fondazione fMC MAGNA CARTA

RISCHIO TERRORISMO

RICONOSCERLO PER PREVENIRLO

RISCHIO TERRORISMO

RICONOSCERLO PER PREVENIRLO

Finito di stampare Dicembre 2018

INTRODUZIONE

Il presente *policy paper*, individuando nella corretta gestione dei flussi migratori un veicolo per prevenire efficacemente il fenomeno terroristico, tratta delle modalità giuridiche tramite le quali procedere nella predisposizione di un sistema di rilevamento biometrico, nel dettaglio di riconoscimento facciale, al fine di poter identificare gli interessati, nella circostanza i migranti, e poter avere contezza della circolazione degli stessi sul territorio italiano al fine di prevenire eventuali reati legati a finalità terroristiche.

Per raggiungere tale scopo è doveroso tener presente che, nella predisposizione di un siffatto sistema, si debba obbligatoriamente porre l'attenzione sulla normativa italiana ed europea circa l'utilizzo dei sistemi biometrici sia in ambito di circolazione delle persone, sia in ambito di protezione dei dati personali.

Nel presente *policy paper*, pertanto, si è dettagliatamente analizzato il quadro prescrittivo sul tema biometria ed immigrazione, estrapolando un indirizzo programmatico adeguato agli obblighi che le normative italiane ed europee impongono.

SOMMARIO

1
TERRORISMO E FENOMENO MIGRATORIO

Non è agevole individuare una nozione corretta di terrorismo. Il concetto costituisce un fenomeno estremamente complesso poiché da un lato, le attività in cui può concretizzarsi sono molteplici ed eterogenee, e non è agevole riscontrarne gli elementi essenziali; dall'altro, è molto difficile anche stabilire quando un atto terroristico acquisti rilevanza internazionale, e di conseguenza quando possano valere le esigenze di cooperazione e assistenza reciproca tra Paesi per la repressione di tali fattispecie.[1] Dal punto di vista della ricerca di una definizione astratta e generale, l'elemento distintivo del terrorismo, rispetto a qualunque altra fattispecie criminosa, è senz'altro il carattere politico del fenomeno, accompagnato da una particolare efferatezza nella manifestazione della condotta con l'effetto di creare, nell'intero corpo sociale, uno stato di panico e disarticolazione, e lo stato di impotenza delle istituzioni di fronte ai reati commessi.

Il terrorismo, quindi, può ben definirsi come metodo di lotta politica fondato sul sistematico ricorso alla violenza, e caratterizzato dalla capacità di colpire chiunque appartenga a una data categoria sociale, secondo imprevedibili e variabili logiche di clandestinità e segretezza. Dal punto di vista soggettivo, l'elemento discriminante è la motivazione ideologica che sostiene il reato. L'ideologia, talvolta, prescinde anche dalla connotazione politica dell'agente, in quanto, la rilevanza sopranazionale del terrorismo, riflette una politicità di ampio respiro e non agevolmente riconducibile all'interno del perimetro delle identità che in uno o nell'altro Stato sono considerate.

In riferimento alle condotte terroristiche perpetrate durante gli anni '70 e nell'evoluzione di quella che erano, precedentemente agli anni '60, definiti come fenomeni anarcoidi e sovversivi, la rilevanza internazionale era un carattere soltanto eventuale, e poteva scaturire dalla fuga dell'agente all'estero o dalla diversa cittadinanza tra soggetto attivo e soggetto passivo. Negli ultimi decenni, a seguito anche degli eventi dell'11 settembre 2001, si sono diffuse nuove forme di terrorismo, dotate di un intrinseco rilievo internazionale, capaci di ledere non solo gli interessi degli Stati concretamente colpiti, ma anche gli interessi dell'intera Comunità internazionale alla sicurezza e al buon funzionamento delle relazioni diplomatiche[2].

Per una definizione più accurata del fenomeno terroristico deve essere necessariamente aperta una parentesi semantica per mostrare come il terrorismo e il fenomeno migratorio

1 DI LAZZARO, M.A., *Reati di terrorismo internazionale. Prospettive di repressione.*, Milano, 2001.
2 PANZERA, F., *Terrorismo - dir. internazionale - Enciclopedia del diritto vol. 154.*

da cui scaturisce siano implicitamente connessi e, di conseguenza, come sia impossibile separare i due concetti da costrutti logici che mirano a identificare il terrorista del nuovo millennio come l'ultima espressione autoreferenziale e antropocentrica dell'ideologia del terrore e quindi del maggior pericolo connesso al fenomeno migratorio. Il famoso assassinio dell'Arciduca Francesco Ferdinando, casus belli della prima guerra mondiale, fu un atto terroristico, che a quel tempo era ancora un crimine comune privo di una definizione adeguata. È passato un secolo da allora e, nonostante le dimensioni internazionali del terrorismo, la mancanza di un consenso internazionale su una singola definizione è ancora un problema ragguardevole e una conseguenza dell'esistenza di questo fenomeno criminale. Le difficoltà derivano principalmente dal fatto che le attività criminali da cui il terrorismo può materializzarsi e le finalità di tali atti variano a seconda del contesto storico e culturale in cui operano i diversi gruppi. È, inoltre, molto difficile persino stabilire quando un atto terroristico sia di importanza internazionale e, di conseguenza, quando possono fare affidamento sulla necessità di cooperazione e assistenza reciproca tra Paesi per il perseguimento di tali casi.

Non è facile identificare gli elementi essenziali del crimine guardando i materiali legislativi che anni di leggi antiterrorismo hanno prodotto nella comunità internazionale: dal 1937, l'anno della prima Convenzione sulla prevenzione e la punizione del terrorismo che "è stato ratificato solo da un singolo Paese"[3] e fino agli anni '70 del secolo scorso, le tipiche forme di eventi criminali terroristici erano connotate nella politica di contesto di un dato Stato, come precedentemente accennato. In riferimento a tali atti criminali, il significato internazionale era solo un possibile problema, e poteva derivare solo da una fuga criminale all'estero o da questioni emerse da diverse cittadinanze dei soggetti coinvolti. Di conseguenza, l'esperienza legislativa internazionale si intensificò quando nuove forme di terrorismo si diffusero con un'intrinseca importanza internazionale.

Esempi tipici, che sono stati fin troppo popolari negli ultimi anni, includono il dirottamento di aerei o navi, il rapimento e gli omicidi di diplomatici. Il risultato fu la creazione, in seno al Consiglio d'Europa, di un gruppo di esperti governativi con il compito di studiare i problemi posti dalle nuove forme di violenza concertate e la nascita del testo della Convenzione europea per la repressione del terrorismo che ha superato il controllo delle istituzioni competenti ed è entrata in vigore il 4 agosto 1978.

Esaminando le caratteristiche generali del documento, si nota innanzitutto che la Convenzione non ha stabilito una definizione di "terrorismo" ma adotta il *case report*, e i reati presi in considerazione, come oggetto di repressione, sono indicati negli articoli 1 e 2 e si riferiscono alla risposta che la comunità internazionale ha dato in quegli anni intesa a limitare alcuni oggetti del crimine, eludendo una definizione più generale della condotta criminale

3 MATERAL, M., *International Criminal Law,* 2009

dietro la parola "terrorismo", mirando specificamente a prevenire il dirottamento che costituiva la "nuova" minaccia a quei tempi[4]: la Convenzione di Tokyo del 1963 sui reati e alcuni altri atti commessi a bordo di aerei, la Convenzione dell'Aia del 1970 per la repressione del sequestro illegale di aeromobili e la Convenzione di Montreal del 1971 per la repressione degli atti illeciti contro la sicurezza dell'aviazione civile e quelli che sono stati adottati dopo il clima politico emerso negli anni del conflitto israelo-palestinese e dopo diversi incidenti durante i voli transnazionali. Con l'obiettivo di indirizzare i casi specifici di terrorismo ai singoli, sono imposti alle parti gli obblighi di impedire atti illeciti da parte dei responsabili di tali reati, attraverso un coordinamento tra le diverse giurisdizioni penali nazionali che è sancito dal principio fondamentale *aut judicare aut dedere* che non ha però risolto il problema di una definizione recepita all'unanimità.

La mancanza di una singola definizione di terrorismo ha portato ad un approccio tematico nei confronti le varie sfaccettature dell'attività terroristica, provenienti da altri Stati o entità non statali, che includevano rapimenti, protezione di materiali nucleari, attentati e, più recentemente, il finanziamento del terrorismo e la sua connessione con i flussi migratori.

