servizi digitali di cancellare informazioni su dati personali e dati di contatto come mail o

[10] art.17, p.3, Regolamento UE n. 2016/679 (GDPR).

numeri di telefono. È possibile richiedere la rimozione di questi dati sia attraverso una richiesta fatta direttamente al titolare del sito web sia richiedendo la deindicizzazione di questi contenuti a Google stessa.
La prima strada chiaramente comporta la ricerca dei contatti del titolare del sito, a cui l'utente dovrà fare richiesta di cancellazione dei dati. Può capitare che queste richieste richiedano parecchio tempo per essere soddisfatte, sia per la difficoltà a reperire i contatti di una specifica azienda e far sì che dia seguito alla richiesta sia, per i rallentamenti dovuti ai casi in cui si creino diatribe legali a seguito del rifiuto di cancellare i dati da parte dell'azienda o sito web.

La seconda strada invece, evita che l'utente debba rivolgersi direttamente al titolare del sito web coinvolgendo direttamente Google o gli altri motori di ricerca.
In questi casi i dati che possono essere rimossi sono i dati riguardanti un individuo presenti su pagine pubbliche indicizzate dal motore di ricerca. Tramite una procedura di richiesta online al motore di ricerca si può richiedere la cancellazione di tutta una serie di contenuti che vanno dalle immagini personali intime non consensuali fino alle informazioni che consentono l'identificazione personale di un individuo. Percorrendo questa strada però le informazioni non vengono effettivamente rimosse dal sito web, il motore di ricerca si limita a rimuovere il contenuto o la pagina su cui è stato pubblicato dai suoi risultati, deindicizzandolo. È quindi uno strumento adatto a chi non vuole che vengano diffuse informazioni o materiali specifici riguardanti la propria persona, piuttosto che per rimuovere i propri dati dalla disponibilità dei servizi web che li hanno raccolti.

Infine, tra i vari siti su cui può essere fatta una richiesta di cancellazione online, è bene citare anche quei siti specificatamente creati per la ricerca di informazioni personali, che sono anche una sottocategoria dei data brokers. Esistono infatti siti come Spokeo o Whitepages[11] che raccolgono e aggregano le informazioni pubbliche sulle persone per permettere la ricerca di informazioni personali e di contatto ad altri utenti. Naturalmente, è possibile richiedere la rimozione dei propri dati personali direttamente dal loro sito web, ma ognuno richiede una procedura specifica.

2.2 Data Brokers
I data brokers sono delle aziende che raccolgono i dati personali degli individui a scopo di profilazione, principalmente per rivenderli a terze parti che li sfruttano in vari modi, principalmente in ambito commerciale e

[11] Vedi https://www.spokeo.com/ & https://www.whitepages.com/ .

pubblicitario. Queste aziende ricercano informazioni sugli utenti da svariate fonti come archivi pubblici e social network, riuscendo a ricostruire dei profili molto accurati contenenti dati personali, dati di contatto e informazioni relative ad interessi o abitudini d'acquisto ricavati dai dati di navigazione. Oltretutto, l'esistenza ed il ruolo dei data brokers spesso non sono noti agli utenti, che il più delle volte sono totalmente inconsapevoli che le loro informazioni siano in vendita in questo modo e per questo Per poter agire contro questo tipo di attori esistono due strategie differenti.
Prima però di procedere con la richiesta di cancellazione, è necessario capire quali data brokers posseggono i propri dati. Esistono per questo motivo dei servizi online che facilitano e velocizzano le richieste di accesso ai data brokers, in modo da sapere se i propri dati personali sono nei loro database e, nel caso ci fossero, di quali data broker specifici.

Una volta a conoscenza di chi possiede i dati, le possibilità per l'utente sono due: la prima, come per i siti web, consiste nell'attivare personalmente le procedure per la cancellazione dei propri dati facendo singolarmente richiesta ad ogni data broker coinvolto. Va considerato però che questa è sicuramente una scelta molto impegnativa, in quanto richiede moltissimo tempo per seguire ogni procedura. Per ovviare a questo problema, la seconda via consiste nell'affidarsi a servizi a pagamento specializzati in questo campo, come ad esempio DeleteMe o Privacy Bee[12], che si occupano specificatamente di portare avanti le richieste di cancellazione degli utenti ai diversi data brokers.

