RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0053

Data commons: privacy e cybersecurity sono diritti umani fondamentali

Arturo Di Corinto

Google sa di noi più cose di quante ne ricordiamo, conosce abitudini e percorsi quotidiani, sa con chi, quando e per quanto tempo siamo stati; Zoom sa con chi lavoriamo; Facebook mette all'asta le nostre preferenze; bot e troll su Twitter influenzano le nostre opinioni. Anche i meme della disinformazione affollano i social e inquinano il dibattito scientifico. Se non impariamo a proteggere i comportamenti trasformati in dati digitali saremo esposti a un potere incontrollabile, quello della persuasione commerciale, della manipolazione politica e della sorveglianza statuale.

Data commons – Privacy – GDPR – Cybersecurity – Big Tech

1. Introduzione

La privacy è come la libertà: se non gli dai valore, rischi di perderla. Già. Nonostante l'eco mediatica e gli interventi resi possibili dal nuovo Regolamento europeo generale sulla protezione dei dati, il GDPR, sono ancora in tanti, troppi, a non dare valore alla riservatezza dei propri dati personali anche se quei dati identificano comportamenti quotidiani e permettono di profilare gli utenti digitali indirizzandone scelte e azioni. E così, come dice lo storico Noah Yuval Harari «La gente è felice di elargire la propria risorsa più preziosa – i dati personali – in cambio di servizi di posta gratuiti e video di gattini. Un po' come è accaduto agli africani e agli indiani d'America che hanno venduto grandi territori in cambio di perline colorate»[1].

I dati sono l'oro e il petrolio dell'umanità connessa e dalla loro corretta gestione dipendono i gradi di libertà delle scelte quotidiane. E allora perché siamo pronti a darli via solo per partecipare a sonore litigate su Facebook, farci buggerare via email da rapinatori digitali e tracciare da poliziotti zelanti con app pensate per i criminali? La verità è che nella gestione della propria presenza online si rivela quel pericoloso divario digitale che ancora oggi, a 30 anni dal Web, riflette antiche disuguaglianze: tra chi è capace di controllare, difendere e rivendicare la tutela dei suoi dati e chi non è in grado di farlo.

Con gli smartphone *always on* e le app a prova di incapace abbiamo messo armi potentissime in mano ad adulti che si comportano come bambini che bisticciano, tifano, si mostrano crudeli verso gli altri, dimentichi di ogni forma di empatia. Questa ignoran-

A. Di Corinto insegna Identità digitale, Privacy, Cybersecurity nel Corso di laurea in Media, comunicazione digitale e giornalismo di Sapienza - Università di Roma.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

za digitale indirizzata dal mercato è il frutto di vari fattori: la diffusione su scala globale di *personal media* sempre più potenti, maneggevoli ed economici; un sapere comunicativo diffuso promosso da scuole e università; l'iperconnessione religiosa ai social; l'avvento della *me-communication*, la "comunicazione autoriferita", come la chiama il sociologo Manuel Castells[2]. Pilotata dai signori delle piattaforme che oggi sono i signori dei dati, l'ignoranza digitale ha generato un nuovo feudalesimo digitale[3], che divide il mondo in due, tra chi produce gratuitamente questi dati e chi li raccoglie e mette a profitto.

La raccolta, l'organizzazione e l'utilizzo dei dati sono al centro del capitalismo estrattivo delle piattaforme[4] che, conoscendo le più intime inclinazioni, il *sentiment*, dei propri utenti, sono in grado di anticiparne mosse e desideri affinché continuino a produrli. Elaborati da potenti algoritmi con le tecniche proprie delle scienze sociali (la psicometria), diventano il carburante per le intelligenze artificiali che ci sostituiranno (già in parte lo fanno) in compiti complessi per i quali una volta si veniva remunerati per sostenere intere famiglie.

