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 mettere in atto le misure di sicurezza più accurate, ma se i cittadini avessero la sensazione di essere controllati, di sottostare a un'intrusione o di poter subire dei pregiudizi esclusivamente in ragione dell'esistenza di quel trattamento, allora potrebbero sentirsi condizionati e, di conseguenza, modificare il proprio stile di vita. Se la sensazione di "essere osservati", che sia navigando in Rete, camminando per strada o partecipando a una manifestazione, spingesse a modificare le proprie abitudini, a far escludere

opzioni che viceversa si sarebbero preferite, ossia precludesse a priori alcune scelte limitando, in sostanza, la possibilità di svolgere la propria personalità, come richiamato dalla nostra Carta costituzionale, in una sorta di autocensura, tutto andrebbe come se in effetti quell'intrusione si fosse realmente realizzata. Questa considerazione chiama coloro che hanno l'onere della responsabilità dei trattamenti e della protezione dei dati personali a spiegare in maniera chiara quanto necessario a eliminare i rischi di un'errata percezione da parte dei cittadini. La trasparenza e la pubblicità sui trattamenti di dati personali concorre in maniera fondamentale al raggiungimento di questo fine di civiltà, e la comunicazione integra in maniera sostanziale la protezione dei dati, diventando essa stessa una misura di *data protection,* al pari di quelle tecnico organizzative dei sistemi di trattamento.

**3. Due diritti inalienabili** Se vogliamo adoperarci per apportare un valore aggiunto in termini di pubblica sicurezza anche attraverso forme più o meno sofisticate di elaborazione di dati personali – esigenza ormai irrinunciabile – dobbiamo orientare i nostri sforzi verso due obiettivi attraverso i quali decostruire l'errata impressione e i suoi nefasti influssi sulla libertà di tutti. Da un lato, occorre studiare dettagliatamente ogni riflesso delle attività di trattamento al fine di svolgere le elaborazioni in maniera tale da desumere solo quanto strettamente necessario alla finalità, utilizzando unicamente i dati indispensabili e proteggendoli in maniera efficace. Dall'altro, è fondamentale comunicare in maniera chiara, comprensibile e trasparente, quali dati trattiamo, come e perché li trattiamo, come li mettiamo in sicurezza e perché il trattamento non comporta intollerabili intrusioni nella sfera privata. Chiarito ciò, occorre non perdere di vista la natura duplice e simmetrica del *gioco a somma zero*: se è vero che non dobbiamo pagare la sicurezza con un'indiscriminata intromissione nella nostra sfera privata, è altrettanto vero che non possiamo sacrificare in modo ideologico la tutela della sicurezza pubblica sul simulacro della privacy e della protezione dei dati personali.

Su questo tema è stato detto tutto e il suo contrario: che le autorità possano accedere indiscriminatamente a qualsiasi informazione oppure, al contrario, che le norme a tutela della privacy siano eccessivamente limitanti l'attività di polizia e che, addirittura, possano essere usate come sponda per garantire maggiore libertà di azione a soggetti intenti ad attività criminose. Le forze di polizia non possono essere ingessate o limitate da una miope declinazione dei concetti di privacy e *data protection*, né la loro azione può indiscriminatamente attingere alla sfera privata delle persone fisiche senza una cornice normativa, giuridica e di controlli meno che rigorosa. Anche in questo contesto la proporzionalità del trattamento aiuta ad inquadrare correttamente le linee di azione: realizzare un trattamento proporzionato rispetto alla finalità vuol dire perseguire la finalità minimizzando dati e informazioni utilizzate a quelle strettamente necessarie. Al contrario, impedire aprioristicamente un trattamento di dati personali non realizza una buona protezione degli stessi: elimina semplicemente alla radice il problema ma impedisce il raggiungimento della finalità. Il mestiere di chi deve curare la *data protection* non è quello di negare nuove ipotesi di trattamenti, ma fondamentalmente è quello di trovare le garanzie e le condizioni (giuridiche, tecniche, organizzative) sotto le quali poterli effettuare in modo sicuro.

La protezione dei dati personali è complessa, ma complessa non vuol dire irrealizzabile. Il recente aggiornamento alla normativa sulla protezione dei dati personali ha introdotto una serie di principi e strumenti che nell'agevolare – tra le altre cose – la proporzionalità e la trasparenza dei trattamenti, forniscono delle direttrici di approccio per superare la sfida del *gioco a somma zero*.