[12] Vedi https://joindeleteme.com/ & https://privacybee.com/ .

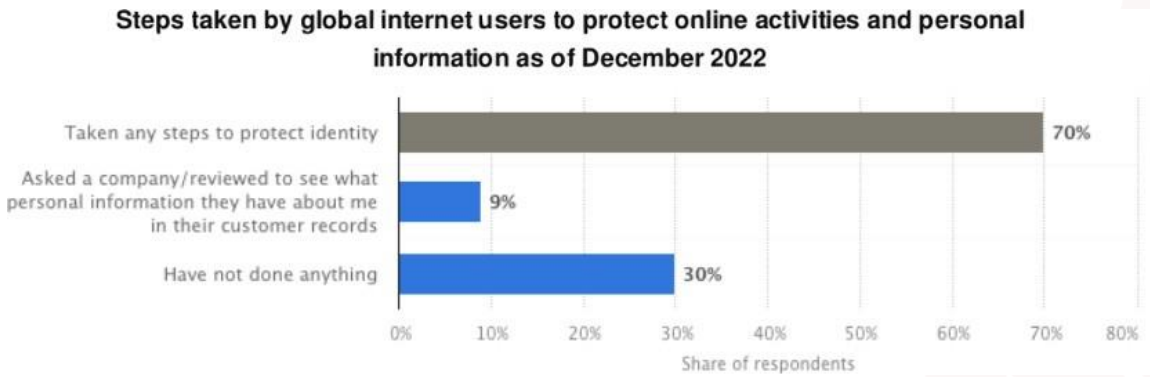


Grafico 4 - Statista, https://www.statista.com/statistics/617422/online-privacy-measures-worldwide/

In entrambi i casi, le procedure per l'eliminazione dei propri dati personali dal web sono sempre molto impegnative e richiedono tempo e risorse agli utenti, sia per individuare i propri dati e chi li possiede sul web, sia per presentare e vedere accettata la propria richiesta di cancellazione dei dati. Tutto considerato quindi, queste soluzioni sono adatte soprattutto a chi non vuole che dei contenuti specifici e particolarmente dannosi vengano diffusi su internet. Coloro che desiderano proteggere la loro navigazione quotidiana senza dover necessariamente essere profilati da qualcuno, potrebbero ricorrere a queste soluzioni solo come punto di partenza per la creazione di un'identità online rinnovata, consapevoli però che le informazioni rimosse dai siti web e i data brokers potrebbero essere ancora presenti su server e database remoti o su dispositivi privati.

3. Il camuffamento

Fin qui la protezione e la rimozione dei propri dati personali dal web sono stati presentati come obiettivi raggiungibili attraverso soluzioni più o meno accessibili a tutti. Ogni utente può impegnarsi ad avere una maggior cura di ciò che condivide online e con chi, ma per come è strutturato il web in questo momento storico, difficilmente riuscirà a mettersi totalmente al riparo dalla raccolta dati che avviene quotidianamente.

Questo perché il web ed i servizi digitali che conosciamo oggi non potrebbero esistere senza il valore economico generato dal monitoraggio degli utenti a fini promozionali e commerciali. Di conseguenza, molti dei servizi a cui siamo abituati, sono ottimizzati in modo da garantire delle esperienze d'uso sempre più veloci ed immediate grazie all'utilizzo dei dati dell'utente condivisi con il servizio. Per fare un esempio Google Maps non avrebbe la stessa utilità se non potesse accedere alla posizione dell'utente.

Per questo motivo, chi desiderasse di allontanarsi il più possibile dal processo di raccolta dati si troverebbe di fronte a due possibilità: trasferire la propria attività online su app, software e sistemi operativi sviluppati nel rispetto della privacy dell'utente o smettere di essere attivo e sfruttare il web.