Ricapitolando, quindi, il fenomeno è nato e si è sviluppato nella sua forma attuale a cavallo degli anni '60, ha subito cambiamenti di natura fondamentale a metà degli anni '80, con l'emergenza del chiaro coinvolgimento dei sostenitori degli Stati, l'intensità del terrorismo ha ripreso il centro della la scena internazionale di nuovo con nuove questioni negli anni Novanta, tra cui l'attacco al World Trade Center di New York nel 1993, il massacro di Oklahoma City nel 1995, il bombardamento della USS Cole attraccata nel porto di Aden nel 2000 manifestandosi, con l'11 settembre 2001, in quella che è oggi: una nuova rete di terrorismo transnazionale, da non confondere con i precedenti comportamenti e con le precedenti forme, che si differenzia dal passato a causa della crescita del fanatismo religioso come motivo scatenante delle azioni e del numero crescente delle vittime, per la maggiore competenza tecnologica degli attentatori, a causa del loro desiderio di ottenere armi chimiche, biologiche e di distruzione di massa e infine, alla possibilità, tramite internet, di attivare cellule dormienti, finanziarle ed istruirle nel *deep web*, confonderle nel flusso migratorio e colpire, pertanto, in maniera indisturbata. Gli esperti credono che le organizzazioni terroristiche di oggi possano essere supportate da forme di finanziamento autonome e diventino sempre più indipendenti e si debbano considerare le fonti di reddito per i gruppi terroristici molto diversificate: i terroristi tendono ad allineare la loro attività a quella delle organizzazioni criminali, come i cartelli della droga in Colombia o nel Sud-Est asiatico, i commercianti di diamanti in Africa, il commercio globale di oppio in Afghanistan, gli scafisti in Libia.[5]

---

4 VIGNA A.G., *La minaccia del terrorismo allo stato libero di diritto: i mezzi di difesa, in Critica Sociale*, 1979, p. 60

5 Centro informazioni sulla difesa degli Stati Uniti (CDI), *Combattere il finanziamento del terrorismo: un aspetto chiave della guerra al terrorismo.*

Una natura così cangiante del fenomeno terroristico e il suo progressivo associarsi al flusso migratorio, come modalità tramite la quale eludere gli strumenti di controllo degli Stati nazionali, rendono necessarie attività concrete per l'identificazione a fini preventivi dei soggetti potenzialmente interessati. L'identificazione, nel caso dei flussi migratori, è un problema che riguarda principalmente i Paesi sviluppati che si trovano quindi a fronteggiare molti problemi riguardanti la regolamentazione, il controllo in ingresso ed in uscita e la permanenza dei migranti.

2
IDENTIFICAZIONE È PREVENZIONE

La possibilità per gli esseri umani di essere identificati tramite caratteristiche che possano contestualizzarli in maniera univoca risalgono sorprendentemente ai tempi dell'antica Babilonia, dove gli strumenti biometrici finalizzati alla conclusione di negozi giuridici erano diffusi soprattutto per quanto riguarda le transazioni commerciali: era tramite le impronte digitali che il patto sinallagmatico alla base delle transazioni veniva sancito.

Non è strano che nell'antica nazione nota per la sua multietnicità si fossero sviluppati degli elementi che potessero coadiuvare nell'individuazione esclusiva di una persona fisica tramite le sue caratteristiche biometriche.

Negli ultimi anni, infatti, proprio grazie all'eliminazione di frontiere socio-culturali e geografiche, all'aumento esponenziale di circolazione di beni e servizi, l'avvento di internet e di tecnologie pervasive, si è manifestata l'esigenza di incrementare la sicurezza dei cittadini tramite l'utilizzo di tecnologie biometriche finalizzate ad agevolare il riconoscimento delle persone fisiche.

La gestione dei flussi migratori, come si diceva, è diventata una necessità incombente per gli Stati e, l'utilizzo di tecniche biometriche è diventato risolutivo e al fine di poter assistere le Autorità nello svolgimento dei compiti di identificazione dei migranti. La tecnologia e il progresso delle ultime decadi ha riportato, quindi, alla ribalta l'uso di tali strumenti ed il diritto, adeguandosi alla realtà attuale, ha mosso dei notevoli passi in avanti nell'individuare e mitigare i possibili rischi che un uso non regolamentato di tali strumenti possa implicare.

Diventa fondamentale, dunque, procedere ad un'analisi di diversi aspetti concernenti l'utilizzo della biometria nella gestione dei flussi migratori, individuando gli aspetti normativi relativi alla *privacy* e alla sicurezza informatica che, ad un primo impatto, sembrano maggiormente limitare l'utilizzo di tali tecnologie per gli scopi suddetti. Innanzitutto è necessario premettere che le tecniche di riconoscimento biometrico sono considerate già da tempo necessarie nell'espletamento delle attività giudiziarie e come strumento anticrimine. L'utilizzo delle impronte digitali nell'espletamento dell'attività giudiziaria e nell'investigazione non si è sviluppato negli ultimi decenni ma già nel corso del 1800.[6]

Ad oggi, però, la riduzione dei costi di creazione e gestione di tali tecnologie ne ha consentito l'espansione nel settore commerciale: tecniche di riconoscimento biometrico sono utilizzate come misure di autenticazione all'interno di svariati sistemi, sia nel campo della

6 AMATO S., CRISTOFARI F., *Biometria: i codici a barre del corpo*, Giappichelli, Torino, 2013.

telefonia mobile, sia nel campo finanziario, con applicazione sempre più frequente di strumenti di autenticazione biometrica finalizzati a garantire ai cliente degli istituti di credito maggiori sicurezze nell'accesso e gestione dei propri conti correnti e carte di credito, utilizzando inoltre i sistemi di riconoscimento facciale nei punti di accesso per verificare l'identità del personale e degli appaltatori esterni o per autenticare i pagamenti e ridurre le frodi nelle applicazioni di *mobile banking* e agli sportelli automatici.

Tale uso crescente delle tecniche di rilevamento biometrico hanno condotto, come precedentemente accennato, il legislatore europeo ad innovare le discipline giuridiche riferite alla biometria con due approcci diversi ma, come si vedrà più avanti, conciliabili.

Il legislatore europeo, infatti, con una duplice prospettiva ha inteso regolamentare e cristallizzare l'utilizzo delle tecniche di riconoscimento biometrico. Da un lato con la regolamentazione dei flussi migratori, ha previsto per gli Stati membri la possibilità di utilizzare tecnologie per il rilievo biometrico al fine di predisporre il rilascio di visti, di favorire la circolazione all'interno dell'Unione Europea e di poter avere contezza, con scopi di prevenzione, individuazione ed investigazione, della presenza e degli spostamenti dei migranti sul suolo europeo. Per altro verso, invece, la normativa in materia di *privacy*, Regolamento Europeo 679/2016, d'ora in avanti "GDPR" classifica i dati biometrici come dati particolari e ne vieta l'utilizzo a meno di soddisfare requisiti altrettanto "particolari", che saranno descritti più avanti. Non ultimo, il legislatore italiano, prima con il Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014 e, successivamente, con il recente Decreto Legislativo n.101/2018 del 10 agosto 2018, innovando la disciplina del D.Lgs 196/2003, pone l'accento sulle necessarie misure tecniche ed organizzative da dover adottare al fine di poter utilizzare dati biometrici legittimamente. Il quadro giuridico europeo ed italiano risulta quindi complesso e di non semplice analisi, stante la difficoltà nel fornire una chiara definizione dei sistemi biometrici stessi.

3
TECNICHE BIOMETRICHE DI RICONOSCIMENTO FACCIALE

Il *Working Party* 29, di seguito WP29, ha descritto i sistemi biometrici come "applicazioni che utilizzano tecnologie biometriche, che consentono l'identificazione automatica e/o l'autenticazione/verifica dell'identità di una persona." Nel parere 3/2012, infatti, coerentemente con quanto sopra esposto circa il carattere di incertezza che permea il quadro definitorio, un sistema biometrico è stato definito come "sistema che estrae ed elabora ulteriormente dati biometrici."[7]

Muovendo quindi da un framework giuridico variegato e potenzialmente caotico è d'uopo procedere con l'analisi di quello che è lo stato dell'arte del sistema biometrico adeguato e più vantaggioso per la gestione dei flussi migratori.

Le caratteristiche fondamentali al fine di poter determinare il sistema biometrico più efficace sono tre: universalità, unicità e persistenza.

Si intende per universalità la presenza in tutti gli individui di quegli elementi distintivi che si analizzano e la loro possibilità di essere agevolmente utilizzati ai fini del riconoscimento. Si può evidenziare come un recente studio ha determinato che gli esseri umani già da feto, nel grembo materno, siano in grado di riconoscere i volti, pertanto, può agevolmente considerarsi il riconoscimento facciale attributo innato dell'essere umano e, quindi, universale.[8]

Relativamente agli aspetti di unicità e persistenza, necessari al fine di differenziare due individui, si segnala come le tecniche biometriche afferenti al riconoscimento facciale si basino sull'effettuazione di una individuazione ed un'analisi degli elementi non alterabili del viso quali l'incavo osseo degli occhi, i lati della bocca, gli zigomi, l'arcata frontale, la distanza degli occhi, la conformazione di mascella e mento. Tali elementi, per quanto non particolarmente cangianti nel breve periodo, risultano comunque alterabili nel lungo periodo. La possibilità che l'alterazione del viso influenzi il processo di riconoscimento e infici quindi alla base l'utilità di tali tecniche può non essere presa in considerazione stante il circoscritto contesto nel quale la si analizza, ovvero la prevenzione del terrorismo nella gestione dei flussi migratori. Tali flussi migratori analizzati non sono caratterizzati dalla permanenza del migrante nel territorio ospitante, la cui identificazione potrebbe essere agevole tramite

7 Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies*, 720/12/EN, 2012
8 REID, V., *The Human fetus preferentially engages with face-like visual stimuli*, Current Biology, 2017.

altri elementi assimilabili dai contesti socio economici nei quali l'individuo si sedimenta (es. richiesta di permessi di soggiorno), bensì sono volti a coadiuvare le identificazioni di quei migranti che compongono la massa di movimenti interni ad un Paese e tra altri Paesi, e che, pertanto, pongono maggiori difficoltà stante l'assenza di elementi ulteriori utilizzabili ai fini identificativi. Un'analisi svolta in un siffatto contesto consentirebbe quindi di soprassedere circa la valutazione di non efficacia del sistema di riconoscimento facciale con riguardo all'alterabilità naturale del volto umano, anzi, tale sistema potrebbe certamente essere considerato come il più efficace poiché consente di riconoscere il migrante in movimento tramite strumenti che non ne blocchino l'incedere o che non richiedano un'interazione immediata.