**4. Lo scenario in Europa e in Italia** In Italia il diritto alla privacy e alla protezione dei dati personali, originariamente riconosciuti solo a livello giurisprudenziale, videro un inquadramento legislativo solo negli anni novanta, con la legge 31 dicembre 1996, n. 675 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali), recante, tra le altre disposizioni, l'istituzione dell'Autorità garante per la protezione dei dati personali. La legge 675/1996 venne poi integrata dal decreto legislativo 28 dicembre 2001, n. 467 e infine abrogata dall'entrata in vigore del cosiddetto "Codice in materia di protezione dei dati personali" (Decreto legislativo 30 giugno 2003, n. 196). Il Codice, legge organica comprendente tanto aspetti di natura generale quanto regole ad hoc per specifici ambiti quali i trattamenti condotti per finalità di polizia, ha rappresentato per 15 anni il riferimento fino all'entrata in vigore delle nuove norme europee sulla protezione dei dati personali: il Regolamento Ue 679 del 2016, detto Rgpd, più noto con l'acronimo anglofono Gdpr, e la Direttiva Ue 680 del 2016, attuata nel nostro ordinamento con il dl 18 maggio 2018, n. 51, meno conosciuta del Gdpr ma tuttavia fondamentale per il tema che stiamo trattando, poiché specificamente dedicata ai trattamenti di dati personali svolti per finalità di polizia e giustizia. Sia il regolamento che la direttiva sono nati dall'esigenza di uniformare il panorama normativo europeo e di adeguare la disciplina sulla protezione dei dati personali al mutato contesto tecnologico, sociale ed economico che da un lato ha ampliato le possibilità di trattamento, e dall'altro ha portato ad una delocalizzazione dei dati, oltre che delle attività stesse. Queste spinte si sono tradotte in un deciso cambio culturale, prima ancora che in una collezione di regole e adempimenti che, se opportunamente metabolizzato, fornisce validi strumenti per rendere concreti i princìpi di proporzionalità e trasparenza che sono presupposti, come visto, per

superare il pregiudizio del *gioco a somma zero*.

Prima della recente legislazione europea, il Codice in materia di protezione dei dati personali presentava una natura fortemente prescrittiva, basata sostanzialmente sull'assunto che fosse possibile individuare un approccio a validità generale per la protezione dei dati personali. Partendo da questo presupposto, il Codice indicava al titolare del trattamento – ovvero la persona fisica o giuridica responsabile di stabilire finalità e modalità del trattamento – un quadro piuttosto rigido di adempimenti rispetto ai quali questi era di fatto chiamato ad assicurare la conformità, posto che detti adempimenti "minimi" erano considerati sufficienti ad assicurare un adeguato livello di protezione, indipendentemente dal trattamento in esame. Un approccio di questo tipo era motivato dal fatto che le attività di trattamento previste all'epoca erano di fatto meno policrome, complesse e distribuite di quelle attuali e fondamentalmente si limitavano, nella maggior parte dei casi, all'acquisizione, memorizzazione e lettura di dati, spesso circoscritti a informazioni anagrafiche o comunque di natura testuale, senza approfondite analisi, profilazioni o elaborazioni con algoritmi evoluti o di intelligenza artificiale. Tale condizione, inoltre, spingeva a porre il focus delle attività sulla protezione dei dati in sé, atteso che le limitate capacità elaborative appiattivano possibili impatti pregiudizievoli sui cittadini sulla mera *disclosure* dei dati stessi piuttosto che sull'estrazione e ricostruzione di possibili informazioni a valore aggiunto relative agli stessi. In un contesto di questo tipo aveva senso una filosofia prescrittiva che disponeva regole comuni per un panorama caratterizzato da poca variabilità. L'allargamento delle attività di raccolta di dati, la differente natura dei dati oggetto di acquisizione, la possibilità che quest'ultima avvenisse senza l'intervento attivo (o la consapevolezza) del soggetto cui i dati si riferiscono e l'introduzione di tecniche adattative di analisi e profilazione sempre più efficaci, facendo venir meno l'assunto di base relativo alla limitata variabilità del contesto, hanno reso non più attuale e via via meno efficace il sistema di protezione disegnato dal Codice del 2003. Inoltre, l'approccio prescrittivo, in accordo al quale la conformità alla norma avrebbe dovuto assicurare un minimo - ma legittimo - livello di protezione, rischiava di appiattire le misure di protezione dei dati personali ad un mero adempimento formale ove le regole proposte dal Codice venivano spesso implementate passivamente senza l'effettiva comprensione del loro valore, depotenziando il sistema di protezione dei dati nel suo più complesso significato.