Entrambe le possibilità sono molto gravose per un utente abituato alle comodità garantite dai servizi digitali odierni. Dovrebbe ad esempio rinunciare alla praticità di alcuni strumenti digitali molto comodi nella vita quotidiana, limitare fortemente gli acquisti fatti tramite e-commerce come Amazon o abituarsi ad una navigazione più lenta con un browser che deve crittografare i dati prima di inviarli sul web. Infine, a seguito di una scelta così drastica potrebbero esserci conseguenze anche nella vita sociale al di fuori di internet, si pensi ad esempio all'importanza per un adolescente o per un giovane adulto di poter consumare gli stessi contenuti dei coetanei o frequentare gli stessi ambienti digitali. In conclusione, considerando gli ostacoli esistenti, la scelta di minimizzare la condivisione dei propri dati personali online e anonimizzare il più possibile il proprio traffico web potrebbe essere attraente solo per chi è particolarmente sensibile a questi temi e mosso da motivi ideologici.

Si può però ipotizzare che se questi comportamenti si diffondessero nella società, il web dovrebbe necessariamente cambiare radicalmente per adattarsi alle nuove esigenze e desiderata degli utenti.
Nella pratica, per limitare al massimo la condivisione dei propri dati online ci sono tre possibilità, ognuna più radicale rispetto alla precedente.

3.1 Utilizzare servizi digitali, app e software alternativi
Di questo primo gruppo avevamo accennato nella sezione dedicata al browser web e include i software e servizi che hanno un focus sulla protezione dei dati degli utenti e che si possono utilizzare ogni giorno in sostituzione dei servizi digitali più comuni. Esistono infatti moltissime alternative ad ognuno degli strumenti digitali che utilizziamo ogni giorno, e spesso sono software open source sviluppati appositamente per soddisfare l'esigenza di protezione degli utenti.

Un primo esempio è dato dai browser web alternativi. Come abbiamo accennato in precedenza esistono molti browser che, rispetto a quelli più diffusi, sono progettati specificatamente per proteggere la navigazione dell'utente. Il più celebre è certamente Tor, un browser che per anni ha avuto una reputazione negativa dovuta al fatto che da sempre viene associato al "deep web", il nome con cui si indica la parte di internet non indicizzata dai motori di ricerca, nota all'opinione pubblica per dare agli utenti la possibilità

di entrare in contatto contenuti pericolosi o attività criminali. In realtà però questo browser non è stato progettato specificatamente per l'accesso a questa parte del web, bensì semplicemente per anonimizzare la navigazione dell'utente crittografando i dati con un protocollo chiamato "onion Routing". Il lato negativo di utilizzare questo browser consiste nel fatto che questo tipo di crittografia comporta un calo nelle prestazioni.

Oltre al browser, esistono alternative rispettose della privacy anche per altri servizi digitali. Tra questi ci sono provider di indirizzi e- mail, software e app di messagistica istantanea, mappe online, office suite, motori di ricerca, social media e storage su cloud. Generalmente sono software open source che garantiscono la massima trasparenza in fatto di privacy permettendo agli utenti di accedere al codice del software stesso.
Nei siti dedicati ai temi privacy è facile trovare delle liste di strumenti contenenti valide alternative alla maggior parte dei servizi online tradizionali[13].

In questa categoria rientrano anche tutti gli strumenti per rendere anonime le transazioni economiche sul web, utili per nascondere i dati di pagamento di un utente in modo da rendere più difficile il tracciamento delle sue abitudini d'acquisto. Ci sono due strumenti a disposizione dell'utente in questo caso: le criptovalute o le carte di pagamento virtuali.

Le criptovalute[14] sono un sistema di pagamento basato sulla tecnologia blockchain di cui si è discusso molto negli ultimi anni, soprattutto in relazione alle fortissime fluttuazioni del valore di alcune di queste cryptocurrencies sul mercato finanziario. Essendo una tecnologia nuova e poco regolamentata, non tutti quanti i servizi digitali permettono però di pagare con questa valuta. Uno strumento che invece può essere utilizzato facilmente sono le carte di pagamento virtuali, delle carte anonime, solitamente usa e getta, che possono essere usate in sostituzione propria carta per fare acquisti online.