La violazione dei dati realizzata da Cambridge Analytica per cui Facebook è stata multata – facendogli il solletico – rientra in questo schema: se conosco gli orientamenti politici del produttore di dati, e lo so in base ai like che ha messo, sarò in grado di cucirgli addosso un messaggio che non potrà rifiutare. Il messaggio andrà a rinforzare le sue convinzioni pre-esistenti e gli stenderà intorno un "cordone sanitario" affinché non acceda a contenuti che le possano mettere in discussione[5].

2. Il potere delle piattaforme

Google sa tutto di noi. Se facciamo una ricerca in rete Google sa che parola chiave abbiamo usato e se abbiamo cliccato o no sul banner pubblicitario di Adsense. Da quella semplice keyword sa se siamo preoccupati del Covid o se cerchiamo una clinica oncologica. Google sa che siti abbiamo visitato e se abbiamo usato il suo indirizzo Gmail per "loggarci" su un certo sito. Questo vale per i siti erotici come per l'accesso ai siti di giornalismo investigativo. Se la ricerca ci porta su Youtube è in grado di suggerirci i video da vedere favorendo i video simili a quelli che abbiamo già cliccato e presentarci dei contenuti razzisti anziché storie di solidarietà quotidiana.

Mentre navighiamo con il suo browser, Chrome, Google raccoglie le informazioni relative alla nostra permanenza su ciascun sito: sa da dove siamo partiti e dove siamo arrivati durante la nostra sessione di *web surfing*. Se però ce ne andiamo in giro, a piedi o in macchina, e usiamo Google Maps, saprà ancora più cose: da dove partiamo e dove andiamo, se quel percorso è ripetuto e frequente, quanto tempo ci mettiamo per arrivare e se ci siamo fermati a fare shopping presso un negozio identificato sulla mappa.

Queste informazioni che Google raccoglie incessantemente sono scritte con la penna, non con la matita, e sono destinate a rimanere archiviate per successive analisi di mercato. Google lo dichiara apertamente: tutte le informazioni che raccoglie su di noi servono a migliorare i suoi servizi e a produrre annunci e risultati personalizzati in base alle nostre ricerche, anche a favore dei suoi clienti.

In cambio di qualche comodità abbiamo così barattato la nostra privacy, quell'elemento della vita associata che ci permette di nasconderci all'occhio inquisitore degli altri garantendoci il diritto a essere imperfetti. È così che il diritto a non essere valutati e sorvegliati si ferma alle porte di Google. Perché Google sa di noi anche quello che non ci ricordiamo più: dove siamo stati, con chi, per quanto tempo, e quello che abbiamo fatto.

Google è una potenza il cui fatturato è superiore a quello di nazioni intere, ed è più avanti di molti governi nello sviluppo di computer quantistici e delle intelligenze artificiali che ci sostituiranno nel lavoro.

Anche Zoom ci spia. La piattaforma per videoconferenze tanto in voga durante la quarantena passa(va) le nostre informazioni a Facebook. WhatsApp, invece, ha chiesto agli europei di accettare in maniera esplicita la condivisione con la casa madre Facebook (oggi Meta), dei dati che generano usando l'app, se vogliono continuare a usare i suoi servizi generando una vasta levata di scudi. Fuori dell'Europa già lo faceva e continua a farlo. Niente di scandaloso, direte, lo stesso vale per altre app, siti e software che grazie ai dati generati dalle nostre interazioni creano profili statici e dinamici, singoli o aggregati, della nostra persona digitale, quella che ci precede nelle interazioni online e che viene usata da Amazon per decidere il prezzo da proporci quando navighiamo tra i suoi prodotti.

Il capitalismo delle piattaforme in fondo fa proprio questo: estrae valore dalla profilazione degli utenti e dal data mining dei nostri comportamenti online. In questo modo le aziende sanno con precisione che cosa offrirci, quando, dove e a quale prezzo, sapendo già cosa siamo propensi a desiderare. Il loro modello di business è basato sulla conoscenza dei soggetti isolati e iperconnessi che più tempo passano con i loro software gratuiti più facilmente manifesteranno desideri, fragilità e sentimenti da soddisfare con un'azione: postare, condividere, cliccare, comprare. Ogni click diventa l'occasione per arricchire il nostro

profilo psicometrico, venderlo al migliore offerente, anche per le campagne politiche. È così che Trump ha vinto nella campagna elettorale Usa 2016.