Riassumendo, preso in considerazione un lungo periodo di tempo possono presentarsi molte difficoltà nel riconoscimento facciale nelle sue caratteristiche necessarie di unicità e persistenza, come conseguenza di eventi intenzionali o non intenzionali, come lesioni, chirurgia, crescita della barba o uso degli occhiali ma, nel periodo limitato di tempo necessario a studiare il movimento del flusso migratorio in divenire, invece, potrebbero risultare ampiamente efficaci.[9]

È necessario produrre una sintesi del funzionamento di un sistema biometrico prodromica all'individuazione delle modalità in cui tale sistema espleta il suo processo, in maniera tale da poter ravvisare gli eventuali rischi, da considerare necessariamente nell'ottica di valutazione tecnico-giuridica che le normative europee impongono e che verranno più avanti delineate nella loro interezza.

I sistemi biometrici raccolgono e memorizzano caratteristiche biologiche tipiche degli individui finalizzate alla verifica automatizzata per l'identificazione degli stessi. Tali processi di verifica si estrinsecano tramite un *matching one-to-one* o un *matching one-to-many.* La differenza sostanziale tra i due *matching* consiste nella quantità di dati a disposizione e nello scopo per i quali sono utilizzati.

Il *matching one-to-one* associa il dato biometrico ad una specifica caratteristica precedentemente memorizzata e consente un riconoscimento positivo, ovvero associa la componente biometrica con un codice identificativo precedentemente memorizzato che ne valida la corrispondenza. È una funzione principalmente utilizzata al fine di impedire a persone diverse di attribuirsi la stessa identità. Il *matching one-to-many*, d'altro canto, ha lo scopo di identificare un individuo attraverso una ricerca dei modelli di tutti gli utenti esistenti in un *database* e impedisce ad un individuo di utilizzare identità multiple consentendo un più agevole riconoscimento.

9 VACCA, J., *Biometric Technolgies and Verification Systems,* Elsevier, 2007

Nel quadro sinora prospettato, per quanto sia possibile utilizzare sistemi biometrici dotati di *matching one-to-one*, essi risultano carenti dell'assenza di una necessaria intermediazione e, pertanto, della possibilità di automatizzare i processi: il confronto con dati identificativi già acquisiti nel contesto dei flussi migratori potrebbero risultare particolarmente ostico stante l'assenza di documenti d'identità esistenti o verificabili in possesso dei migranti.

Prendendo in considerazione quindi unicamente il funzionamento dei sistemi biometrici dotati di *matching one-to-many*, si delineano tre fasi tecniche consistenti in iscrizione, confronto e decisione.

L'iscrizione consiste nell'estrapolazione delle caratteristiche fisionomiche individuali creando un modello digitalizzato. La fase di confronto consiste nella comparazione tra il dato digitalizzato e i campioni precedentemente raccolti. La fase di decisione consiste in identificazione e verifica, intesi come i processi tramite i quali si associano modello e campione per stabilire un'identità o verificarne l'esattezza.[10] Occorre segnalare come una corrispondenza biometrica non implica *ex se* un riconoscimento preciso ma piuttosto si è in presenza di una probabilità che un riconoscimento abbia avuto un esito positivo in termini di correttezza mentre una non corrispondenza fa insorgere una probabilità che la persona sia sconosciuta al sistema. Il riconoscimento facciale, come sistema di riconoscimento biometrico, presenta caratteristiche intrinseche che aumentano le probabilità di riconoscimento poiché, gli sviluppi nei sistemi di acquisizione dei connotati fisionomici del volto sono tecnologicamente ampiamente sviluppati e consentono di acquisire immagini di buona qualità tramite dispositivi presenti nella vita quotidiana, come gli smartphone.

Le tre fasi descritte riguardanti i sistemi biometrici in generale sono maggiormente dettagliati nell'Opinione 2/2012 del WP29 nel caso delle tecniche di riconoscimento facciale e constano in quattro differenti fasi. La prima fase riguarda il rilevamento del volto, la seconda fase consiste nella standardizzazione dell'acquisizione fisionomica, la terza fase è relativa nell'estrazione della caratteristica da confrontare mentre la quarta fase afferisce al riconoscimento. Lo stesso WP29 delinea come sia fondamentale la fase afferente al riconoscimento, definita di iscrizione, poiché, nel caso in cui un individuo sia sottoposto a tecniche di riconoscimento facciale per la prima volta, tali immagini possono essere archiviate al fine di procedere a successivi confronti assurgendo pertanto a modello e per procedere, inoltre, a quella che il WP29 definisce categorizzazione ovvero l'estrapolazione di caratteristiche delle immagini degli individui tali da poter catalogare le stesse in base a diversi attributi quali etnia, età, sesso, consentendo, pertanto, un riconoscimento che prescinda dall'identificazione dell'individuo ma che si assesti su specifici elementi distintivi dello stesso.[11]

10 Article 29 Data Protection Working Party, *Working document on biometrics, 720/12/EN,* 2013

11 Article 29 Data Protection Working Party, *Opinion 2/2012 on facial recognition in online and mobile devices, 727/12/EN,* 2012

4
LE NORMATIVE INTERNAZIONALI IN TEMA DI IMMIGRAZIONE E BIOMETRIA

4.1. Gli Stati Uniti d'America e l'impulso all'utilizzo della biometria su scala globale

Poco dopo l'11 settembre un gran numero di iniziative normative e nuove leggi sono state emanate dal Congresso degli Stati Uniti d'America per aumentare le misure di sicurezza per la prevenzione dei fenomeni terroristici, poiché si è palesata immediatamente rilevante la forte connessione tra i documenti di viaggio, la lotta al terrorismo e l'utilizzo di sistemi biometrici.

La commissione sugli attacchi terroristi dell'11 settembre evidenziò come "per i terroristi, i documenti di viaggio sono importanti quanto le armi."[12]

Il Congresso degli Stati Uniti ha trattato un gran numero di proposte per una nuova legislazione che coinvolgesse l'utilizzo della biometria e altre tecnologie di sicurezza e tale analisi giuridica portò all'emanazione del *Patriot Act*, alla creazione del *Department of Homeland Security* e del programma VISIT. Tale programma ed il successivo programma *Visa Weiver* hanno implementato l'acquisizione di impronte digitali e riconoscimento facciale tramite scansione per tutti i cittadini stranieri in ingresso o in uscita dagli Stati Uniti, ponendo come base identificativa per il flusso migratorio l'utilizzo di parametri biometrici. Non di meno ha assunto notevole rilevanza l'interoperabilità delle informazioni raccolte tramite biometria al fine di condividere efficacemente le informazioni sui flussi migratori tra le varie agenzie governative operanti sul territorio statunitense.

I requisiti di tale interoperabilità si sono sostanziati in due elementi di importanza cruciale a livello programmatico: l'interoperabilità *by design* e la rimozione delle barriere legali e culturali che impediscono il corretto interscambio informativo. L'applicazione di un tale disegno si è concretizzata considerando l'informazione biometrica il miglior mezzo attraverso il quale consentire la connessione di fonti di informazione precedentemente non collegate contenute in diversi database rilevandosi vantaggioso in termini operativi e organizzativi. Per quanto ciò si sia rivelato solo un discreto miglioramento nella tematica di gestione dei passaporti poiché si possedevano già dati quali nazionalità, data di nascita, sesso e codici identificativi, nel caso di pratiche esistenti non automatizzate l'uso della biometria si è manifestato come essenziale.

12 National Commission on Terrorist Attacks on United States, 384, 2004

I processi di rilevazione delle impronte digitali nel caso di accesso fisico ad edifici controllati o relativi all'identificazione dei detenuti non hanno posto evidenti problemi di operatività mentre l'aumento considerevole delle utenze da attenzionare tramite il programma *US Visit*, che ha registrato già nel 2007 un numero di ingressi superiore alle quarantacinque milioni di unità, hanno richiesto un diverso approccio relativo alla sicurezza.

Stante la circostanza che vede impronte digitali e altri sistemi biometrici potenzialmente utilizzabili per identificare gli individui, le autorità governative potrebbero avere difficoltà a raccogliere le impronte digitali o le scansioni dell'iride di terroristi sospetti per costruire il database con cui confrontare un individuo sconosciuto.

I sistemi biometrici di riconoscimento facciale, tuttavia, offrono un modo per aggirare il problema. In particolare, i sistemi di riconoscimento facciale consentono l'identificazione di un terrorista sospetto anche se le uniche informazioni identificative possedute consistono in una fotografia. [13]

Nel contesto europeo, essendo geograficamente più agevole l'arrivo di migranti che possano eludere gli strumenti di controllo posti nelle frontiere dell'Unione, tali strumenti potrebbero risultare maggiormente efficaci. Bisogna in ogni caso considerare come gli Stati Uniti d'America non dispongano di norme federali relative alla *privacy*, pertanto, la gestione dei sistemi di riconoscimento facciale nella folla non pone particolari problemi giuridici ed è considerata quindi un'opzione accolta favorevolmente.