Tutti i servizi digitali e gli strumenti elencati hanno però delle criticità se confrontati alle controparti più diffuse sulla base della sola comodità d'uso. La condivisione dei dati personali ha infatti permesso la creazione di funzionalità aggiuntive a cui può essere difficile rinunciare. Inoltre, la difficoltà ad emergere di alcuni di questi servizi potrebbe dipendere dalla minore capacità di investimento rispetto ai servizi delle grandi compagnie tech.

[13] Vedi https://www.privacytools.io/ .
[14] The idea and a brief history of cryptocurrencies, in "Guardian Nigeria", 26 dicembre 2021, (https://guardian.ng/technology/tech/the-idea-and-a-brief-history-of-cryptocurrencies/).

Resta infine da sottolineare che il passaggio a questo tipo di servizi può risultare difficile anche a causa della varietà di proposte disponibili sul web e la velocità con cui possono cambiare le condizioni d'uso dei singoli servizi digitali. Per mantenere il livello di privacy scelto, è necessario quindi controllare periodicamente quali servizi digitali si stanno utilizzando e se tra questi ci sono stati aggiornamenti alle condizioni di utilizzo che ne pregiudicano la sicurezza.

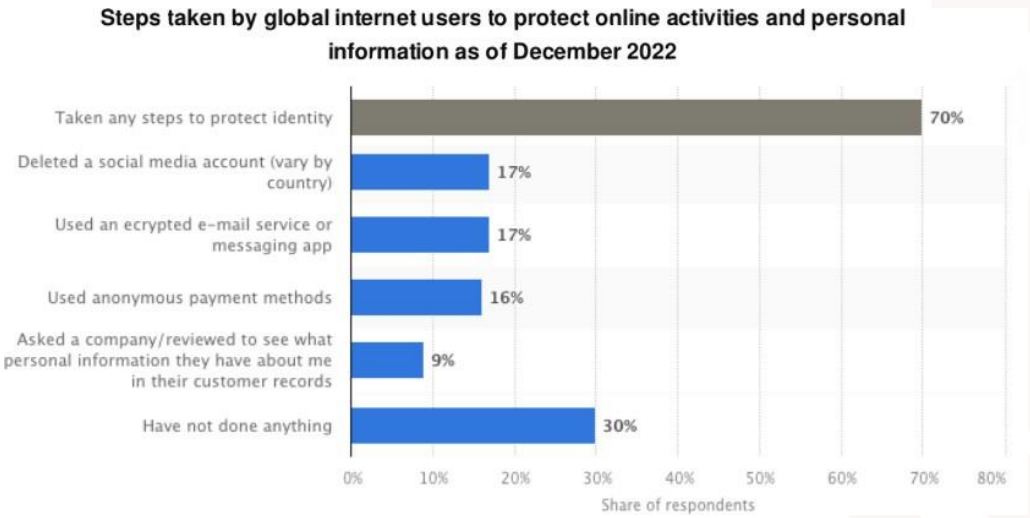


Grafico 5 - Statista, https://www.statista.com/statistics/617422/online- privacy-measures-worldwide/

3.2 Sistemi operativi alternativi

Il passo successivo per aumentare la sicurezza della propria navigazione consiste nel sostituire i sistemi operativi predefiniti dei vari dispostivi con alternative più focalizzate al rispetto della privacy dell'utente.
Esistono infatti alcune soluzioni sia per i dispositivi mobili che per i computer che possono essere utilizzati per aumentare ancor di più il controllo dei propri dati.

Nel caso dei pc e dei laptop esistono da sempre sistemi operativi sviluppati per poter essere utilizzati da chi si trova nella necessità di rimanere anonimo, come nel caso dei giornalisti d'inchiesta o attivisti, che garantiscono la massima protezione per ogni informazione condivisa tramite internet.
In questo campo Linux è il sistema più utilizzato e molte distribuzioni di questo sistema operativo sono sviluppate focalizzandosi sulle esigenze di privacy degli utenti[15].

