PRIVACY A RISCHIO PANDEMIA

di GIACOMO CORVI

L'EMERGENZA COVID-19 HA IMPOSTO DEROGHE, TEMPORANEE MA INEVITABILI, ALLA TUTELA DEI DATI PERSONALI. IL CORONAVIRUS HA MESSO IN EVIDENZA TUTTA LA FRAGILITÀ DI UN SISTEMA CHE, FRA NORME NON APPLICATE E COMPORTAMENTI POCO VIRTUOSI, NON GARANTISCE LA SALVAGUARDIA DI UN DIRITTO FONDAMENTALE. RISCOPRIRE UN USO ETICO DEL DATO NON SARÀ FACILE

Il lockdown per l'emergenza coronavirus ci ha catapultato in una situazione paradossale. Chiusi fra le quattro mura domestiche per evitare ogni rischio di contagio, abbiamo avuto per la prima volta la possibilità di entrare (almeno virtualmente) in abitazioni in cui fino a poco tempo fa, quando parlare di condizioni normali aveva ancora un senso, non avremmo mai avuto accesso. In televisione abbiamo potuto apprezzare l'ordine di pregiate librerie che si stagliavano alle spalle di virologi ed epidemiologi che, da semplici esperti della materia sono diventati, piccole celebrità del mondo ai tempi del Covid-19. In videoconferenza abbiamo potuto finalmente comprendere che la confusione del nostro collega di ufficio non è prerogativa della scrivania di lavoro. E nelle sessioni di didattica a distanza dei nostri figli e nipoti abbiamo ammirato i salotti, le cucine e le camere da letto di quegli insegnanti che prima vedevamo soltanto ai colloqui di metà anno scolastico. Pur restando nel calore della nostra casa, siamo dunque riusciti a entrare nelle case degli altri. Abbiamo insomma avuto la possibilità di violare la privacy altrui. E anche gli altri, senza magari che ce ne accorgessimo, hanno fatto lo stesso con noi.

"Il coronavirus ha fatto saltare tutti gli schemi", afferma **Nicola Bernardi**, presidente di **Federprivacy**. "Durante il lockdown – spiega – si è verificata una situazione di tale emergenza che è stato inevitabile accantonare temporaneamente la tutela del diritto fondamentale alla privacy per una causa di forza maggiore come la salvaguardia della vita umana".

VITTIMA COLLATERALE DELLA PANDEMIA

Parafrasando **Arthur Ponsonby**, si potrebbe dire che la prima vittima della pandmia di Covid-19 è stata la privacy. Un sacrificio inevitabile come ha ammesso lo stesso **Antonello Soro**, all'epoca presidente dell'Autorità garante per la protezione dei dati personali, in un'intervista rilasciata lo scorso 17 marzo all'Ansa. "I diritti possono, in contesti emergenziali, subire limitazioni anche incisive", aveva affermato nelle battute iniziali del colloquio, salvo poi precisare immediatamente che "queste devono essere proporzionali alle esigenze specifiche e temporalmente limitate".

***Nicola Bernardi**, presidente di Federprivacy*

Sulla stessa linea si pone anche Bernardi, il quale sottolinea come anche la *Carta di Nizza* ammetta "deroghe momentanee al rispetto di diritti fondamentali in situazioni di particolare emergenza". A patto che, come già ribadito, si tratti di accantonamenti soltanto momentanei. Bernardi prende a tal proposito l'esempio dell'adeguamento al *General data protection regulation*, il regolamento europeo sulla protezione dei dati personali, più conosciuto con la sigla *Gdpr*, che è entrato in vigore nel maggio del 2018. "Il coronavirus – avverte – non può diventare per le piccole e medie imprese una giustificazione al mancato adeguamento alla normativa: poteva esserlo durante il blocco delle attività per le misure di lockdown, ma poi gli operatori devono tornare a mobilitarsi per rendersi pienamente conformi alla disciplina".

LA QUESTIONE IMMUNI

L'app *Immuni* ha rappresentato senza dubbio l'argomento che ha maggiormente alimentato il dibattito sulla tutela della privacy durante la pandemia. A metà settembre appena 5,9 milioni di persone, pari soltanto al 15% della popolazione target, si erano dotati dell'applicazione. E il 29% di chi non l'aveva scaricata, stando a un'indagine di **Swg** pubblicata a luglio, affermava di non averlo fatto per timori per la propria privacy. Numeri di un flop annunciato che, a detta di Bernardi, poteva essere evitato.
"L'app è conforme al Gdpr, come ha stabilito il garante per la protezione dei dati personali", premette Bernardi. Quello che è mancato, a detta del presidente di Federprivacy, è un sistema di gestione che potesse garantire il successo dello strumento. "Il funzionamento di Immuni presenta varie lacune: il cellulare può essere lasciato a casa, smarrito o sostituito con quello di un familiare. Tutto – prosegue – è lasciato poi al buon senso del cittadino: non c'è l'obbligo di download ed è compito dell'utente segnalare l'eventuale positività al tampone". In quest'ottica, secondo Bernardi, non era difficile prevedere il fiasco di uno strumento che fra l'altro, per essere efficace, dove essere scaricato da almeno il 60-70% della popolazione. Tanto valeva allora non fare nulla. "Il Gdpr prevede il principio di minimizzazione, ossia l'invito a cercare la soluzione che presuppone la minor intrusione nei dati personali per compiere una determinata azione: visto che era palese dal principio che Immuni non avrebbe raggiunto il suo obiettivo – dice Bernardi – forse era meglio non fare niente".