La visione statunitense della biometria come misura di sicurezza nella gestione dei flussi migratori è stata esportata principalmente attraverso due organizzazioni internazionali: il G8 e l'Organizzazione internazionale dell'aviazione civile, ICAO. Il G8 ha fornito un forum in cui i leader del mondo industrializzato hanno accettato di discutere relativamente all'introduzione della tecnologia *de quo*; l'ICAO ha elaborato specifiche tecniche al fine di promuovere la standardizzazione e l'interoperabilità di tali sistemi su scala globale. La Risoluzione di Berlino del 2002 dell'ICAO ha sancito il riconoscimento facciale come lo standard interoperabile a livello globale per passaporti e documenti di viaggio con il documento ICAO n. 9303, rendendo il riconoscimento facciale il dato biometrico primario e obbligatorio.

4.2. L'approccio dell'Unione Europea

Il WP29, nell'*Opinion 3/2013* sulla limitazione delle finalità del trattamento ha delineato come i dati personali possano essere trattati unicamente nel contesto di scopi predeterminati ed espliciti e tale principio è stato inoltre cristallizzato nell'art. 5.1.b del GDPR, arric-

13 WOODWARD, J., *Biometrics: Facing up to terrorism,* RAND Arroyo Center, 2001

chendo il quadro giuridico di riferimento. I dati personali quindi possono essere raccolti unicamente per scopi specifici espliciti e legittimi e tale legittimità è stata evidenziata dalla Corte di Giustizia dell'Unione Europea per quanto riguarda l'utilizzo di dati personali finalizzato alla prevenzione dei crimini, delegando agli Stati membri la possibilità di individuare correttamente i criteri oggettivi tramite i quali le Autorità competenti possano trattare dati personali.[14]

Alla luce delle presenti considerazioni è necessario analizzare come le normative europee in tema di immigrazione delineino come legittimo l'utilizzo di sistemi informatici prodromici alla regolamentazione dei flussi migratori specificatamente richiamando l'attenzione sulle dinamiche di rimpatrio dei migranti irregolari e sulla prevenzione e lotta al terrorismo.

In Europa, pertanto, ogni Stato membro ha la responsabilità del controllo dei propri confini, coadiuvato dalla Commissione Europea che pone l'accento sulla necessaria collaborazione tra Stati membri al fine di ridurre l'immigrazione illegale, facilitare l'attraversamento dei confini esterni per i viaggiatori in buona fede, combattere il terrorismo e la criminalità organizzata e migliorare la gestione dei flussi migratori.

L'Unione Europea, di conseguenza, ha creato diversi sistemi informativi condivisi al fine di agevolare l'interscambio di informazioni tra Paesi membri per il raggiungimento degli scopi summenzionati e tali sistemi includono la possibilità di utilizzare dati biometrici. Da un punto di vista legislativo la formalizzazione di tali obiettivi risale al 2004, quando, creando il sistema FRONTEX e il Regolamento 275/2000, mirato ad agevolare l'individuazione tramite riconoscimento biometrico dei richiedenti asilo, si è istituito e consolidato un *framework* normativo comunitario relativo alla gestione dei flussi migratori.

Il sistema VIS, inoltre, nato anch'esso nel 2004, ha agevolato la procedura relativa alle domande di visto all'interno dell'Unione, prevedendo un sistema centrale e diversi sistemi nazionali che condividono dati che comprendono una fotografia del richiedente e le impronte digitali di entrambe le mani.

4.2.1. SIS e SIS II

I SIS Schengen, ovvero sistema informativo Schengen I e II, sono nati come conseguenza della introduzione di uno spazio di libera circolazione delle persone, con la soppressione dunque dei controlli alle frontiere interne degli Stati membri, mediante l'accordo di Schengen e consistono nell'introduzione di un sistema in grado di garantire ordine e sicurezza negli Stati membri. Si tratta di garantire un sistema di informazione comune estrinsecatosi

14 CGUE, *cause riunite C-293/12 e C-593/12*, 2014

nell'utilizzo collettivo da parte degli Stati di un database centralizzato alimentato dai database nazionali sul quale confluiscono i dati rilevanti ai fini del monitoraggio del fenomeno migratorio e della lotta al terrorismo per coadiuvare le cooperazioni internazionali e colmare eventuali lacune potenziali nel sistema di sicurezza comunitario. Tale sistema consente l'accesso in tutto lo spazio europeo, per le Autorità, ai dati dei non cittadini di uno Stato membro dello spazio Schengen, ai quali non è consentito entrare o anche circolare nello spazio Schengen.

L'8 novembre 2017 il Comitato dei rappresentanti permanenti ha approvato il mandato per i negoziati su tre regolamenti relativi all'uso del sistema d'informazione Schengen nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, nel settore delle verifiche di frontiera e per quanto riguarda il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare. I progetti di regolamento introducono la possibilità di utilizzare tecniche di riconoscimento facciale a fini di identificazione, in particolare per garantire la coerenza nelle procedure di controllo di frontiera.[15]

4.2.2. Eurodac

Prendendo in considerazione il regolamento n. 603/2013 del Parlamento europeo e del Consiglio del 26 giugno 2013 che riforma il sistema Eurodac si riscontra come l'approccio dell'Unione Europea nei confronti dell'utilizzo di dati biometrici relativi al riconoscimento facciale si sia modificata prevedendo tali soluzioni come necessarie ai fini della collaborazione delle Autorità per la prevenzione e lotta contro la minaccia terroristica. Eurodac è un database biometrico comunitario che contiene le impronte digitali dei richiedenti asilo e dei cittadini di Paesi terzi ed è utile al confronto di questi dati fra gli organi preposti dei vari Stati membri con il controllo della preposta Agenzia Europea per la gestione operativa dei sistemi, che regola l'utilizzo dei dati raccolti.

Gli obiettivi del Regolamento Eurodac consistono nella semplificazione dell'assegnazione della competenza per l'esame delle domande d'asilo e la possibilità per le Autorità preposte al contrasto al terrorismo internazionale di operare utilizzando i dati raccolti.

Il sistema Eurodac obbliga ogni Paese membro a raccogliere le impronte digitali dei richiedenti asilo e trasmetterle al sistema stesso se trovato illegalmente in un Paese membro e in caso di indagini per terrorismo o altri reati gravi. Una recente proposta di riforma del sistema Eurodac prevede l'implementazione di misure biometriche ulteriori rispetto alle impronte digitali quali il riconoscimento facciale.[16]

15 Dal sistema d'informazione Schengen (SIS 1+) al sistema d'informazione Schengen di seconda generazione (SIS II) - eur-lex.europa.eu/legal-content/IT/TXT/?URI=LEGISUMM%3Ajl0010

16 Identification of Applicants - Migration and Home Affairs - ec.europa.eu

4.2.3. Ecris-TCN

Entrato in funzione nell'aprile 2012, ECRIS è il sistema europeo di informazione sui casellari giudiziali. La relativa disciplina è contenuta nella decisione quadro 2009/315/GAI e della decisione 2009/316/GAI. In sostanza, ECRIS si basa su una struttura decentrata di interconnessione fra gli Stati membri che consente lo scambio di informazioni prese dai casellari giudiziali.

La proposta prevede che il *record* di dati possa contenere anche le immagini del volto del cittadino di Paese terzo condannato, definendo altresì un regime specifico per tale tipologia di informazione. In particolare, l'articolo 6 stabilisce che le immagini del volto siano utilizzate al solo scopo di confermare l'identità del cittadino di paese terzo identificato grazie all'interrogazione con dati alfanumerici o con dati relativi alle impronte digitali. Il medesimo articolo tuttavia prevede che tali immagini possano essere utilizzate anche per identificare un cittadino di Paese terzo in base al suo identificatore biometrico.[17]

17 Report on the proposal for a regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011 (COM(2017)0344 – C8-0217/2017 – 2017/0144(COD)) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2018 0018+0+DOC+XML+V0//EN

5
LA NORMATIVA EUROPEA ED ITALIANA RELATIVA ALLA PROTEZIONE DEI DATI PERSONALI

Sul fronte della protezione dei dati personali all'interno dell'Unione Europea, mentre da un lato si intensificano le proposte per l'utilizzo di dati biometrici quali i dati relativi al riconoscimento facciale dei migranti, dopo anni di discussione e negoziazione, è stato adottato il Regolamento 679/2016 "GDPR" che sostituisce la direttiva 95/46/CE e pone l'accento sulle misure di protezione necessarie al fine di poter trattare i dati biometrici.

Indipendentemente dal luogo di residenza, le organizzazioni che raccolgono ed elaborano dati personali dei cittadini dell'Unione Europea dovranno conformarsi ai requisiti imposti dalla normativa europea e, in mancanza di adeguamento, il rischio per le aziende è di incorrere in sanzioni finanziarie fino al 4% del fatturato globale annuo e subire dei conseguenti notevoli danni reputazionali.

5.1. Definizioni

Un dato personale, nella lettura del Regolamento, è una qualsiasi informazione riguardante una persona fisica identificata o identificabile, l'"interessato"; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Per trattamento si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come 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.