***Una nuova figura professionale*** Le norme sulla protezione dei dati personali prevedono inoltre una nuova figura professionale: il Responsabile della protezione dei dati (Rpd o Data protection officer – Dpo), caratterizzata dall'indipendenza nello svolgimento delle proprie mansioni, al fine di garantire terzietà e incisività nei controlli. Nello spirito dei pesi e contrappesi, il responsabile della protezione ha fondamentalmente compiti di controllo rispetto alle norme, di formazione e informazione; in sostanza, è una figura di supporto al titolare del trattamento.

Il ruolo del Responsabile della protezione dei dati è molto importante per il titolare del trattamento, le cui scelte sono sempre e comunque oggetto di un controllo indipendente e terzo rappresentato dal Garante della privacy, per il quale il Responsabile della protezione dei dati funge da punto di contatto, favorendo una più semplice interlocuzione tra istituzioni. Il vantaggio di tale soluzione è duplice: il responsabile della protezione dei dati rappresenta un utile supporto al titolare del trattamento per l'instradamento delle attività fondamentali per la data protection e, al contempo, essendo molto "vicino" ai trattamenti, ha la giusta sensibilità per poter verificare puntualmente la rispondenza dei trattamenti alle norme.

**5. Un cambio di passo culturale: il principio di responsabilità** Il nuovo impianto normativo definito dal Gdpr e dalla Direttiva 680 del 2016 ribalta il presupposto proponendo una nuova filosofia per la protezione dei dati personali meglio adattata a una disciplina più matura e calata in un contesto ove la raccolta e l'elaborazione intelligente dei dati ha ormai assunto caratteri di elevata pervasività. Il nuovo paradigma, enunciato tanto per i trattamenti di carattere generale quanto per quelli, qui di maggiore interesse, condotti per finalità di polizia, permette un più efficace perseguimento dei concetti di proporzionalità e trasparenza.

L'assunto di base, riconoscendo l'elevata specificità di ogni operazione di trattamento di dati personali, respinge l'ipotesi di poter individuare un approccio universale per la *data protection*: ogni trattamento ha le proprie caratteristiche – una particolare finalità, una tecnologia a supporto, una propria natura e profondità di dati raccolti, una specifica estensione e un determinato profilo di rischio per gli interessati dal trattamento – e quindi anche il sistema di gestione della protezione dei dati deve adattarsi ai diversi scenari. Secondo questo approccio, il titolare del trattamento non è più chiamato a curare l'esecuzione di una collezione di misure che la legge ha stabilito per lui, ma ha l'onere di definire, scegliere e documentare le regole necessarie per quello specifico trattamento ed è di conseguenza responsabile tanto dell'idoneità delle regole scelte quanto dell'efficace messa in opera delle stesse: non più mero esecutore, ma responsabile nella progettazione della *data protection*. Se, precedentemente, l'idea di base era quella per la quale la conformità alla Legge era assicurata

dall'osservanza delle misure minime, adesso vale il contrario: partendo dall'analisi dei rischi, è il sistema di protezione dei dati, opportunamente progettato, realizzato e documentato, che assicura la conformità alla Legge. Il titolare del trattamento è quindi chiamato a dimostrare che le regole che si è dato, nel rispetto della norma, siano idonee e che le stesse siano effettivamente implementate. Questo reinquadramento di responsabilità – per gli anglofoni "accountability" – rappresenta una rivoluzione copernicana: riconoscere la specificità di ogni singolo trattamento permette di progettare un sistema di protezione dei dati personali tale da assicurare il massimo contenimento dei rischi per i diritti e le libertà degli interessati. Così come un abito confezionato non potrà mai vestire bene come un abito di sartoria cucito su misura, l'aver abbandonato i criteri "minimi" in favore di un maggior grado di responsabilità del Titolare del trattamento abilita un innalzamento dei livelli di protezione non raggiungibili prima. Ancora, la forte responsabilizzazione riconosciuta in capo al Titolare, con sanzioni pesantissime in caso di inadempienza, deflaziona il rischio di una declinazione della *data protection* meramente orientata alla conformità formale e non sostanziale. Insomma, se ad una prima lettura della norma il termine "*misure idonee*" poteva sembrare aleatorio se non addirittura ambiguo, grazie al principio di responsabilità acquisisce un significato molto chiaro. Il principio di responsabilità rappresenta quindi il centro di gravità intorno al quale orbitano e si comprendono meglio altri concetti fondamentali introdotti dalla normativa:

**i registri delle attività di trattamento**, documenti dettagliati e critici che descrivono i trattamenti in essere, permettono al titolare di avere piena contezza di quanto sotto il suo controllo e delle specificità da tenere in conto, rappresentando pertanto il punto di partenza per il giusto rispetto della proporzionalità del trattamento;

il principio di **protezione dei dati personali fin dalla progettazione e per impostazione predefinita**, la cui implementazione è obbligatoria, promuove la protezione dei dati personali a parte integrante e intrinseca di un trattamento di dati invece che ad un controllo reso a posteriori: in accordo a tali principi, le misure di protezione sono progettate e studiate come requisito fondamentale -al pari di quelli funzionali- in modo da guidare l'utente verso la minimizzazione dei dati, negando alla radice, almeno in linea teorica, la possibilità che il titolare del trattamento possa realizzare un trattamento non proporzionato;

la previsione di una **valutazione di impatto sulla protezione dei dati personali**, laddove i trattamenti prevedano un rischio elevato per i diritti e le libertà delle persone fisiche, obbliga il titolare del trattamento ad un momento di riflessione strutturata e documentata prima di eseguire un trattamento dal quale possano originarsi rischi per la privacy degli interessati, prevedendo al tempo stesso il ruolo fondamentale del Garante della privacy quale autorità terza chiamata a esprimersi sul trattamento;

l'obbligo di **notifica delle violazioni** di dati personali (c.d. *data breach*) favorisce la trasparenza e, al contempo, richiede al titolare del trattamento l'instaurazione di processi di gestione degli incidenti di sicurezza fondamentali, promuovendo implicitamente un maggiore livello di sicurezza del trattamento;

la disciplina inerente alla condivisione dei dati con i Paesi terzi (l'uniformità del livello di protezione all'interno dell'Unione europea è assicurata dalla natura stessa delle norme europee) prevede, ove non sussista un via libera da parte della Commissione europea, che il titolare autorizzi esplicitamente il trasferimento dei dati previa analisi intorno al livello di protezione dei dati offerto dal paese terzo – o dall'organizzazione internazionale – destinataria della condivisione. Tale approccio proietta l' *accountability* del titolare anche nello scenario della cooperazione internazionale e assicura anche in questo contesto un'adeguata protezione per i diritti degli interessati.

***Non soltanto trattamenti "elettronici"*** Un grave errore concettuale ancora piuttosto comune consiste nel ritenere che i trattamenti di dati personali siano soltanto quelli afferenti a sistemi informatici. Non è assolutamente così e la legge è estremamente chiara al riguardo: per "trattamento" si intende infatti qualsiasi operazione effettuata su dati personali con o senza l'utilizzo di sistemi informatici. Per maggiore chiarezza la norma precisa che costituisce trattamento "la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione". Quindi, anche la mera trasmissione tra uffici di una lettera che contenga dati personali costituisce un trattamento e come tale deve essere rispondente ai dettami della norma.

**6. L'esperienza della Direzione centrale della polizia criminale** La Direzione centrale della polizia criminale vanta un'esperienza pluriennale nella protezione dei dati personali: i primi accertamenti svolti dal Garante della privacy sul Ced interforze risalgono infatti al 2005. Sebbene, all'epoca, il tema di

un’efficace protezione dei dati personali non avesse ancora raggiunto l’attuale maturità, gli esiti furono confortanti ed il Garante giunse alla conclusione che non vi fossero profili di criticità, ma fosse comunque opportuno impartire delle prescrizioni “volte ad assicurare un rafforzamento del livello di protezione delle informazioni registrate nel Ced”. Successivamente, anche l’articolazione nazionale del Sistema informativo Schengen, N.SIS., fu sottoposta ad analoghi accertamenti che risultarono in prescrizioni volte all’innalzamento dei livelli di sicurezza e protezione dei dati personali.

Sempre con riferimento al Sistema informativo Schengen, la Commissione europea conduce regolari campagne di *audit* sui sistemi nazionali finalizzate alla verifica della corretta applicazione dell’*aquis* di Schengen, inclusi gli aspetti di protezione dei dati personali, con regolari campagne di audit, l'ultimo dei quali è stato eseguito nel mese di settembre 2021.

A distanza di tempo, il bilancio delle verifiche del Garante della privacy e della Commissione europea, seguite da ulteriori controlli sul rispetto delle prescrizioni emanate, non va letto soltanto in chiave di mero adempimento per rendere l’infrastruttura e i processi conformi alle prescrizioni (conformi alle norme lo erano già); in effetti, è stata l’occasione per una profonda riflessione e per un’evoluzione culturale che ha reso la disciplina della sicurezza informatica e della protezione dei dati parte integrante del Dna nello sviluppo dei sistemi informativi a supporto dell’attività di polizia. È anche grazie al confronto con il Garante della privacy iniziato nel 2005, a volte non privo di intensa dialettica, che la Direzione centrale ha potuto essere pronta, nel 2018, ad affrontare quel vero e proprio tsunami rappresentato dall’introduzione delle nuove norme europee.