IL BUSINESS (MA NON SOLO) DEL DATO

Per quanto abbia gravitato attorno a sé l'intero dibattito, Immuni non è stato il solo elemento a porre a serio rischio la tutela della nostra privacy. Gli ormai famosi termoscanner raccolgono dati estremamente sensibili come la temperatura corporea. E le già citate piattaforme di videoconferenza immagazzinano e inviano dati in server che spesso sono collocati all'estero, in Paesi come Stati Uniti, Cina e Israele. Poi vai a sapere quello che ci fanno.
"Nella gestione di informazioni strettamente personali il rischio zero non esiste", ammette Bernardi. "I dati sono diventati una materia prima, qualcuno li definisce il nuovo petrolio. Le grandi compagnie ci si fiondano di getto quando vedono la possibilità di sfruttare informazioni sulle nostre abitudini e preferenze: non è sicuramente un caso – dice – se al bando per la realizzazione dell'app di contact tracing, poi vinto dagli sviluppatori di Immuni, ci fossero proposte totalmente gratuite". Il modus operandi di queste società è ormai noto: i dati vengono aggregati e rielaborati per creare identikit del singolo cittadino e indirizzare proposte disegnate sulle sue esigenze. È una sorta di segmentazione di mercato all'ennesima potenza, qualcosa che esiste da decenni nel mondo del marketing e della pubblicità. Con la differenza, sottoli-

VIGILANZA POCO VIGILANTE

Secondo Nicola Bernardi, presidente di Federprivacy, non servono nuove leggi per tutelare la privacy dei cittadini: basterebbe applicare quelle che già ci sono. A cominciare dal Gdpr. "Nel 2019 sono state comminate sanzioni per più di 410 milioni di euro a seguito di violazioni al regolamento europeo sul trattamento dei dati personali", spiega. "A fronte di comportamenti rigorosi come quello tenuto dal garante italiano – prosegue – nel resto d'Europa non si sono sempre registrati gli stessi livelli di impegno: in Irlanda, dove hanno sede società come **Facebook** e **Microsoft**, il garante ha comminato soltanto due sanzioni, rivolte per di più allo stesso istituto per bambini". Nei due anni e mezzo dall'entrata in vigore del Gdpr, i giganti del web non sono stati toccati da sanzioni di alcun genere. "In queste condizioni non ci può essere alcun effetto deterrente", sottolinea Bernardi.


© iBrave - iStock

nea Bernardi, che questa volta la definizione del target viene fatta utilizzando anche "quei messaggi che adesso scriviamo su *WhatsApp* e che prima avremmo detto soltanto all'orecchio del nostro confidente". Non necessariamente poi i dati vengono utilizzati solamente per meri scopi di marketing pubblicitario. "Quattro anni fa un signore è diventato presidente degli Stati Uniti facendo leva su società come **Cambridge Analytica**, che raccolgono ed elaborano dati per personalizzare l'offerta comunicativa", ricorda Bernardi.

UN USO ETICO DEL DATO

A metà settembre è uscita la notizia di una class action contro **YouTube** in Regno Unito. A detta dei promotori, il portale di streaming della galassia **Google** avrebbe raccolto dati di utenti al di sotto dei 13 anni di età senza l'esplicito consenso dei genitori, violando così le disposizioni del Gdpr e del britannico *Data protection act*: se l'iniziativa dovesse andare a buon fine, il colosso di Mountain View sarebbe costretto a sborsare complessivamente 2,5 miliardi di sterline, pari a 3,2 miliardi di dollari.

"Credo che casi di questo genere diventeranno sempre più frequenti in futuro", dice Bernardi. Almeno fino a che le società, in particolare i giganti delle tecnologie, non si adegueranno a un uso etico dei dati personali. Bernardi recupera a tal proposito la lezione di **Giovanni Buttarelli**, compianto magistrato che dal 2014 ha ricoperto la carica di garante europeo per la protezione dei dati fino alla sua scomparsa, avvenuta nel 2019. "Aveva avuto la lungimiranza di fare dell'etica il suo cavallo di battaglia, perché aveva capito che era l'unica via per creare un regime di equo trattamento dei dati personali", ricorda Bernardi. "Purtroppo – aggiunge – da quando è scomparso si sente parlare meno di etica". La sua lezione, prosegue, è però rimasta nel testo del Gdpr quando "invita a trattare i dati in maniera lecita, pertinente, trasparente e non eccedente il principio di minimizzazione: in una parola eticamente. Gli utenti devono avere la possibilità di navigare su Internet senza aver paura di essere ingannati, di cedere i propri dati senza ritrovarsi vittime di sofisticate analisi che vanno contro i loro stessi interessi: è questo – conclude – l'unico modo per creare un mercato digitale sicuro ed equo".

PRIVACY, UN MARCHIO DI QUALITÀ

La gestione del dato è da sempre parte integrante del business delle assicurazioni. In un contesto di forte crescita dell'attenzione sulla tutela dei dati personali, mostrarsi virtuosi può rassicurare la clientela e costituire un vantaggio competitivo. In quest'ottica, l'adesione a un codice di condotta può rivelarsi un efficace mossa strategica. Federprivacy, a tal proposito, ha elaborato una serie di norme a cui le imprese possono aderire per certificare la correttezza delle proprie attività: una volta suffragata l'adesione della società alle disposizioni del codice di condotta, Federprivacy conferisce il marchio di qualità *Privacy Ok* che può essere apposto su sito web e altri materiali di comunicazione.