La colpa di un uso così disinvolto dei dati è anche nostra. Non abbiamo ancora capito il valore della nostra presenza online. I dati che generiamo quando siamo online indicano dei comportamenti e, in una società digitale, questi comportamenti sono trasformati in dati digitali. Il trattamento dei dati digitali consente di interpretare e spiegare i comportamenti passati ma anche di predire i comportamenti futuri. È così che i nostri dati vengono resi "produttivi". Siccome quei dati possono essere venduti e comprati, le piattaforme ci offrono gratis i loro servizi. Ma quei servizi li paghiamo con i nostri dati. Quando non paghi qualcosa il "prodotto" sei tu.

3. I termini di servizio della nostra vita *onlife*

Quando ci iscriviamo a un sito, app o servizio Internet, in genere ci viene richiesto di accettare i "Termini di servizio", i ToS, che indicano come i nostri dati sono raccolti e usati. La maggior parte delle volte non li leggiamo, semplicemente perché non ne abbiamo il tempo e la voglia, ma soprattutto perché non li capiamo, visto che sono scritti in "legalese".

Eppure è così che perdiamo il controllo dei dati che ci identificano come cittadini, lavoratori e consumatori. Quei dati infatti verranno utilizzati per creare dei profili dettagliati dei nostri comportamenti e verranno commerciati per usi che non sempre conosciamo.

Ad esempio i ToS di Facebook ed Amazon dicono che i nostri dati sono usati per tracciare il nostro comportamento su altri siti, mentre LinkedIn raccoglie, usa e condivide i dati di geolocalizzazione e Instagram ci mette sopra il suo copyright.

I termini di servizio di Reddit, Yahoo e WhatsApp dicono che usandoli accettiamo «di difendere, indennizzare e sollevare il servizio da ogni responsabilità in caso di reclamo». Quasi tutti prevedono che gli stessi termini possono essere modificati in qualsiasi momento a discrezione del fornitore, senza preavviso per l'utente.

Nel suo *Data Manifesto*[6], Kevin Kelly, tecnologo e co-fondatore della rivista *Wired*, dice che i dati «non esistono da soli», che hanno valore solo se messi in relazione ad altri dati e che circolando diventano una risorsa condivisa. Per questo possono risentire della tragedia dei beni comuni, cioè di un'egoistica azione di appropriazione – come quando un privato recinta un pezzo di parco pubblico impedendo ad altri di usarlo – e pertanto vanno protetti dai governi. Noi aggiungiamo che vanno protetti dai Signori dei dati, le aziende che ne fanno costantemente incetta.

Ma i dati sono un bene comune perché, sulla base dei dati raccolti, possiamo costruire una società migliore. I dati che noi produciamo incessantemente attraverso l'interazione con i dispositivi digitali, rappresentano comportamenti quotidiani e possono essere una base di conoscenza importante per sviluppare politiche efficaci, servizi utili alle persone e nuovi prodotti commerciali utili e rispettosi dell'ambiente. I dati, anonimizzati e aggregati, possono servire a migliorare la capacità di uno Stato di rispondere alle esigenze dei propri cittadini.

Due esempi semplici semplici. Se noi abbiamo i dati, anonimi e aggregati, dei pazienti ospedalieri, probabilmente saremo in grado di pianificare meglio le risorse sanitarie necessarie a garantire la salute pubblica. Già viene fatto, pensate agli sforzi di raccolta e analisi dei dati epidemiologici. Se abbiamo i dati di quanti e quali attacchi cibernetici ci sono stati negli ultimi anni, saremo in grado sia di anticipare nuovi attacchi che di imparare a difenderci.