È necessario, quindi, definire correttamente le tipologie di dati personali. Si definiscono dati comuni tutti i dati personali che non appartengono alle categorie dei dati particolari e giudiziari dove questi ultimi sono dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza mentre i dati particolari sono dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco

una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Ai fini di una corretta lettura del disposto normativo è d'uopo distinguere dati genetici, dati biometrici e dati relativi alla salute. I dati genetici sono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione. I dati relativi alla salute, e che quindi godono di maggior tutela, sono i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute. I dati biometrici, nella prospettiva del Regolamento, sono i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

A meno di condizioni che verranno più avanti esaminate e che sono esposte nell'art. 9.2. del GDPR, il trattamento dei suddetti dati particolari, compresi quelli biometrici, può essere consentito solo previo consenso dell'interessato, definito come qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva che implichi un assenso a ché i dati personali che lo riguardano siano oggetto di trattamento.

Particolare attenzione è posta dal legislatore europeo sul tema della violazione dei dati personali, il cosiddetto *data breach*, che è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Un focus particolare è dedicato anche al tema della profilazione, intesa come qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona. Parimenti il GDPR disciplina la tematica del trattamento automatizzato inteso come una decisione basata unicamente sul trattamento automatizzato stesso, compresa la profilazione, che produca effetti giuridici che riguardano l'interessato o che incida in modo analogo significativamente sulla sua persona.

Il GDPR pone al centro, inoltre, il tema della pseudonomizzazione dei dati personali inteso come il trattamento dei dati personali in modo tale che gli stessi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condi-

zione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. Tali forme di protezione devono essere poste in essere dal titolare e/o dal responsabile del trattamento, intesi come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri e, per quanto riguarda il responsabile del trattamento, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

L'art. 37 del GDPR inoltre crea la figura del *Data Protection Officer,* d'ora in avanti DPO, che è una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37.1 GDPR dal titolare del trattamento o dal responsabile del trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR.

Ai fini di scongiurare trattamenti di dati che possano ledere i diritti e libertà delle persone fisiche, il Regolamento delinea una metodologia per valutare l'impatto sui diritti e le libertà delle persone fisiche di un progetto, servizio, applicazione, programma, prodotto o qualsiasi altra iniziativa che implichi il trattamento di dati personali che presenta alti rischi per i suddetti diritti e libertà delle persone fisiche e, dopo aver consultato tutti i terzi coinvolti nel trattamento dei dati e il DPO, consente di prendere le misure necessarie per evitare o minimizzare l'impatto negativo. Si tratta di un processo continuo che deve iniziare nella fase più preliminare possibile del progetto, servizio, applicazione, programma, prodotto o iniziativa, quando, sia ancora possibile influenzarne il risultato, in modo tale da garantire la *privacy by design* di cui si dirà più avanti.[18]

5.2. Ambito di territorialità

Nella necessaria disamina riguardante il *framework* normativo preso in considerazione risulta fondamentale analizzare l'ambito di applicazione territoriale e materiale del Regolamento.

Il Regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile

18 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) - https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679

del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione. Il Regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

L'applicazione del Regolamento, pertanto, dipende dall'applicazione congiunta di una serie di criteri non solo geografici ma anche logici e di destinazione delle attività svolte dal titolare o dal responsabile del trattamento. Il paragrafo 2 non può essere interpretato, quindi, nel senso che gli interessati devono risiedere nell'Unione, è sufficiente per essi la mera presenza sul territorio europeo. I considerando 2 e 14 chiariscono meglio tale prospettiva. Nel considerando 2 si afferma: *"I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche"*. Il considerando 14 approfondisce la tematica dell'applicazione che prescinde dalla nazionalità con il seguente tenore: *"È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto."*

Un approccio diverso inoltre sarebbe negato anche dalla lettura dei *travaux preparatoires* prodromici all'emanazione del Regolamento poiché il riferimento alla residenza nell'Unione era stato presentato nell'iniziale proposta e poi superato, inoltre la scelta terminologica stessa fa esplicito riferimento ad una condizione non stabile estendendosi al mero passaggio all'interno del territorio dell'Unione, producendo tutele giuridiche anche per coloro i quali si trovino in uno stato transitorio.

Dal punto di vista del monitoraggio dei comportamenti precisato dall'art. 3.2.b risulta necessario, ai fini interpretativi, fare riferimento al contenuto del considerando 24: *"È opportuno che anche il trattamento dei dati personali degli interessati che si trovano nell'Unione ad opera di un titolare del trattamento o di un responsabile del trattamento non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al monitoraggio del comportamento di detti interessati, nella misura in cui tale comportamento ha luogo all'interno dell'Unione. Per stabilire se un'attività*

di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali."[19]

5.3. L'uso di sistemi biometrici di riconoscimento facciale per scopi di prevenzione del terrorismo alla luce del GDPR e della Direttiva 680/2016

Da qui l'importanza di analizzare come un sistema di raccolta dei dati biometrici tramite riconoscimento facciale, che abbia le caratteristiche tali da consentire di poter studiare ed analizzare lo spostamento dei migranti sul territorio dell'Unione, al fine di prevenire atti di terrorismo, sia consentito unicamente nel verificarsi di alcune circostanze che, si nota, non esauriscono però la necessaria prudenza che nella creazione di un sistema siffatto deve essere obbligatoriamente prestata.

L'art. 2 del GDPR infatti, alla lettera d), dispone che il Regolamento non si applichi ai trattamenti di dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Il considerando 16, infatti, sancisce che il regolamento non si applica a questioni di tutela dei diritti e delle libertà fondamentali o di libera circolazione dei dati personali riferite ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività riguardanti la sicurezza nazionale. Il Regolamento non si applica al trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività relative alla politica estera e di sicurezza comune dell'Unione.

In tal senso è ancora più chiara la disposizione contenuta all'interno del considerando 19 che afferma come la protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, e la libera circolazione di tali dati sono oggetto di uno specifico atto dell'Unione. Il Regolamento non dovrebbe pertanto applicarsi ai trattamenti effettuati per tali finalità. I dati personali trattati dalle autorità pubbliche in forza del presente regolamento, quando utilizzati per tali finalità, dovrebbero invece essere disciplinati da un più specifico atto dell'Unione, segnatamente la direttiva 2016/680

19 ibid

del Parlamento europeo e del Consiglio.[20] Gli Stati membri possono conferire alle Autorità competenti ai sensi della Direttiva 2016/680 altri compiti che non siano necessariamente svolti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, affinché il trattamento di dati personali per tali altre finalità, nella misura in cui ricada nell'ambito di applicazione del diritto dell'Unione, rientri nell'ambito di applicazione del Regolamento. Con riguardo al trattamento dei dati personali da parte di tali Autorità competenti per finalità rientranti nell'ambito di applicazione del Regolamento, gli Stati membri dovrebbero poter mantenere o introdurre disposizioni più specifiche per adattare l'applicazione delle disposizioni del Regolamento. Tali disposizioni possono determinare con maggiore precisione requisiti specifici per il trattamento di dati personali da parte di dette Autorità competenti per tali altre finalità, tenuto conto della struttura costituzionale, organizzativa e amministrativa dei rispettivi Stati membri. Quando il trattamento dei dati personali effettuato da organismi privati rientra nell'ambito di applicazione del Regolamento, è opportuno che lo stesso preveda la facoltà per gli Stati membri, a determinate condizioni, di adottare disposizioni legislative intese a limitare determinati obblighi e diritti, qualora tale limitazione costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia di importanti interessi specifici, comprese la sicurezza pubblica e le attività di prevenzione, indagine, accertamento e perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica.

Alla luce di un siffatto quadro normativo è altresì necessario analizzare il contenuto della direttiva 680/2016, recepita in Italia con il D.Lgs 51/2018 pubblicato il 24 maggio 2018.[21]

L'obiettivo della Direttiva è quello di agevolare lo scambio e l'impiego dei dati giudiziari al fine di rendere maggiormente efficaci la prevenzione e gli strumenti di contrasto della criminalità e terrorismo. Le disposizioni del Decreto che ha recepito la Direttiva si applicano a norma dell'art.1 ai *"trattamenti interamente o parzialmente automatizzati di dati personali delle persone fisiche contenuti in un archivio o ad esso destinati, svolti dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica"*.

---

20 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio - https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ITA

21 DECRETO LEGISLATIVO 18 maggio 2018, n. 51 Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonchÈ alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. (18G00080) (GU Serie Generale n.119 del 24-05-2018)

Direttiva, decreto di recepimento e GDPR evidenziano come il presupposto fondamentale per tali trattamenti sia la liceità dello stesso, ovvero purché siano adeguatamente garantiti i diritti e le libertà dell'interessato, e, alla luce di tale lettura, si esclude dall'ambito di liceità il trattamento automatizzato, come sopra definito, in quanto maggiormente rischioso per l'interessato.

Il titolare del trattamento deve operare una distinzione rispetto alle categorie degli interessati, potendo trattare esclusivamente i dati di persone sottoposte a indagine, imputati, persone sottoposte a indagine o imputate in procedimento connesso o collegato, persone condannate con sentenza definitiva, persone offese dal reato, parti civili, persone informate sui fatti, testimoni. Tale distinzione è stata altresì recepita dall'art. 4 del Decreto Legislativo n.51/2018.

