Poliziamoderna

Protezione dei dati personali e attività di polizia

1. Premessa

È esperienza comune che le situazioni di emergenza portino alla ribalta del dibattito pubblico tematiche che sono spesso oggetto di approfondimenti soltanto da parte delle comunità di riferimento. Ne è un esempio il recente utilizzo di applicazioni informatiche di *contact tracing* per mappare la diffusione da Sars-Cov2 che ha riacceso il dibattito sulla rilevanza della tutela della riservatezza e della protezione dei dati personali nel più ampio panorama dei diritti di libertà che è dovere dello Stato riconoscere e garantire.

Questa rinnovata attenzione alla privacy e alle condizioni entro le quali un utilizzo dei dati personali dei cittadini possa essere efficacemente messo al servizio del bene pubblico, offre un'interessante occasione per esprimere delle considerazioni ed approfondire princìpi e modi per coniugare al meglio privacy, protezione dei dati personali e sicurezza pubblica. È utile ricordare che privacy e protezione dei dati personali, per quanto vicini, rappresentino due concetti distinti e dalle implicazioni diverse, tanto da essere entrambi tutelati come diritti dalla Carta dei diritti fondamentali dell'Unione europea, agli articoli 7 e 8. Il diritto alla riservatezza (privacy) riconosce a ogni individuo la tutela della propria sfera più intima e si pone pertanto come tutela di un soggetto relativamente all'esposizione di informazioni che possano violare tale intimità. In altre parole, il diritto alla riservatezza stabilisce che esistono aspetti della nostra vita privata che non vogliamo vengano resi pubblici e ci tutela dalla loro pubblicità senza il nostro consenso, in mancanza di un preminente interesse pubblico. Di contro, il diritto alla protezione dei dati personali attiene alle informazioni che un individuo acconsente a rendere note esclusivamente per specifiche finalità come, ad esempio, per la sottoscrizione di una polizza assicurativa o del contratto di fornitura dell'elettricità, per l'abbonamento ad una rivista, eccetera. Più raramente, purtroppo, accade che gli individui siano consapevoli delle implicazioni che comporta dare il proprio consenso al trattamento in contesti erroneamente considerati "non a rischio", come in alcuni social network o nel disinvolto utilizzo di *App* apparentemente innocue.

In questo contesto, il concetto di finalità è cruciale e rappresenta presupposto e perimetro per il trattamento di quei dati personali che, pertanto, devono essere gestiti solo per quella finalità e non per scopi diversi o ultronei, siano questi ultimi di nocumento o meno per il soggetto che li ha forniti. Le implicazioni sociali del diritto alla protezione dei dati personali sono di portata ampia e profonda, considerata anche la potenziale lesione dell'immagine pubblica e la potenziale nascita di pregiudizi personali e discriminazioni – si pensi ai rischi di profilazione – che possono originarsi a causa di un trattamento illegittimo di dati personali. Trattamenti dei dati di particolare delicatezza, quali quelli inerenti alle attività di polizia, portano con sé timori che non possono e non devono essere liquidati con il luogo comune "chi non ha nulla da nascondere non ha nulla da temere", che non solo è capziosamente fuorviante, ma anche estremamente pericoloso: preferiamo, al riguardo, un'altra citazione di Edward Snowden, per il quale "non preoccuparsi del diritto alla privacy perché non si ha nulla da nascondere equivale al non curarsi della libertà di espressione solo perché non si ha nulla da dire." Privacy e protezione dei dati personali sono presidi di democrazia e libertà quanto la Pubblica Sicurezza che rimane – anch'essa – un imprescindibile prerequisito per il godimento di tutti i diritti inviolabili ed è pertanto in questa chiave che occorre cercare un sapiente bilanciamento tra le diverse istanze.

Iniziamo con il chiederci se sia veramente corretto affermare che per garantire il diritto alla sicurezza, che è un diritto fondamentale, occorra necessariamente limitare la privacy, anch'essa un diritto fondamentale. Per quanto possa sembrare un vizioso ragionamento circolare, se non un paradosso logico, l'argomento è di cruciale importanza. I molteplici riflessi delle scelte che le società attuali stanno facendo vanno studiati in profondità e le risposte influenzeranno il nostro futuro per gli anni a venire, tanto più in una fase storica nella quale il progresso tecnologico apre a scenari – e a rischi – precedentemente inimmaginabili anche dalla migliore letteratura fantascientifica.

Nella Teoria dei giochi, area della matematica applicata che studia le condizioni sotto le quali diverse entità interagiscono perseguendo obiettivi comuni, diversi o conflittuali, esiste un concetto interessante

che sembra ben descrivere il rapporto tra privacy e sicurezza pubblica: il cosiddetto “gioco a somma zero”, ovvero un esempio di interazione strategica tra decisori dove il guadagno di un giocatore è perfettamente bilanciato dalla perdita della controparte, e viceversa.