La sfida di fronte alla quale è posta la Direzione centrale della polizia criminale è cruciale: in un periodo storico caratterizzato da forti preoccupazioni sulla potenziale lesività di trattamenti di dati personali, rinforzare la fiducia generale promuovendo una protezione dei dati personali matura e trasparente, e salvaguardare – anzi, se possibile, aumentare – l’efficacia dell’azione a tutela della *mission* istituzionale. Un esempio concreto è dato dall’istituzione, nel 2015, dell’Ufficio per la sicurezza dei dati, esempio pionieristico di struttura organizzativa finalizzata alla protezione dei dati personali, tra i primi nel panorama della pubblica amministrazione italiana e primo nelle forze di polizia, la cui vocazione è stata riaffermata nella recente riorganizzazione del Dipartimento della pubblica sicurezza mutandone la denominazione in un più pertinente “Ufficio protezione dati”. Il “bacino” di competenza dell’ufficio è delicatissimo, ha compiti di responsabile della protezione dei dati di tutti i sistemi informativi interforze: il Ced interforze, il Sistema Schengen nazionale (N.SIS.), la Banca dati nazionale del Dna e il recentissimo sistema Pnr (Passenger name records). L’ufficio ha sviluppato un notevole know-how che gli è valso anche il riconoscimento internazionale: rappresenta l’Italia nel ristretto Comitato permanente Interpol deputato alla revisione del Regolamento per il trattamento dei dati e, inoltre, fa parte della rete Eden (Europol data protection experts network).

Proprio in virtù del ruolo di punta ricoperto dall’Italia in questo settore, la Direzione ha organizzato a Roma, nel mese di ottobre 2021, la *7a Eden conference on data protection in law enforcement*, in partnership con Europol e con l’Accademia europea di diritto. L’evento annuale è particolarmente prestigioso poiché rappresenta un momento di confronto non soltanto tra le forze di polizia europee, ma è aperto al pubblico e vede la partecipazione di specialisti del settore provenienti dal mondo accademico, privato, dei media, a ulteriore dimostrazione dell’approccio di trasparenza e condivisione su un tema così delicato.

Tra le altre iniziative messe in campo dalla Direzione centrale della polizia criminale, volte alla tutela dei dati personali, rientra a pieno titolo il nuovo Cyber security operations center (C-Soc) delle banche dati interforze. Si tratta della realizzazione di una moderna e tecnologicamente avanzata struttura dedicata al monitoraggio *real time* (24/7) della complessa infrastruttura informatica delle banche dati interforze. In effetti, la capacità di un’infrastruttura di identificare prontamente un incidente informatico, attraverso l’attivazione di corrette procedure di gestione, risulta di cruciale importanza al fine di porre in essere efficaci azioni di risposta e di contenimento delle conseguenze dell’evento. La realizzazione di questo centro è quindi accompagnata dall’attivazione di processi e procedure – conformi sia agli standard nazionali ed internazionali in materia di sicurezza delle informazioni che ai dettami della norma – per consentire il riconoscimento e la gestione di eventuali incidenti informatici (cosiddetti *“data breach”*) con le conseguenti attività di escalation e notifica al Garante della privacy nei tempi – 72 ore – e nei modi previsti dalla normativa.

***L’audit*** Processo ispettivo di verifica di conformità di un servizio (o di un prodotto, o di un’organizzazione) rispetto a dei criteri predefiniti (tecnici, normativi, organizzativi o un mix dei tre) la cui caratteristica principale è l’indipendenza. L’audit, infatti, deve essere condotto da qualificati enti esterni, in condizione di totale terzietà rispetto alla realtà sotto osservazione e si basa sull’analisi di evidenze documentali, interviste al personale e osservazione delle prassi, con rigorosi metodi

scientifici. Quando ben eseguito, è uno strumento fondamentale per la crescita e il miglioramento continuo dell'organizzazione, del prodotto o del servizio in esame: non è (soltanto) un esame di maturità, ma un'opportunità per far emergere aspetti da migliorare. Insomma, non è un esercizio fine a sé stesso poiché non è fondamentale cosa si scopre durante un audit, ma come l'organizzazione evolve in relazione a cosa è emerso da questo.

***L'importanza dell'accuratezza dei dati*** Tra i princìpi che si applicano al trattamento di dati personali, oltre a quelli già illustrati nel testo, la legge prevede che i dati trattati siano "esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati".