La direttiva infatti, in combinato disposto e coerentemente con l'art. 32 del GDPR, prevede l'adozione delle misure di sicurezza adeguate per garantire che il trattamento sia effettuato in conformità alle norme comunitarie applicando i principi di *privacy by design*, a norma dell'art. 18. La coerenza normativa tra la Direttiva 680/2016 e il GDPR è mantenuta anche nel rafforzamento della necessaria tutela contro il rischio di *data breach* e la designazione obbligatoria di un DPO, come sopra definiti.

In conclusione la Direttiva 680/2016 regola la cooperazione giudiziaria e di polizia in materia penale tra Stati membri ed amplifica ed estende il grado di protezione degli interessati nell'ambito considerato, anche perché non si limita più a stabilire regole in materia di mera cooperazione tra Stati, incidendo invece sugli obblighi di salvaguardia interni a ciascuno Stato. Le Autorità competenti a trattare dati per i fini anticrimine e di sicurezza pubblica possono includere non solo le Autorità giudiziarie, la polizia o altre Autorità incaricate dell'applicazione della legge ma anche qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'Autorità pubblica e i poteri pubblici ai fini della direttiva. Qualora tali organismi o entità trattino dati personali per finalità diverse da quelle della direttiva, si applica il GDPR.

È pertanto necessario prendere in considerazione come i sistemi di biometria e, nel dettaglio, di riconoscimento facciale, che consentano non solo riprese dei sospettati per fini preventivi riguardanti la commissione di atti terroristici ma anche di eventuali richiedenti asilo e operatori del settore dell'immigrazione, trattando *de facto* dati personali al di fuori delle finalità consentite, siano sottoposti alle necessarie valutazioni di liceità ed adeguatezza imposte dal GDPR. Per quanto riguarda l'utilizzo di dati biometrici, definiti dal GDPR nell'art. 9 dati particolari, il necessario focus, quindi, riguarda il tema del consenso ed il suo eventuale superamento.

5.4. Trattamento di categorie particolari di dati personali

L'art. 9 del GDPR inserisce i dati biometrici all'interno della categoria dei dati particolari che richiedono una maggiore tutela.

La necessità di tale tutela rafforzata risiede nei rischi che comporta l'utilizzo di tali dati personali e richiede, pertanto, la rigida osservanza di una serie di cautele, al fine di evitare che si verifichino dei pregiudizi connessi ad un'indebita o non autorizzata utilizzazione degli stessi, al di fuori degli scopi specifici per i quali sono stati acquisiti dal sistema.

Per queste ragioni, il GDPR, all'art. 9.1 stabilisce che in linea generale è vietato il trattamento di "dati biometrici intesi ad identificare in modo univoco una persona fisica" ad esclusione del ricorrere di una serie di casi ben precisi delineati nell'art. 9.2 GDPR.

Il dettato normativo quindi esclude un divieto di trattamento quando l'interessato ha dato il proprio consenso esplicito al trattamento dei dati personali per uno o più specifici utilizzi; quando tale trattamento è effettuato nell'ambito di rapporti di lavoro e di previdenza; quando l'impiego di questi particolari dati personali si rende necessario per proteggere un interesse vitale dell'interessato o di un'altra persona fisica; quando il soggetto cui i dati si riferiscono si trova in una situazione di incapacità, fisica o giuridica, di prestare direttamente il proprio consenso per tale utilizzo; nell'ambito di un procedimento giudiziario e, in particolare, per accertare, esercitare o difendere un diritto, tanto in sede amministrativa quanto stragiudiziale; per motivi di particolare interesse pubblico, previsti dalla legge; nel settore della sanità pubblica, per finalità di sicurezza sanitaria, per il controllo e l'allerta, per la prevenzione o il controllo di malattie trasmissibili e, in generale, per tutelarsi da altre minacce gravi alla salute delle persone.

L'utilizzo dei dati biometrici, pertanto, risultano soggetti ad una disciplina particolarmente tutelante e fondata su una serie di adempimenti obbligatori, quali ad esempio l'obbligo di predisporre un registro dei trattamenti ex art.30 GDPR e di svolgere una valutazione d'impatto sulla protezione dei dati, DPIA, ex art. 35 GDPR.

D'altra parte, esaminando le deroghe che il GDPR prevede circa il divieto di utilizzo dei dati biometrici, è agevole analizzare la ratio con la quale il legislatore europeo ha operato, sancendo una netta differenza tra la predisposizione di regimi di tutela che più avanti verranno analizzati nei loro aspetti specifici (*privacy by design*, DPIA, nomina DPO, misure organizzative e tecniche) e la circolazione libera dei dati biometrici stessi.

Nell'ottica del legislatore europeo, infatti, grazie ad una tutela dettagliata, strutturata su cautele giuridiche di natura documentale e misure di sicurezza che possono estrinsecarsi

sia in contesti organizzativi che tecnici, l'utilizzo di dati biometrici può essere consentito se risulti proporzionato alla finalità perseguita e inserito in un contesto che garantisca la protezione dei diritti e delle libertà degli interessati.[22]

Il GDPR e la Direttiva 680/2016 sono state recepite in Italia rispettivamente tramite il Decreto Legislativo n. 101/2018 che emenda il Decreto Legislativo 196/2003, cd. Codice Privacy, e il Decreto Legislativo n. 51/2018.

5.5. Decreto Legislativo 51/2018, Decreto Legislativo 101/2018 e le linee guida in tema di biometria: la preventiva consultazione presso l'Autorità Garante e le necessarie misure di sicurezza

Per ragioni di completezza espositiva è utile introdurre brevemente la successiva trattazione analitica delle norme contenute nei decreti legislativi 51/2018 e 101/2018. Tali decreti delineano un quadro preciso circa gli obblighi che un'Autorità competente nella prevenzione, indagine, accertamento e perseguimento di reati quali il terrorismo deve rispettare e gli obblighi residuali che un titolare del trattamento deve considerare. Tali obblighi discendono dalla circostanza che un sistema biometrico di riconoscimento facciale potrebbe trattare dati non solo di sospettati o rei soggetti al controllo dell'Autorità competente, ma anche di operatori del settore dell'immigrazione e richiedenti asilo, fuoriuscendo tale sistema, come precedentemente accennato, per sua stessa natura, dall'applicazione esclusiva delle norme contenute nella direttiva 680/2016 e, quindi, nel Decreto Legislativo 51/2018 che la recepisce, ma dovendosi applicare anche le norme contenute nel Regolamento GDPR e nel Decreto Legislativo 101/2018.

5.5.1. Decreto Legislativo 51/2018[23]

Il decreto 51/2018 regolamenta il trattamento dei dati personali per finalità di prevenzione e repressione di reati, esecuzione di sanzioni penali, salvaguardia contro le minacce alla sicurezza pubblica e prevenzione delle stesse, da parte sia dell'Autorità giudiziaria, sia delle forze di polizia.

Si tratta di un testo contenente principi generali e specifici di regolamentazione della

22 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) - https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679

23 DECRETO LEGISLATIVO 18 maggio 2018, n. 51 Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonchÈ alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. (18G00080) (GU Serie Generale n.119 del 24-05-2018)

materia penalistica in ambito di trattamento di dati personali. Ai fini della presente analisi è necessario soffermarsi solo su alcuni punti strettamente connessi al trattamento di dati biometrici e specificatamente dati generati da sistemi di riconoscimento facciale ai fini del controllo dei flussi migratori.

Il decreto impone che i dati personali siano conservati con attenzione alla necessaria *data retention* seguendo il criterio del conseguimento delle finalità per i quali sono trattati ed inoltre, sancisce l'obbligo di sottoporre tali trattamenti ad una valutazione circa la loro attualità prospettando cancellazioni od anonimizzazioni dei dati una volta raggiunto il limite temporale massimo di conservazione. Il decreto, inoltre, per quanto riguarda la disciplina di accesso ai dati personali, delineata anche nel GDPR agli articoli dal 15 al 22, prevede uno speciale procedimento attraverso il quale qualsiasi interessato, durante il procedimento penale o dopo la sua definizione, può chiedere la rettifica, la cancellazione o la limitazione dei dati personali che lo riguardano.

Per quanto riguarda la disciplina della sicurezza del trattamento, tanto cara al legislatore europeo e *ratio* principale delle disposizioni prese in considerazione, si prevede come obbligatoria anche per l'autorità giudiziaria la nomina del responsabile della protezione dati, DPO e l'individuazione nella figura dell'Autorità Garante l'organo deputato a vigilare sul rispetto delle norme attuative della direttiva.

La violazione delle norme prevede l'irrorazione di sanzioni amministrative e irrorazione di sanzioni penali per il trattamento operato con finalità illegittime. Ai fini della presente analisi gli articoli 7, 8, 15, 16, 20, 23, 24, 25, 26, 27, 28, 29 e 30 del Decreto Legislativo n. 51/2018 risultano essere di grande interesse e costituiscono gli obblighi a cui sono sottoposti i titolari del trattamento che vogliano utilizzare dati personali e nello specifico dati particolari derivanti da sistemi biometrici di riconoscimento facciale ai fini di controllo dei flussi migratori con lo scopo di prevenire reati terroristici.