Quindi, il dato inteso come bene comune è questo: è un dato che può essere utilizzato in maniera utile dagli Stati per consentire una migliore qualità della vita delle persone e garantire diritti all'altezza delle democrazie in cui vogliamo vivere.

Il GDPR prevede, in caso di grave violazione dei database, la comunicazione diretta ai singoli interessati entro 72 ore, a pena di multe salatissime, fino a 20 milioni di euro e al 4 per cento del fatturato annuo aziendale. Le sanzioni possono essere un deterrente, ma non lo sono per i grandi player della rete.

Perciò anche noi dobbiamo fare la nostra parte e capire se, quando e come ci conviene cedere i nostri dati.

4. Privacy e cybersecurity sono diritti umani fondamentali

Ma c'è un'altra questione, il rapporto stretto tra la privacy e la cybersecurity. Il motivo è semplice da capire: in un mondo digitale i dati che identificano i nostri comportamenti sono digitalizzati; se non riusciamo a tutelare questi dati digitali, non riusciamo a tutelare i nostri comportamenti. In particolare non riusciamo a tutelare i comportamenti passati dalle tecnologie che li possono spiegare e dalle tecnologie che li possono predire. I dati personali sono uno strumento di intelligence. Pensiamo alle massive violazioni di basi di dati personali usati per orientare il comportamento delle persone. Con i dati ormai ci si fa la "guerra".

Però. Se la privacy è l'altra faccia della cybersecurity è anche vero che la privacy è un diritto fondamentale dell'Unione europea, mentre la cybersecurity non lo è.

Eppure, in un mondo in cui ogni comportamento viene datificato diventando un dato digitale, proteggere quei dati che rimandano ai comportamenti quotidiani è cruciale, lo ripetiamo, proprio per la loro capacità di spiegare i comportamenti passati e di predire quelli futuri.

Se non riusciamo a proteggere i dati che ci definiscono come cittadini, elettori, lavoratori, e vicini di casa, potremmo essere esposti a un potere incontrollabile, quello della sorveglianza di massa, della manipolazione politica e della persuasione commerciale.

Pertanto privacy e cybersecurity sono la precondizione per esercitare il diritto alla libertà d'opinione, d'associazione, di movimento, e altri diritti altrettanto importanti.

Se accettiamo questa premessa possiamo pensare alla sicurezza informatica dei nostri dati come a un diritto umano fondamentale.

5. Privacy e anonimato

Eppure. Mentre la Bbc decide di portare i suoi contenuti nel *dark Web* per tutelare l'anonimato del proprio pubblico all'interno di paesi illiberali, in Italia si discute ancora di identificare gli utenti del Web.

Il dibattito, che pensavamo chiuso dopo le mobilitazioni degli anni scorsi contro la censura in rete, è ricominciato con la proposta di un parlamentare di *Italia Viva* a suo dire preoccupato per il dilagare dell'odio in rete, e che ha suggerito, parole sue, di rendere obbligatorio depositare un documento d'identità prima di aprire un profilo social «per impedire che il Web rimanga la fogna che è diventato».

Purtroppo questa risposta a problemi reali, l'hate speech, le fake news, il cyberbullismo, lo stalking online, il revenge porn, è sbagliata. Per vari motivi. Il primo è che molti odiatori in rete si presentano già con nome e cognome e il riscontro anagrafico non sarebbe un deterrente. Il secondo è che nessuno in rete è veramente anonimo e non c'è bisogno della carta d'identità per risalire ai dati anagrafici dei bulli in rete nonostante abbiano uno pseudonimo.

Per farlo occorrono tempo e risorse, riuscirci non è facile né immediato, ma si fa quando serve. Viceversa l'identificazione in massa degli utenti è un processo tecnicamente complesso e oneroso.