L'importanza di questo concetto, a validità generale, è tanto più stringente e significativa se ci riferiamo ai dati contenuti nei sistemi informativi interforze. Pensiamo, ad esempio, al Sistema di indagine (Sdi), che contiene una notevole mole di dati personali e rappresenta il più vasto "contenitore" di dati utilizzato dalle forze di polizia.

L'art. 7 della legge 1 aprile 1981, n. 121 ("Natura e entità dei dati e delle informazioni raccolti") stabilisce i criteri per poter trattare quei determinati dati personali, ma da un punto di vista pratico, ai fini di un'efficace attività di polizia, che sia di prevenzione o repressione dei reati, inserire in una banca dati informazioni accurate e aggiornate significa, al momento del loro utilizzo, disporre di un concreto ausilio all'attività di istituto. Non serve un'eccessiva mole di informazioni, che alla fine rischiano – al contrario – di costituire una sorta di "rumore di fondo" né, tantomeno, sono utili informazioni non aggiornate: servono le informazioni "giuste" al momento "giusto".

---

**Sicurezza e privacy/1** *Ne parliamo con Agostino Ghiglia, componente del Collegio dell'Autorità garante della privacy*

**Sono passati 15 anni da quando il Garante della privacy ha svolto la prima verifica presso il Ced interforze. Come sono cambiate le cose da allora nella gestione dei dati personali da parte delle forze di polizia?** Faccio parte del Collegio del Garante dall'estate del 2020, ad alcune domande posso rispondere direttamente, per questa mi baso sugli atti di ufficio e sulle valutazioni del personale addetto. Nel 2005 gli accertamenti del Garante furono disposti per verificare l´idoneità delle misure di sicurezza anche a seguito di un´indagine penale nella quale venne contestato l´abusivo utilizzo di dati registrati nel Ced Interforze (Art. 12 l. n. 121 del 1981). Non emersero profili di violazione degli obblighi penalmente sanzionati di adozione delle misure minime di sicurezza, ma il Garante rilevò la necessità di impartire prescrizioni, limitatamente al profilo delle misure di sicurezza dei dati personali e dei sistemi, volte ad assicurare un rafforzamento del livello di protezione delle informazioni registrate nel Ced Interforze. Da allora la normativa si è affinata, e, nel rispetto della differenza dei ruoli, la collaborazione tra l'Autorità ed il Dipartimento è stata costante, sicché oggi spesso le cautele e le misure adottate dal Ced Interforze costituiscono per l'ufficio parametro di raffronto per le nuove iniziative in materia di istituzione di banche dati o di collegamento tra banche dati, per finalità di polizia.

**Il vostro è un osservatorio privilegiato. Come definireste il livello di maturità del sistema di protezione dei dati personali delle banche dati interforze, anche in raffronto agli omologhi organismi europei?** Non è facile rispondere a questa domanda. La Direttiva 680/2016 è il primo approccio globale alla protezione dati nel campo dell'attività di contrasto, in precedenza ciascuno strumento di contrasto era governato dalle proprie norme sulla protezione dei dati. Non abbiamo avuto occasione di esprimere valutazioni in qualche misura relative ad omologhe banche dati di altri Paesi europei, mentre quando personale del Garante partecipa a valutazioni all'estero, per es. per quanto riguarda Europol, ovvero nell'ambito delle valutazioni Schengen di altri Paesi, lo fa con esperti proposti dall'Autorità, la cui attività si svolge tuttavia nell'ambito del team di valutazione, senza riferire all'Autorità stessa. Posso però registrare con soddisfazione la conferma dell'autorevolezza del sistema italiano.

**Esiste realmente un'antitesi tra sicurezza pubblica e privacy e come garantire che la prima non avvenga a scapito della seconda? Come agisce il Garante in tal senso?** Più che di un'antitesi parlerei di un dialogo da prospettive diverse. Credo sia questa la ricchezza di un sistema pluralista, nella consapevolezza che l'adempimento del dovere di ciascuno porti al miglior equilibrio del sistema, e questo può farsi solo in posizione di ascolto reciproco, sicché per cambiare occorra agire insieme,