[15] Tails (https://tails.boum.org/index.it.html).

Anche per dispositivi mobili sono stati sviluppati sistemi operativi con lo stesso obiettivo. Sulla base del sistema operativo Android, ad esempio, sono state sviluppate diverse alternative che rimuovono tutte quante le fonti di tracciamento che normalmente sono presenti nel sistema operativo di proprietà di Google[16]. Questi sistemi operativi sono spesso accompagnati anche da App Store proprietari che, una volta installati, risparmiano all'utente la fatica di cercare i singoli file di installazione delle diverse app.

Va ricordato però che, ad oggi, questi sistemi operativi potrebbero diventare inutilizzabili o addirittura pericolosi, qualora fossero utilizzati da un utente senza le conoscenze tecniche adeguate. Oltre a ciò, è importante considerare che a differenza delle grandi compagnie tech, questi sistemi operativi spesso non dispongono di veri e propri servizi clienti o persone dedicate al supporto dell'utente, né possono garantire versioni compatibili con tutta la varietà di dispositivi disponibili sul mercato.
Infine, le conoscenze tecniche e l'impegno richiesti all'utente per utilizzare questi sistemi operativi non sono assolutamente trascurabili, soprattutto considerando la fase di installazione, che può richiedere competenze tecniche avanzate.
Tutto considerato, la complessità di utilizzo e installazione di alcune di queste soluzioni, la mancanza di una assistenza clienti paragonabile alle grandi aziende tech e la possibile incompatibilità di questi sistemi operativi con alcuni dispositivi, rimangono ostacoli difficilmente trascurabili che ad oggi impediscono la diffusione di questi prodotti tra gli utenti comuni.

3.3 Digital detox e rimozione dal web
La soluzione più radicale a disposizione dell'utente per proteggere i propri dati consiste nell'abbandono del web, temporaneo o permanente. Una soluzione che però è diventata quasi un privilegio, dato che abbandonare il web sarebbe possibile solo a chi non ha la necessità di utilizzarlo nella vita quotidiana, una condizione abbastanza rara nella società odierna.
Dopo la pandemia iniziata nel 2020 infatti, il lavoro da casa tramite internet è diventato sempre più diffuso e sembra che questa tendenza proseguirà anche nel prossimo futuro[17].

[16] GrapheneOS (https://grapheneos.org/).
[17] K. Parker, J.M. Horowitz, R. Minkin, How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work, Pew Research Center, 9 dicembre 2020, (https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work/).

L'abbandono temporaneo del web può essere una scelta legata a molteplici fattori come stress o dipendenza, e spesso ci si riferisce a questa pratica con l'espressione "Digital Detox". Come nel caso degli utenti che utilizzano le VPN con l'unico scopo di accedere a contenuti non disponibili nel proprio paese, chi inizia un periodo di digital detox potrebbe non essere spinto dal desiderio di proteggere i propri dati bensì semplicemente dalla volontà di eliminare una fonte di stress dalla propria vita. Nondimeno questo tipo di scelte su larga scala potrebbe avere degli effetti sul mercato dei dati online in quanto alcuni attori, come i data brokers, avrebbero più difficoltà nel costruire dei profili di utenti veritieri e vendibili.

La scelta più estrema, cioè l'abbandono del web, ai fini della privacy è chiaramente di per sé la più efficace, ma d'altro canto è chiaramente anche la meno attuabile.
Come già detto infatti, per la maggior parte delle persone è infatti impossibile immaginare una vita senza l'ausilio del web e degli strumenti che ci fornisce ogni giorno solamente in nome della privacy e del diritto a mantenere i propri dati personali privati. Oltre a ciò, rimane il problema che ancora una buona parte di chi utilizza Internet non ha consapevolezza del mercato che esiste grazie ai dati condivisi online da ciascuno degli utenti, e senza una consapevolezza più diffusa su questi temi sarà difficile che diventino centrali nel discorso pubblico e che venga regolata maggiormente la raccolta e compravendita dei dati generati dagli utenti.