È in effetti un comune sentire che il rapporto tra privacy e sicurezza espliciti l’idea per la quale maggiore è il livello di sicurezza desiderato, più profonda è l’intrusione nella nostra sfera privata che sembra necessario accettare. Ad esempio, dopo gli attentati dell’11 settembre 2001, con il *Patriot act* statunitense, rimasto in vigore fino al 2015, successivamente temperato con il *Freedom act*, parte della società americana è sembrata rassegnata a considerare la privacy quale moneta pregiata con cui pagare la sicurezza nazionale, ma non sono mancate vibranti proteste, voci critiche e denunce di abusi. Quello che dobbiamo domandarci oggi è se questo assunto, che vede privacy e sicurezza inversamente proporzionali, sia realistico e sia un valido modello descrittivo della realtà o se – piuttosto – rappresenti una lettura errata, non dissimile dall’*illusione di Ebbinghaus* (vedi foto sopra) o da altri inganni ottici, dove il contesto porta in fallo la nostra percezione. In altri termini, il *gioco a somma zero* tra privacy e pubblica sicurezza è un dato di realtà o la realtà è più complessa?

2. Più sicurezza equivale a meno privacy?

In primo luogo, si sa, il diavolo si annida nei dettagli. Affermare che paghiamo la nostra sicurezza, la nostra libertà, sacrificando la privacy non è aderente al vero, se non in prima, superficiale approssimazione. È più corretto dire che è possibile garantire un più alto livello di sicurezza sfruttando le informazioni desunte (anche) dall’elaborazione di alcuni dati personali: non sono i dati personali che pagano la sicurezza, ma le informazioni che se ne possono desumere attraverso le elaborazioni e, soprattutto, l’uso che di esse se ne fa. E pertanto, ogni considerazione in tal senso non può compiutamente svolgersi senza studiare quali dati sono trattati, con quali modalità (tecniche e di principio) e mettendo tali esiti in relazione con la finalità perseguita. Il principio che guida l’analisi in tal senso – la proporzionalità del trattamento –, se ben applicato, permette di avvicinarsi sensibilmente alla quadratura del cerchio tra adempiere al dovere di garantire la pubblica sicurezza e proteggere al massimo i dati personali, assicurando un vantaggio sociale e limitando entro chiari, ben definiti, trasparenti e controllati limiti il potenziale senso di “intrusione” nella sfera privata.

Declinare correttamente la proporzionalità di un trattamento di dati personali implica riconoscere in prima istanza la finalità specifica che si vuole perseguire e, sulla base di ciò, traguardare, tra le altre cose, i seguenti criteri:

identificare l’insieme minimo di dati personali da trattare: un matematico direbbe i dati “necessari e sufficienti”, un giurista “pertinenti e non eccedenti”, entrambi intendendo tutti e soli i dati in assenza dei quali non sia possibile raggiungere la finalità prefissata;

determinare il periodo di tempo per il quale sia necessario conservare tali dati;

minimizzare l’insieme dei soggetti abilitati a trattare i dati e definirne i requisiti;

progettare e realizzare sistemi e misure di sicurezza idonei e adeguati che assicurino il rispetto degli attributi di riservatezza, integrità e disponibilità dei dati oggetto di trattamento.

Realizzare un trattamento “proporzionato” (rispetto alla finalità) è il primo passo per deflazionare il concetto di *gioco a somma zero*, riportandolo piuttosto in un contesto nel quale il vantaggio ottenuto in sicurezza supera la sensazione di intrusione dovuta al trattamento dei dati personali, specie da parte delle forze di polizia, o dalle autorità in genere. Concretizzare tale principio in interventi efficaci e ragionati sulle attività di trattamento richiede, ovviamente, una comprensione profonda del contesto e senza una precisa analisi delle specificità dei trattamenti e dei rischi connessi sarebbe assai difficile trovare le risposte corrette ai problemi sopra elencati. Il principio di proporzionalità, quindi, richiede di indirizzare la protezione dei dati personali non solo come adempimento giuridico, da realizzare più per obbligo che per convinzione, ma come componente fondamentale nello svolgimento delle attività istituzionali.

Messa a fuoco l’importanza della proporzionalità per raggiungere il bilanciamento tra privacy e sicurezza, occorre analizzare la questione anche da un’altra prospettiva, altrettanto importante. C’è un aspetto, essenziale, che riguarda la percezione del problema. Possiamo realizzare un trattamento

diligentemente proporzionato, proteggere i dati nel modo più meticoloso, possiamo met

...

Consultazione dell'intero articolo riservata agli abbonati

01/02/2021