Il punto è qui che gli odiatori che spesso si presentano con nome e cognome in genere sono persone che semplicemente non sanno che un insulto, una minaccia espressa online, può essere perseguita come se fatta a scuola o al bar. I flame, i litigi in rete, inoltre, sono un elemento costitutivo della comunicazione virtuale: i social e i canali di chatting sono strumenti di dialogo veloce, dove si interagisce d'impulso, luoghi dove l'assenza fisica dell'interlocutore fa venire meno il timore della rappresaglia e spesso anche il pudore, la vergogna e la cautela nell'esprimere opinioni estreme.

Eppure la questione è più ampia. Il Web, o i social che ne rappresentano una parte, non è fatto solo di maleducati, odiatori, bulli, stalker, per i quali in realtà ci sono leggi anche severe che ne puniscono i comportamenti.

Il Web usato in maniera anonima è anche il Web dei dissidenti politici, dei profughi senza documenti, dei rifugiati, perseguitati nei loro paesi per essere omosessuali o per avere evaso la leva obbligatoria. E poi ci sono i cooperanti che vivono in zone di guerra, i blogger antimafia che non possono farsi riconoscere, e ci sono i *whistleblower*, i *citizen journalist*, gli impiegati di enti, ministeri e forze armate che devono giocoforza assumere identità fittizie per evitare ritorsioni a fronte delle loro denunce.

In aggiunta ci sono soggetti fragili che per raccontare esperienze di abusi e maltrattamenti mai e poi mai vorrebbero presentarsi con nome e cognome.

Quindi la domanda è: per provare a spaventare gli odiatori in rete è giusto cancellare l'anonimato di chi grazie ad esso può esprimersi liberamente?

Senza anonimato cadrebbero nell'autocensura e nel conformismo preventivo. E saremmo stati noi a togliergli quella tanto faticosamente conquistata libertà di parola. Le catacombe parlamentari sono piene di disegni di legge per limitare la libertà d'opinione in rete.

All'epoca della televisione erano tentativi surrettizi di mantenere la società divisa tra chi ha potere di parola e chi no, come diceva Michel Foucault. Ma oggi? Se queste energie venissero impiegate per educare le persone al rispetto degli altri e al rispetto delle leggi che ci sono, sarebbe già abbastanza.

6. Anonimato, fake news e disinformazione

L'anonimato in rete però permette anche di agire pratiche di disinformazione. E questo è un altro motivo per tutelare i dati personali e collettivi.

Sappiamo che le strategie di disinformazione si basano sulla manipolazione delle percezioni. La disinformazione è un'arma per indurre l'avversario a fare delle scelte sbagliate. Le fake news oggi sono la testa d'ariete di queste strategie di disinformazione

e servono a farci "comprare" quello che altri hanno deciso che "vogliamo" comprare: uno shampoo, una strategia, oppure un candidato politico.

Insieme alla profilazione dei social network le fake news pongono un problema molto serio anche alla sicurezza nazionale soprattutto quando usano deep fake video e deep fake audio o profili di persone che non esistono ma possono essere generate da un'intelligenza artificiale.

Una volta le campagne di disinformazione bersagliavano i decisori – i funzionari pubblici di alto livello, i politici, i giornalisti affermati, i funzionari dello Stato –, oggi queste campagne di disinformazione sono dirette a manipolare quella forma larvale di dibattito pubblico che c'è sui social network.

Come? Agendo attraverso la propaganda computazionale che sfrutta i social media e la credulità di chi li abita, la psicologia umana che non distingue la realtà dalla finzione, le voci e i pettegolezzi tanto cari ai cospiratori e gli algoritmi per manipolare l'opinione pubblica. È così che funzionano i *dark ads*: messaggi promozionali a pagamento diretti solo a specifici indirizzi o territori.

I dati raccolti dalle piattaforme sono usati per creare profili individuali e collettivi. Questa profilazione può essere usata per comunicazioni mirate e geolocalizzate, anche durante le elezioni.