4. L'attivismo

In questa ultima sezione si parlerà invece delle iniziative collettive che riguardano la protezione dei dati personali e il contrasto allo sfruttamento economico dei dati degli utenti online.

Se infatti questi temi sono poco conosciuti dagli utenti, sono invece affrontati sotto variegati punti di vista nel mondo accademico e dell'attivismo sociale. La volontà di sensibilizzare le persone ad impegnarsi per cambiare le attuali dinamiche di sfruttamento dei dati degli utenti è stata quindi tradotta in iniziative molto differenti tra loro che vanno dallo sviluppo di software e protocolli a supporto della privacy fino a siti deposito in cui vengono segnalati strumenti e modalità di protezione a disposizione dell'utente comune.

Le iniziative più comuni sono quelle che consistono nel creare centri di ricerca dedicati al tema della società algoritmica che svolgono ricerche in questo

campo per monitorare lo sviluppo delle tecnologie e della loro applicazione su Internet[18]. Possono essere delle iniziative di accademici e università, organizzazioni no profit o think tank specializzati sui temi relativi alle nuove tecnologie e la loro applicazione nella società.
In alcuni casi oltre alle attività di ricerca più svariate che possono essere fatte su questi temi, questi centri di ricerca e organizzazioni no profit si occupano anche di fare attività di sensibilizzazione su questi temi, organizzando eventi, webinar ed incontri dedicati. In altri casi sviluppano degli strumenti più pratici per educare, sensibilizzare ed informare gli utenti, come nel caso delle newsletter create sui temi della protezione dati e del monitoraggio[19] o delle guide alla protezione dei dati destinate agli utenti o alle aziende[20].
Infine, questi attori possono anche portare avanti iniziative che provino a sensibilizzare su questi temi con un approccio meno formale attraverso l'utilizzo di toni più leggeri, come nel caso di StealingYourFeelings[21], un sito web che, richiedendo l'accesso alla fotocamera del browser, riesce a spiegare all'utente in maniera semplice e divertente come a partire da alcuni dati biometrici è possibile creare dei profili personali da utilizzare per la targhettizzazione dei contenuti.

Altre iniziative che affrontano questi temi con un approccio più pratico forniscono agli utenti strumenti per risolvere alcuni dei problemi creati dalla difficoltà di mantenere l'anonimato su internet. Un esempio è Irpileaks, un'iniziativa per creare un canale di comunicazione sicuro potenzialmente utilizzabile da chiunque e completamente anonimo. L'obiettivo di questa iniziativa è quello di permettere a chiunque avesse bisogno di comunicare informazioni riguardo temi particolarmente delicati come la corruzione o la criminalità organizzata, di poterlo fare senza timore di ripercussioni e senza rischiare che la sua comunicazione venga tracciata.
Per fare un altro esempio possiamo citare Comuzi, un'iniziativa che ha portato alla progettazione di un cappello che confonde gli algoritmi per il riconoscimento facciale, oppure Hudi, un protocollo web per permettere all'utente di monetizzare parte del valore generato dalla compravendita dei suoi dati[22].

[18] Algosoc (www.algosocvacancies.org), Data Justice Lab (https://datajusticelab.org/), Surveillance Studio Network (https://www.surveillance-studies.ca/), Berkman Klein Center (https://cyber.harvard.edu/research/privacy_tools), Data Ethics (https://dataethics.eu), MyData (https://www.mydata.org/).
[19] Vedi Monitor di Hermes Center (https://www.hermescenter.org/it/monitor/).
[20] https://dataethics.eu/digital-selfdefense/ & https://www.privacytools.io.
[21] https://stealingurfeelin.gs/.
[22] Comuzi (https://www.comuzi.xyz/invisiblemask) & Hudi (https://humandataincome.com/).