per riprendere lo spunto sulla teoria dei giochi. Il Garante, non solo in questo campo, ha il dovere di conoscere la realtà sulla quale incidono le sue valutazioni, e questo non sempre è facile, anche a prescindere dalle difficoltà generali che viviamo in questi tempi. Le valutazioni sono interdisciplinari, e cerchiamo sempre di vedere ogni questione dai due punti di vista, quello del soggetto che tratta i dati, qui con la finalità di pubblica sicurezza, e quello del soggetto i cui dati sono trattati. Nell'era dei *Big data* c'è la suggestione della semplicistica equazione quantità dei dati uguale qualità dei dati. La protezione dei dati nell'ambito delle attività di contrasto alla criminalità è lì anche per ricordare che la qualità dei dati non si ottiene per accumulo, e che i principi di accuratezza e pertinenza sono necessari proprio per l'efficacia dell'azione di indagine. Dunque da parte delle Autorità di protezione dei dati vi è la doverosa considerazione della delicatezza e complessità della materia. È di aiuto anche lo scambio con le altre Autorità in seno ai diversi gruppi di lavoro in ambito Ue. Hanno rilievo le decisioni dei giudici, anche di primo grado, perché forniscono la regola del caso concreto, a fronte di norme generali come quelle sulla protezione dei dati. Ovviamente non sempre le posizioni coincidono, ma direi che c'è considerazione per le posizioni dell'Autorità anche quando le decisioni ci sono sfavorevoli. In qualche caso le sentenze delle Corti europee hanno disegnato equilibri diversi da quelli che si riteneva di aver raggiunto, ma questo è il frutto di un sistema dotato nel suo insieme di un certo livello di coesione, senza la quale le decisioni sarebbero prive di effettività.

**La tecnologia è in continuo e sorprendente sviluppo, e con essa la preoccupazione di potenziali usi che potrebbero violare la privacy dei cittadini. Quali sono le prossime sfide e quali le cautele che i cittadini devono mettere in atto?** L'evoluzione degli strumenti va al di là di quanto possa prevedersi in un dato momento, perché è veramente un fenomeno globale. La sfida che proviene dall'intelligenza artificiale e da forme pervasive di controllo - tramite la raccolta l'analisi ed il confronto di immagini, di voci, di dati biometrici, di dati di natura disparata aggregati grazie ad enormi potenzialità di calcolo – riguarda in termini generali l'utilizzo della conoscibilità dei comportamenti umani e delle emozioni. Porre in essere cautele richiede, più che conoscenze specialistiche, consapevolezza da parte di ciascuno della complessità, ed equilibrio nelle scelte quotidiane, a cominciare dall'uso dei social media, ma questo non è affatto facile. Oggi sulle questioni tecnologiche possiamo fare un passo avanti, chiedendoci in che modo la tecnologia può aiutarci a mitigare i rischi della tecnologia stessa. La forbice si allarga: la tecnologia può darci grandissime capacità ma anche, potenzialmente, severe limitazioni alle libertà individuali. Il beneficio sarebbe solo apparente, se a spese delle libertà. In questo dibattito si parla di privacy by design proprio a questo scopo, integrare le tutele nel trattamento in modo da separare quanto più possibile i benefici dai rischi sin dalla progettazione delle tecnologie. È una sfida del nostro tempo, tecnologica e giuridica. Le Istituzioni possono contribuire non solo con le loro decisioni e operazioni, ma anche immettendo nel discorso comune elementi di conoscenza e riflessione, e perciò mi rallegro di questa iniziativa e credo che anche il Garante debba investire per creare spazi di approfondimento e confronto.

---

**Sicurezza e privacy/2** *Ne parliamo con Vittorio Rizzi, vicecapo del Dipartimento di pubblica sicurezza*

**Basta navigare in Rete per imbattersi nelle tesi più fantasiose e bizzarre, tra cui una ricorrente è quella secondo la quale la polizia sarebbe una sorta di grande fratello che può fare un po' quello che vuole con i dati dei cittadini. Stanno così le cose?** Assolutamente no. I sistemi informativi interforze sono istituiti in forza di leggi che ne regolano in modo rigoroso il funzionamento, i limiti e ne stabiliscono i meccanismi di controllo. Inoltre, proprio in virtù della delicatezza delle informazioni gestite, i nostri sistemi informativi sono sottoposti a regolari audit da parte del Garante della privacy e, nella massima trasparenza, gli esiti delle ispezioni, le relative prescrizioni e i provvedimenti sono disponibili sul sito web del Garante.