La logica qui è doppia: se so chi sei, so quali contenuti farti vedere. Se conosco le tue scelte passate sono in grado di mostrarti solo le notizie che sei pronto a cliccare. Ogni click dice quali sono le nostre preferenze culturali e politiche, proprio quelle che sono collezionate nei giganteschi database che i padroni dei dati come Google, Amazon e Facebook usano per definire i nostri profili sociali, economici, ed elettorali.

Quindi la manovra è a tenaglia: prima la profilazione e l'esposizione alle fake news per polarizzare l'elettorato, poi il messaggio politico ritagliato *ad hoc* sotto forma di una comunicazione nominativa, diretta a una moltitudine di singoli elettori, ai quali viene recapitata in maniera ripetuta un'informazione specifica e coerente con il proprio profilo psicologico ed elettorale.

Nell'era di Internet la disinformazione fa largo uso delle fake news e la sua viralità approfitta soprattutto di Facebook, Google, Instagram fino a WhatsApp, piattaforme che agiscono da potenti casse di risonanza per i nostri pregiudizi, soprattutto quando sono veicolati da chi ci fidiamo di più: amici e conoscenti. Rappresentano un problema cibernetico.

Se la natura originaria delle bufale è quella di creare traffico web, e quindi macinare soldi dagli annunci pubblicitari, molti "spacciatori" di notizie false agiscono sotto falsa identità e hanno una motivazione ideologica: affermare un punto di vista anziché un altro, distorcere la realtà delle cose e creare "fatti alternativi". Una tecnica propagandistica salita prepotentemente alla ribalta durante la corsa alla Casa Bianca del 2016 e l'assalto a Capitol Hill dopo la sconfitta elettorale del presidente Trump da parte del democratico Joe Biden, ma che ha degli antenati "illustri" nelle *psy-ops*, le operazioni di guerra psicologica condotte da eserciti rivali per demoralizzare le truppe avversarie, influenzare il *sentiment* della popolazione e disorientare i governi.

A produrre disinformazione ci sono oggi i gruppi di *nation-state hackers*, chiamati anche APT (*Advanced Persistent Threat*), "minacce avanzate persistenti" che hanno come obiettivo di interferire con la democrazia. Si tratta di gruppi paramilitari cibernetici che vengono dai ranghi dell'intelligence, della polizia e dell'esercito, e hanno il compito, per conto dello Stato a cui hanno giurato temporanea fedeltà, di raccogliere informazioni su aziende concorrenti, su Stati avversari, su decisori pubblici per orientarne i comportamenti. Possono anche compiere azioni di sabotaggio o di guerra cibernetica. Perché? Per destabilizzarne l'economia o indebolire un avversario, ma anche per realizzare operazioni psicologiche orientate a creare malumore, diffidenza o paura nelle popolazioni, facendo uso di informazioni fasulle su target ben individuati.

Ecco, le campagne di disinformazione orchestrate dagli APT si basano sulla conoscenza del target, sui dati da essi prodotti, e servono a indirizzare le percezioni e le scelte maturate nell'agorà pubblica del Web. Quindi non vanno solo tutelati i dati personali in quanto tali, ma i dati che contribuiscono a definire la nostra persona digitale e che "rappresentano" scelte e desideri.

7. *Data breach* e banche dati

Ovviamente sono i *data breach* il pozzo principale a cui attingono i delinquenti, i cybercriminali e gli APT. Nel dicembre 2019 abbiamo saputo che la banca Unicredit era stata violata o, meglio, che tre milioni di profili dei suoi clienti erano stati violati a seguito di un attacco informatico avvenuto nel 2015. Ma che dire della violazione delle PEC di cinquecentomila indirizzi relativi ai Ministeri che afferiscono al CISR (Comitato interministeriale per la sicurezza della Repubblica) avvenuto nel 2018?

Tra il 2020 e il 2021 una serie di incursioni informatiche operate da gruppi specializzati che le hanno rivendicate nei loro blog del *dark Web* hanno esposto i dati di singoli cittadini, rappresentanti di or-

dini professionali e personaggi istituzionali. In Italia ci sono stati gli attacchi *ransomware* alla campagna vaccinale della Regione Lazio, all'Ordine dei notai e a quello nazionale forense, a livello globale alla società di consulenza Accenture, al Dipartimento del Tesoro Usa e ad altre agenzie nazionali europee.

