*decentralizzat*e. Inoltre è utile usare password lunghe e un password manager[1].

Per mettere in pratica queste linee guida suggeriamo di usare software come questi:

Per messaggistica e telefonate: ***Signal*** **e** ***Matrix*** (decentralizzato)
Per navigare in internet: ***TOR***, ***Brave*** e ***Firefox***
Plug-in per il navigatore: ***Privacy Badger***, ***HTTPS Everywhere***
Servizi email criptati: ***Protonmail*****.com**, ***posteo.de***, ***tutanota.com***, ***mailbox.org***
Social networks distribuiti: ***Mastodon***, ***Diaspora***
Servizio di video decentralizzato: PeerTube (es. ***peertube.uno***)
Mappe off-line, basato su OpenStreetMap: ***OsmAnd***
Traduttore: ***Deepl.com***
Servizio di elaborazione e condivisione dati decentralizzato: ***Nextcloud***
Sistema operativo per personal computer: ***GNU/Linux***
Smartphones e computers con Google-Free Android e GNU/Linux: ***/e/***, ***puri.sm***, ***tuxedocomputers***
Sistema operativo Android, Google-Free: ***LineageOS***
Gestori di password: ***KeePass, Firefox Password Manager***
E tanto altro: ad es. ***leAlternative***
Frequentare i negozi della propria ***comunità,*** piuttosto che Amazon

Note

(**1**) https://protonmail.com/blog/
(**2**) https://it.wikipedia.org/wiki/ Persone_pi%C3%B9_ricche_del_mondo_secondo_Forbes
(**3**) Errore di Sistema. Edward Snowden, 2019. Longanesi.
(**4**) Tecnologie radicali. 2017, Piccola Bibliotca Einaudi.
(**5**) Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri. Shoshana Zuboff, 2019, Ed. Luiss University Press.
(**6**) http://www.rai.it/programmi/ report/
(**7**) https://it.wikipedia.org/wiki/ Free_and_Open_Source_Software

Versione estesa e aggiornata su miniguide.minifox.fr
Testo a cura di Francesco Reyes

Mini-Guida alla Protezione dei Dati Personali

per la tutela delle persone e della democrazia (Mag/2020)

Diffondersi della comunicazione digitale

Gli ultimi 20 anni hanno visto il diffondersi di tecnologie basate sulla connettività a internet, a partire dagli smartphone e le loro applicazioni: Whatsapp, Telegram, etc., servizi di posta elettronica, motori di ricerca, mappe, come Google-Search, -Mail e -Map, con i quali comunicare o cercare informazioni apparentemente a "costo zero".

In questo periodo, aziende come Facebook (proprietaria anche di Whatsapp e Instagram), Google e Amazon hanno raggiunto un numero esorbitante di clienti, maggiore di qualsiasi stato nazionale (fino a 2.5 miliardi nel caso di Facebook)[1].

"Costo zero"? Il business dei giganti Hi-Tech

Negli anni in cui la ricchezza globale si è andata concentrando in sempre meno mani, i proprietari dei giganti Hi-Tech sono diventati gli uomini più ricchi del pianeta[2]. Per fare un esempio, nel 2018 Google ha fatturato 136 miliardi di dollari, in media 91dollari per ogni suo utente Gmail.

Anche se i prodotti di queste aziende non richiedono un pagamento diretto in denaro, esse riescono ad estrarre enormi capitali dalla popolazione, attraverso la vendita di informazioni e profili comportamentali dei propri utenti ad altre aziende. Inoltre, più volte sono state documentate la cessione massiva di dati a governi[3] e la loro vendita illegale a società private[1].

Dati (e meta-dati) personali ceduti online

I dati raccolti mentre usate questi strumenti informatici possono includere ciò che si scrive nei messaggi o email, che si dice durante una telefonata, le proprie preferenze sessuali (es. Tinder), le pagine internet che visitiamo, gli

acquisti effettuati in forma digitale, i “like” su Facebook, i commenti lasciati su un blog.

Oltre questi dati viene raccolta anche una gran quantità di informazioni tecniche (chiamate “metadati”), che rivelano innumerevoli cose su di noi e il contesto in cui abbiamo comunicato. I metadati sono facili da analizzare in maniera automatica (con dei computer) allo scopo di conoscere abitudini di vita, relazioni e preferenze degli utenti. I metadati raccolti comprendono la rete dei vostri contatti, le persone che contattate di più e di meno, e quelle con cui non parlate per niente, la sequenza di persone che ha condiviso uno stesso messaggio su WhatsApp, i movimenti del dito o del mouse sullo schermo quanto visitate un sito internet dotato di cookies traccianti (la maggioranza dei siti usa i cookies di Google[1]), il tragitto descritto dal GPS del vostro telefono, il luogo in cui vi siete connessi a una rete Wifi[4,5], ….

I dati che abbiamo (involontariamente) ceduto non sono più i nostri, ma apparterranno ad un “nuovo proprietario” a tempo indeterminato, memorizzati in qualche datacentre[3,4].

Come può fruttare il business dei dati?

I dati raccolti contengono una descrizione dettagliata della società e dei rapporti tra i suoi membri, delle opinioni e posizioni politiche di ogni cittadino.

Gli utilizzi possibili di dati come questi sono numerosissimi. Visto il costo e le competenze necessarie a stoccare e analizzare questi dati, però, chi sfrutta realmente questa raccolta dati di massa sono generalmente le grandi multinazionali e i servizi segreti: le prime a fini di controllo di flussi economici[5], i secondi per controllo politico e manipolazione dell'opinione pubblica[3].
Tutto ciò avviene in modo quasi invisibile perché tramite sistemi tecnologici con cui noi utenti medi non abbiamo dimestichezza. Inoltre, la

verifica dei software da parte di specialisti è generalmente ostacolato da copyright o segreti militari[4].

Tra gli usi possibili di “dati di massa”, in ambito aziendale: battere la concorrenza grazie a una minuziosa conoscenza delle nostre vite, convincere l’utente ad acquistare certi prodotti con pubblicità mirate al singolo individuo, cambiare il prezzo di un prodotto sulla base del nostro profilo. In ambito governativo: adattare la propaganda politica agli umori della popolazione in modo da apparire sempre vincente, influenzare elezioni, fomentare o impedire rivolte, individuare e reprimere avversari politici, trafugare scoperte scientifiche[6].

Come tutelare i dati personali e quindi il sistema democratico

Non va affatto bene che poche aziende molto ricche possiedano ed utilizzino a proprio vantaggio le informazioni su ogni singola persona del mondo, se la popolazione mondiale non può decidere nulla sul comportamento di tali aziende. In un mondo in cui tanto delle nostre vite passa attraverso strumenti digitali, dovremmo evitare che tali informazioni sfuggano dalle nostre mani, essendo noi i legittimi proprietari delle nostre informazioni.

Il modo più sicuro per non cedere le informazioni personali è quello di non generarle (lasciando a casa telefono e computer, o togliendogli la batteria), ma senza spingerci a tanto, possiamo invece scegliere software molto più rispettosi della privacy.

In particolare è preferibile usare software 1) *free/open source:* il cui contenuto è verificabile in modo trasparente da altre persone[7], 2) che invii messaggi leggibili solo dal vero destinatario (usando la cosiddetta cifratura *“end to end”*), 3) che riduca al minimo i metadati memorizzabili da terze parti durante l’uso, 4) che non si appoggia ad un'unica azienda (dove la concentrazione di grandi quantità di dati possa attirare l’appetito di altre aziende o governi), ma usi standard aperti e condivisi su reti