Infine, esistono tutta una serie di iniziative istituzionali volte a diffondere consapevolezza su questi temi sia tra gli individui che tra le aziende o a creare policy, organi di controllo e leggi a tutela della privacy dell'utente sempre più adatta all'odierno ambiente digitale.
Come già accennato in precedenza, ad oggi nell'Unione Europea il diritto alla protezione dei propri dati personali è più tutelato che nel resto del mondo grazie al GDPR, un regolamento entrato nel 2018 che garantisce a tutti i cittadini europei di poter far valere i propri diritti in materia di tutela della privacy e protezione dei dati personali.
Altri paesi, come il Canada o gli Stati Uniti, hanno dei regolamenti e delle leggi che tutelano i dati personali e il loro utilizzo ma questo non sono assolutamente paragonabili al livello di garanzia fornito dal GDPR.
Tutto considerato comunque la situazione attuale a livello normativo sembra essere migliore rispetto al 2020, e la porzione di popolazione coperta da regolamentazioni sulla privacy sembra destinata ad aumentare31.

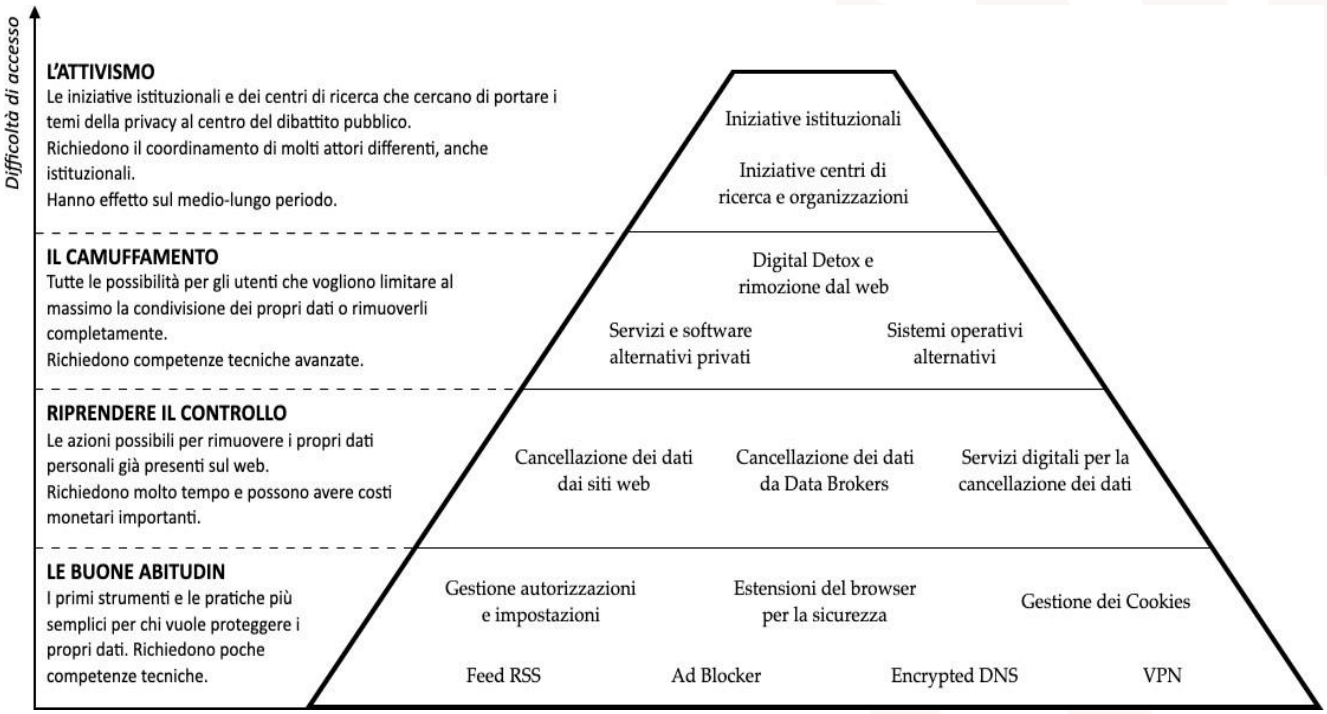


Figura 2 - Riassunto delle categorie e dei tool analizzati