Sicuramente c'è un tema che riguarda la formazione, la consapevolezza, ma anche la preparazione ad affrontare questi attacchi per tutelare la privacy di tutti: "non chiederti se verrai attaccato ma quando". Un concetto altrettanto importante di quello di resilienza, la capacità di ripartire dopo uno shock, in questo caso informatico.

8. Le infrastrutture critiche e la privacy

Se non è ancora chiaro, possiamo pensare al fatto che un attacco informatico di successo non solo può impossessarsi dei dati dei contribuenti, dei risparmiatori, dei legislatori, ma può determinare l'interruzione di servizi essenziali e bloccare la produzione industriale e mettere a rischio l'incolumità stessa di cittadini. Immaginatevi che cosa potrebbe succedere se ad un certo punto si spegnessero contemporaneamente in una grande città italiana i semafori, si bloccassero le operazioni chirurgiche, le ambulanze non ricevessero più le comunicazioni per andare a prendere i feriti come è successo con il *ransomware* Wannacry lanciato ai danni della Sanità inglese nel 2017. Nel 2021 un attacco cibernetico ha bloccato per giorni il ciclo dei rifiuti dell'area urbana di Firenze in Italia.

Ma cose del genere sono già successe. Nel 2013 ci fu il tentativo di aprire le chiuse della diga di New York utilizzando un telefonino. L'Estonia e l'Ucraina hanno subito il blackout della griglia elettrica a seguito di un attacco informatico. In realtà gli esempi potrebbero continuare all'infinito. Se ricordiamo la minaccia Mirai, la *botnet* che bloccò per quasi un giorno intero le comunicazioni dagli Stati Uniti verso l'Italia, per 18 ore non fu possibile raggiungere i computer che ci permettevano di accedere al New York Times, a Twitter, a Netflix, Amazon e così via. Gli attacchi cibernetici sono sempre più pericolosi: in una società digitalizzata e iperconnessa, sempre più dipendente dalla tecnologia, gli attacchi cibernetici possono fare danni enormi.

9. Perimetro nazionale

Con l'obbiettivo futuro di proteggere dati e informazioni l'Italia ha selezionato una squadra nazionale di hacker. Sono i futuri *cyberdefender*, scelti da scuole e università attraverso la *Cyberchallenge*. L'Italia ha la *Golden Power*, cioè speciali poteri di veto nei confronti di produttori e tecnologie, come il 5G, che possono rappresentare un pericolo per la democrazia e l'economia della penisola. L'Italia ha pure un *Internet kill switch*. Significa che in presenza di un rischio grave ed imminente alla sicurezza nazionale causato dalla vulnerabilità di reti, sistemi informativi e servizi informatici, il Presidente del Consiglio può disporre la disattivazione, totale o parziale, di Internet. Con le necessarie garanzie di legge. Una possibilità remota, ma prevista dalla legge sul Perimetro nazionale di sicurezza cibernetica.

La legge chiarisce la costante e contemporanea evoluzione dell'assetto cibernetico italiano, la «postura», si dice in gergo, e la mette in relazione con alcuni fattori di crescita e di innovazione che in una società aperta, digitale e iperconnessa, possono trasformarsi nel loro contrario e diventare vere e proprie minacce: cioè gli algoritmi di intelligenza artificiale, la crittografia e l'informatica quantistica. Settori su cui l'Italia dovrebbe investire di più.

E tuttavia ci ricorda che con la legge sul Perimetro nazionale, grazie al raccordo con la normativa sul *Golden Power*, alla nascita del Centro di Valutazione e Certificazione Nazionale, al futuro Csirt per rispondere prontamente alle emergenze, e ai poteri speciali di intervento, l'Italia prova ad «affrontare con la massima efficacia e tempestività situazioni di rischio grave e imminente per la sicurezza nazionale in ambito cyber».