A norma dell'art. 7 il trattamento di dati di cui all'articolo 9 del GDPR, che include i dati biometrici, è autorizzato solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento, ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha oggetto dati resi manifestamente pubblici dall'interessato. Tale disposto normativo implica un chiaro riferimento alle garanzie adeguate per i diritti e le libertà dell'interessato che trovano applicazione quindi così come delineate all'interno del GDPR.

L'art 8 è strettamente connesso, per sua stessa natura, all'art. 22 del GDPR. Apprezzabile è lo sforzo del legislatore europeo e di conseguenza di quello italiano nella fase di recepi-

mento della direttiva, di uniformare le discipline normative relative alla protezione dei dati personali. Il processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato risulta vietato, salvo se autorizzato da specifiche disposizioni di legge o dal diritto dell'Unione europea che devono prevedere, però, garanzie adeguate per i diritti e le libertà dell'interessato.

In ogni caso è garantito il diritto di ottenere l'intervento umano da parte del titolare del trattamento. Relativamente ai dati biometrici tale divieto risulta maggiormente delineato poichè i trattamenti automatizzati non possono basarsi sulle categorie particolari di dati personali di cui all'articolo 9 del GDPR, salvo che siano in vigore misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato, il che implica una tutela rafforzata con esplicito riferimento, inoltre, all'articolo 21 della Carta dei diritti fondamentali dell'Unione europea, vietando la profilazione finalizzata alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali, quali i dati biometrici.

L'art. 15 impone al titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato in conformità alle norme del decreto, se del caso riesaminando e aggiornando qualora necessario e, ove proporzionato rispetto all'attività di trattamento, le misure stesse.

L'art. 16 del Decreto definisce la pseudonimizzazione come misura tecnica e organizzativa adeguata al fine di tutelare i diritti degli interessati ed inoltre, tratta il tema dell'impostazione predefinita di un sistema che li abiliti a trattare solo i dati personali necessari per ogni specifica finalità, vietando, altresì la diffusione di dati personali a numeri indefiniti di persone fisiche. Tale articolo, quindi, mutua la struttura dell'art. 25 del GDPR, riguardante la cd. *privacy by design*, che diventa necessaria al fine di una corretta predisposizione di un sistema biometrico di riconoscimento facciale.

L'art. 20 del Decreto sancisce l'obbligo già presente nell'art. 30 GDPR, ovvero la tenuta di un registro dei trattamenti da parte del titolare o del responsabile del trattamento che contenga al suo interno: a) il nome e i dati di contatto del titolare del trattamento e, se previsti, di ogni contitolare del trattamento e del responsabile della protezione dei dati; b) le finalità del trattamento; c) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi o presso organizzazioni internazionali; d) una descrizione delle categorie di interessati e delle categorie di dati personali; e) se previsto, il ricorso alla profilazione; f) se previste, le categorie di trasferimenti di dati personali verso un Paese terzo o verso organizzazioni internazionali; g) un'indicazione del titolo giuridico del trattamento cui sono destinati i dati personali, anche in caso di trasferimento; h) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati personali; i) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di

cui all'articolo 25, comma 1, che verrà analizzato più avanti. Meno gravosi da un punto di vista contenutistico l'insieme dei dati da inserire nel registro dei trattamenti per i responsabili del trattamento, che consistono ne a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agiscono e, se esistente, del responsabile della protezione dei dati; b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento; c) i trasferimenti di dati personali effettuati su istruzione del titolare del trattamento verso un Paese terzo o verso un'organizzazione internazionale; d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 25, comma 1.

L'art. 21 impone che le operazioni di raccolta, modifica, consultazione, comunicazione, trasferimento, interconnessione e cancellazione di dati, eseguite in sistemi di trattamento automatizzati, debbano essere registrate in appositi file di *log* che consentano di conoscere i motivi, la data e l'ora di tali operazioni e, se possibile, di identificare la persona che ha eseguito le operazioni e i destinatari, da utilizzare, inoltre, ai soli fini della verifica della liceità del trattamento, per finalità di controllo interno, per garantire l'integrità e la sicurezza dei dati personali e nell'ambito di procedimenti penali e potenzialmente sottoponibili all'Autorità Garante.

L'art. 23 sancisce l'obbligo di una valutazione d'impatto sulla protezione dei dati (DPIA) se il trattamento, per l'uso di nuove tecnologie e per la sua natura, per l'ambito di applicazione, per il contesto e per le finalità, presenta un rischio elevato per i diritti e le libertà delle persone fisiche.

Tale obbligo è coerente con le disposizioni del GDPR e, pertanto, può considerarsi inteso come graniticamente previsto e da seguire necessariamente al fine di poter procedere al trattamento dei dati personali.

Un ulteriore aspetto, fondamentale in tema di biometria, riguarda la consultazione preventiva del Garante di cui all'art. 24 del Decreto Legislativo 51/2018. Il titolare del trattamento o il responsabile del trattamento consultano il Garante prima del trattamento di dati personali che figureranno in un nuovo archivio di prossima creazione se a seguito di una DPIA è risultato essere presente un rischio per diritti e libertà degli interessati particolarmente elevato, ma anche, a prescindere da tale valutazione e senza però escluderla, se il tipo di trattamento implica l'utilizzo di dati biometrici. Il titolare del trattamento, a norma del medesimo articolo, è obbligato a trasmettere al Garante la DPIA e, su richiesta, ogni altra informazione, al fine di consentire a detta autorità di effettuare una valutazione della conformità del trattamento, dei rischi per la protezione dei dati personali dell'interessato e delle relative garanzie. Se tale valutazione dovesse condurre ad un risultato negativo circa la legittimità del sistema in oggetto relativamente alle disposizioni del Decreto, il Garante

inoltra al titolare del trattamento un parere per iscritto entro sei settimane, termine prorogabile eventualmente per particolari complessità del caso concreto esaminato.

L'art. 25 del Decreto affronta il tema della sicurezza del trattamento e si esprime coerentemente con quanto contenuto nell'art. 32 GDPR. Il titolare del trattamento, o il responsabile del trattamento, quindi, a norma dell'art. 25 del Decreto, tenuto conto delle cognizioni tecniche disponibili, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del grado di rischio per i diritti e le libertà delle persone fisiche, deve mettere in atto misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio di violazione dei dati. Il secondo comma dell'art. 25 del Decreto individua delle misure specifiche al fine di proteggere le modalità in cui si estrinseca il trattamento automatizzato, sempre previa redazione della valutazione d'impatto di cui sopra. Tali misure di sicurezza sono elencate nel secondo comma dell'art. 25 e consistono in: a) vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»); b) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»); c) impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»); d) impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»); e) garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»); f) garantire la possibilità di individuare i soggetti ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»); g) garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»); h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»); i) garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»); l) garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

Gli articoli 26, 27, 28, 29 e 30 delineano altri obblighi mutuati dal GDPR, oltre al suddetto obbligo di tenuta di un registro dei trattamenti, quali la nomina di un DPO e di notifica al Garante e/o agli interessati di una violazione di dati personali, cd. *data breach*.

In conclusione, l'utilizzo di dati personali particolari quali i dati ricavati da sistemi di biometria con riconoscimento facciale impongono particolari cautele ed obblighi anche per le Autorità competenti in materia di indagine e prevenzione del reato di terrorismo. Tali cautele ed obblighi possono riassumersi nella necessità di nominare un DPO, predisporre una valutazione d'impatto (DPIA), redigere e mantenere un registro dei trattamenti, procedere ad una preventiva consultazione con l'Autorità Garante, predisporre procedure di cooperazione ed eventuale notifica di data breach con l'Autorità stessa e adottare misure tecniche quali un sistema di *logging* e l'adozione delle misure di sicurezza elencate nel comma 1 dell'art. 25 del Decreto.

La portata applicativa di un sistema di riconoscimento facciale per il controllo dei flussi migratori al fine di prevenzione del reato di terrorismo, però, come già ribadito, fuoriesce in parte dal perimetro di applicazione della Direttiva 680/2016 e del Decreto 51/2018. L'utilizzo di dati biometrici nei quali potrebbero essere coinvolti soggetti esterni rispetto a quelli elencati nella suddetta Direttiva e nel suddetto Decreto non consente di limitare l'analisi all'applicazione delle già analizzate norme, è pertanto doveroso procedere ad analizzare il Decreto Legislativo n.101/2018 che ha emendato il Decreto Legislativo 196/2003 armonizzando la normativa italiana con il Regolamento europeo 679/2016 (GDPR).

Alcuni degli obblighi appena riassunti trovano la medesima applicazione anche per quanto riguarda i titolari del trattamento che non siano autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali o che non riguardino i soggetti di cui all'art. 4 del Decreto 51/2018 (persone sottoposte a indagine, imputati, persone sottoposte a indagine o imputate in procedimento connesso o collegato, persone condannate con sentenza definitiva, persone offese dal reato, parti civili, persone informate sui fatti, testimoni), mentre precise disposizioni riguardo ai dati biometrici, che si aggiungono a quelle sinora descritte, si trovano nel Decreto Legislativo n. 101/2018 e nelle linee guida dell'Autorità Garante sulla biometria.