**La nuova normativa sta cambiando radicalmente lo scenario nella gestione dei dati personali nelle forze di polizia. Come si sta muovendo il Dipartimento della pubblica sicurezza in questo campo?** Prima di tutto promuovendo la massima trasparenza, poiché siamo fermamente convinti che questo sia un fattore determinante sia come operatori della sicurezza che come cittadini. È sufficiente andare sul sito della Polizia di Stato e delle altre forze di polizia per trovare tutte le informazioni riguardanti i sistemi informativi interforze, le norme che li regolano e semplici istruzioni per esercitare i propri diritti. In questo senso, la Direzione centrale della polizia criminale da anni dedica molta attenzione a gestire ogni richiesta che proviene dai cittadini, e stiamo parlando di più di 10.000 istanze l'anno, con un trend in costante crescita. Anche il fatto che siamo qui a parlare di questo argomento, dimostra il nostro impegno per la trasparenza. La Direzione centrale ha organizzato la 7a conferenza Eden, aperta a chiunque abbia voluto partecipare: questa è un'altra cristallina manifestazione del nostro impegno in questa direzione. Un altro fronte su cui ci si è mossi in maniera decisa è la formazione: consideri che per i corsi per dirigenti, la protezione dei dati personali è diventata una disciplina obbligatoria, stabilmente inserita nei nostri programmi formativi. Dal 2015, anno di istituzione

dell'Ufficio per la sicurezza dei dati, sono stati oggetto di formazione specifica più di 1.500 funzionari e ufficiali delle forze di polizia, e più di 1.000 unità di personale afferente ai ruoli agenti/assistenti e ispettori della Polizia di Stato, anche in modalità e-learning durante la corrente pandemia. L'istituzione di un ufficio dedicato, ancor prima dell'entrata in vigore della nuova normativa europea, è un ulteriore, tangibile segnale dell'attenzione rivolta a questo tema. Da ultimo, ma non certo per importanza, è il proficuo rapporto instaurato con il Garante della privacy: noi consideriamo il rapporto con quell'Autorità ad alto valore aggiunto, strategico, un'opportunità per fare le cose per bene dall'inizio, ancor prima di essere sottoposti a verifiche, e la disponibilità del Garante a esprimere il proprio punto di vista in questa sede ne è la conferma.

**La Direzione centrale della polizia criminale ha realizzato un proprio Cyber security operations center, il cosiddetto C-Soc, a protezione dei sistemi informativi interforze. Anche questa iniziativa va inquadrata nello scenario che ha appena descritto?** Esattamente. L'impegno della Direzione centrale è su entrambi i fronti: attenzione al cittadino e innovazione al servizio delle forze di polizia. La realizzazione del C-Soc è la sintesi di diverse esigenze, principalmente l'innalzamento dei livelli di sicurezza informatica delle banche dati interforze e la conformità alle più recenti prescrizioni in tema di protezione dei dati personali. Sicurezza informatica e protezione dei dati sono discipline differenti ma contigue, e noi abbiamo deciso di mettere nel C-Soc il meglio delle nostre risorse umane e strumentali in questo settore, e lo abbiamo fatto in grande, tra i primi in Europa e con il contributo dell'Europa, grazie anche ai Fondi europei ISF1. Adesso siamo dotati sia della più avanzata tecnologia che dei processi di prevenzione e reazione alla minaccia cyber, in conformità non solo alla normativa sulla privacy, mi riferisco in particolare agli obblighi in caso di "data breach", ma anche alla Direttiva NIS e al dpcm 30 luglio 2020, n. 131, il Regolamento in materia di perimetro di sicurezza nazionale cibernetica.

**Quali sono le strategie per fronteggiare un quadro così complesso e quali sono i temi che ci troveremo ad affrontare nel prossimo futuro?** La strategia è fare rete, sistema. Condividere i diversi saperi e la conoscenza. Non è possibile affrontare tematiche globali con un approccio diverso, e stiamo parlando peraltro di materie caratterizzate da intrinseca interdisciplinarietà, che vanno affrontate unendo tutte le intelligenze di cui siamo capaci. La condivisione, lo scambio delle informazioni e la loro robusta ed affidabile gestione sono il prerequisito fondamentale per assicurare un elevato livello di sicurezza interna in Europa e la libera circolazione delle persone nell'area Schengen, e un'efficace protezione dei dati personali è anch'essa un prerequisito fondamentale. In questo contesto, nel prossimo futuro, con l'adozione dei regolamenti che hanno introdotto i nuovi sistemi Entry exit system (Ees), European travel information and authorisation system (Etias) ed European criminal record information system for third-country nationals (Ecris-Tcn), verrà instaurato un processo per migliorare concretamente i sistemi informativi dell'Ue nei settori delle frontiere, dell'immigrazione, dei visti e della sicurezza nell'Unione europea: l'aggiornamento dei sistemi informativi esistenti, l'introduzione di nuovi e la loro interoperabilità determineranno l'individuazione di importanti mutamenti nell'architettura dei sistemi informativi centrali dell'area giustizia e affari interni nell'ottica, appunto, di cooperare sempre di più all'interno dell'Unione europea e non solo.

*direttore dell'Ufficio protezione dati della Direzione centrale della polizia criminale*

14/01/2022