Il grande lavoro svolto dal Dipartimento informazioni per la sicurezza, DIS, ha favorito la realizzazione della legge sul Perimetro nazionale di sicurezza cibernetica. Nelle audizioni precedenti alla conversione della legge è stata detta una cosa molto importante, che il "rischio zero" non esiste e che tutti quanti noi ci dobbiamo impegnare affinché non accada che un ragazzino diciottenne dall'India possa fermare i treni che viaggiano in Italia.

La neonata Agenzia per la cybersicurezza nazionale, ACN, nata nell'agosto del 2021 dovrà mettere a sistema tutte queste innovazioni.

Quindi se la privacy è un diritto fondamentale nell'Unione europea, lo è anche la cybersecurity, la tutela cibernetica di dati, reti e informazioni sono la precondizione per esercitare altri diritti come diceva a proposito della privacy *en general* Stefano Rodotà: il diritto di associazione, di espressione, di opinione, di movimento e così via.

C'è una frase, che viene attribuita anche al presidente americano Thomas Jefferson, che dice «Chi pensa di rinunciare alla propria libertà per avere maggiore sicurezza, non merita né la libertà né la sicurezza». Voleva dire che l'equilibrio nelle scelte che

facciamo per garantire sia la libertà sia la sicurezza dovrebbe essere l'oggetto della nostra attenzione.

Il nostro Paese, a cominciare dal "decreto Monti", successivamente con il "decreto Gentiloni", la legge sul Perimetro nazionale, il recepimento della direttiva NIS, del regolamento GDPR, l'allineamento del lavoro del nostro Parlamento con il *Cybersecurity Act* europeo, ci ha permesso di rimanere saldi in questo equilibrio tra privacy e cybersecurity. Bisogna continuare così.

Negli ultimi anni gli Stati si sono distratti e hanno lasciato che poche multinazionali avessero più dati sugli italiani di quanti ne ha il Governo che protegge gli italiani. Il tema della sovranità digitale diventa il trait d'union fra la questione della privacy e la questione della sicurezza dei dati personali, comuni, aziendali, perciò non ci si può dire sovranisti senza pensare alla sovranità tecnologica e digitale. E non si può essere sovrani senza avere il controllo dei propri dati.

Con un'avvertenza: i dati vanno raccolti nel rispetto dei diritti costituzionali, archiviati in maniera sicura e trattati nel rispetto della legge. E quando si tratta di dati sensibili, come quelli relativi alla salute, vanno distrutti se non servono più.

Note

[1] Y.N. Harari, *21 Lezioni per il XXI secolo*, Bompiani, 2018.

[2] M. Castells, *Comunicazione e Potere*, Università Bocconi Editore, 2017.

[3] P. Mason, *Il Futuro migliore*, Il Saggiatore, 2019.

[4] Cfr. D. Harvey, *La guerra perpetua. Analisi del nuovo imperialismo*, Il Saggiatore, 2006; C. Formenti, *Cybersoviet. Utopie postdemocratiche e nuovi media*, Raffaello Cortina Editore, 2008; S. Zubof, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, 2019.

[5] W. Quattrociocchi, A. Vicini, *Liberi di crederci*, Codice, 2018.

[6] K. Kelly, *Data Manifesto*, 2019.

* * *

Data commons: Privacy and cybersecurity are fundamental human rights

Abstract: Google knows more about us than we remember: it knows our daily habits and paths, it knows with whom, when and for how long we have been there; Zoom knows who we work with, Facebook puts our preferences up for auction; Twitter bots and trolls influence our views. Misinformation memes also crowd social media and pollute the scientific debate. If we do not learn to protect personal behaviors turned into digital data, we will be exposed to an uncontrollable power, that of commercial persuasion, political manipulation and state surveillance.

Keywords: Data commons – Privacy – GDPR – Cybersecurity – Big Tech