5.5.2. Decreto Legislativo n. 101/2018[24]

Tra le principali novità significative introdotte dal Decreto legislativo n. 101/2018 che ha armonizzato la disciplina relativa alla protezione dei dati personali contenuta nel Decreto legislativo n. 196 del 2003 con il GDPR (d'ora in avanti ci si riferirà al Decreto Legislativo n.196/2003 emendato dal Decreto Legislativo n.101/2018 come "Codice", essendo

24 DECRETO LEGISLATIVO 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchÈ alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018)

esso assimilabile dialetticamente ed analogicamente ad un Codice, non già penale o civile ma sul tema della protezione dei dati personali), si riscontra la presenza della tematica del trattamento di dati biometrici. Va ricordato come l'art. 9 del GDPR, che cataloga i dati biometrici tra i dati particolari, nel suo secondo paragrafo, deroga alcuni dei divieti ad alcune condizioni che sono state già oggetto della presente trattazione. Il paragrafo 4 dell'art. 9 del GDPR, non precedentemente affrontato, riguarda la possibilità per gli Stati membri di introdurre ulteriori condizioni circa il trattamento di dati biometrici. Il legislatore italiano, infatti, ha colto l'occasione di dettagliare maggiormente le condizioni di liceità di un trattamento di dati biometrici, a norma non solo del succitato paragrafo 2 dell'art. 9 GDPR ma anche del nuovo art. 2-septies del Codice e del nuovo art 2-quater. Stante il disposto normativo dell'art. 2-sexies, che disciplina i trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi della lettera g), paragrafo 2, del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante (quali nelle materie relative a cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato a norma della lettera d del secondo comma del medesimo articolo) nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. Per i dati genetici, biometrici e relativi alla salute il trattamento deve avvenire comunque nel rispetto di quanto previsto dall'articolo 2-septies.

L'art. 2-septies dispone che i dati biometrici possano essere oggetto di trattamento in conformità alle misure di garanzia disposte dal Garante con proprio provvedimento, da adottarsi con cadenza almeno biennale. Lo schema di provvedimento è sottoposto dal Garante a consultazione pubblica per un periodo non inferiore a 60 giorni. Il Garante terrà conto, nell'adottare il provvedimento, delle linee guida, raccomandazioni e *best practice* pubblicate dal Comitato Europeo per la protezione dei dati (precedentemente WP29), dell'evoluzione scientifica e tecnologica nel settore della biometria e dell'interesse per la libera circolazione dei dati personali nel territorio europeo. Tali misure di garanzia dovranno essere compatibili con il GDPR e saranno adottate in relazione a specifiche finalità e suddivise presumibilmente in paragrafi con scenari e casi d'uso che consentiranno di individuare ulteriori condizioni sulla base delle quali il trattamenti dei dati biometrici sarà consentito, escludendo il caso del consenso dell'interessato, poiché escluso dallo stesso Codice nel sesto comma dell'art. 2-septies, in quanto limitato ai dati genetici.

Una corposa novità riguardante i dati biometrici è il via libera al loro utilizzo con riguardo alle procedure di accesso fisico e logico ai dati da parte di soggetti autorizzati ma anche tale provvedimento ex art.2-septies comma 7 sarà soggetto ad una necessaria rivisitazione

una volta adottato il provvedimento del Garante circa le misure di garanzia suddette che potranno comprendere, tra l'altro, tecniche di cifratura e pseudonimizzazione, misure di minimizzazione e specifiche modalità di accesso ai dati per rendere le informazioni agli interessati, nonché quelle ulteriori a garantire i diritti degli interessati.

Oltre alle misure di garanzia, l'art. 2-quater inserisce nel quadro normativo da rispettare la categoria delle regole deontologiche, da adottare in seguito all'approvazione e pubblicazione, che diventano condizione essenziale per la liceità e la correttezza del trattamento. L'art. 2-quinquedecies prevede che per trattamenti nell'esecuzione di un compito di interesse pubblico che può presentare rischi particolarmente elevati, di cui all'art. 35 GDPR, ossia per quei trattamenti per i quali sarebbe necessaria una valutazione di impatto (DPIA), il Garante può adottare d'ufficio provvedimenti a carattere generale prescrivendo misure ed accorgimenti a garanzia dell'interessato mantenendo comunque necessario lo svolgimento della DPIA e l'adozione comunque degli accorgimenti e garanzie previste in tali tipologie di provvedimenti. Nel titolo secondo, capo primo, che disciplina i trattamenti da parte delle forze di polizia, è presente la disposizione ex art. 55 del Codice che sancisce il principio secondo cui il trattamento di dati personali che implica maggiori rischi di un danno all'interessato, con particolare riguardo a banche di dati genetici o biometrici, a tecniche basate su dati relativi all'ubicazione, a banche di dati basate su particolari tecniche di elaborazione delle informazioni e all'introduzione di particolari tecnologie, è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato previa valutazione e comunicazione all'Autorità Garante.

Il comma 11 dell'art. 22 del Decreto Legislativo n. 101/2018 contiene una previsione che apre uno scenario particolarmente ostico ai fini interpretativi e di adeguamento alle norme contenute nel Codice. Tale disposizione, infatti, stabilisce che le disposizione del Decreto Legislativo n. 196/2003 (anche le disposizioni abrogate dallo stesso Decreto 101/2018), relative al trattamento di dati biometrici, continuano a trovare applicazione in quanto compatibili con il GDPR sino all'adozione delle misure di garanzia di cui all'art. 2-septies del Codice. Una siffatta impostazione, di fatto, "riporta in vita" i provvedimenti del Garante e, l'esercizio di valutazione tra la compatibilità normativa, la sopravvenienza delle nuove norme e la sopravvivenza delle norme e dei provvedimenti abrogati non risulta agevole, pertanto, si consiglia di attendere il primo provvedimento contenente le misure di garanzia a norma dell'art. 2-septies del Codice prima di considerare abrogato il Provvedimento generale prescrittivo in tema di biometria e le relative allegate linee guida sulla biometria rilasciate dall'Autorità Garante nel novembre del 2014.

Le regole deontologiche ex art.2-quater, le misure di garanzia per il trattamento di dati biometrici ex art. 2-septies, nonché provvedimenti generali per trattamenti che sarebbero

soggetti a valutazione di impatto arricchiscono il quadro normativo già precedentemente delineato. Nella fase di transizione, precedente all'approvazione delle misure di garanzia ex art. 2-septies del Codice, è necessario considerare ancora in vigore il suddetto provvedimento del Garante in tema di biometria.

5.5.3. Provvedimenti dell'Autorità Garante

L'Autorità Garante, nel novembre del 2014, ha emanato un Provvedimento recante delle linee guida sul trattamento dei dati biometrici che sarà valido sino all'entrata in vigore del provvedimento ex art. 2-septies sullo stesso tema. Tale provvedimento dispone che i trattamenti di dati biometrici devono essere connotati da caratteristiche di liceità, intesa come rispetto delle norme del Codice ed eventuali altri provvedimenti del Garante od obblighi di legge; necessità, intesa come la riduzione al minimo dell'utilizzazione dei dati secondo il principio di minimizzazione, valutando se le medesime finalità possano essere perseguite utilizzando dati anonimi e pertanto è necessario cancellare immediatamente, e possibilmente in modo automatico, i dati biometrici e le informazioni a essi correlate in caso di cessazione del trattamento, ferme restando eventuali disposizioni che prevedano una disciplina differente per casi specifici; finalità, intesa come divieto di trattare dati per scopi diversi da quelli per i quali sono stati raccolti; proporzionalità, intesa come pertinenza e non eccedenza rispetto alle finalità perseguite, evitando l'acquisizione di dati ultronei rispetto a quelli necessari per la finalità perseguita nel caso concreto e che occorra evitare, se non per motivate ed eccezionali esigenze, di ricorrere a sistemi che impieghino più di una caratteristica biometrica dell'interessato. Le linee guida predispongono anche degli adempimenti giuridici da rispettare nel caso di trattamento di dati biometrici. Prima dell'inizio del trattamento il titolare deve fornire agli interessati un'informativa idonea e specifica relativa all'utilizzo dei dati biometrici, contenente tutti gli elementi previsti dall'art. 13 del Codice come la finalità perseguita e la modalità del trattamento, la loro natura obbligatoria o facoltativa. Nel caso in cui i sistemi utilizzati in determinate sedi siano potenzialmente idonei al rilevamento di dati biometrici dell'interessato senza la sua cooperazione occorre informare gli interessati dando loro la possibilità di scelta relativamente all'accesso a una zona soggetta a tale tipo di controlli biometrici mediante apposita segnaletica in prossimità delle aree soggette a rilevamento biometrico o delle postazioni di rilevamento, oppure può essere fornita con altri mezzi prima dell'interazione dell'interessato con il sistema biometrico. Le linee guida recano disposizioni anche circa la conservazione del dato biometrico e le misure di sicurezza, che d'ora in avanti si citeranno filtrando le disposizioni che contengono norme abrogate dal GDPR e/o dal Decreto Legislativo n. 101/2018 ed anche rispetto al contesto del sistema di riconoscimento facciale volto al controllo dei flussi migratori ai fini di prevenzione del terrorismo. Il dato

può trovarsi nella disponibilità del titolare del trattamento ed essere conservato in un'unica banca dati centralizzata, nelle postazioni di lavoro informatiche, sugli stessi dispositivi di acquisizione biometrica, in dispositivi sicuri affidati alla diretta ed esclusiva disponibilità degli interessati.

I *filesystem di smart card e token biometrici* devono essere leggibili dai soli lettori autorizzati, quantomeno nella porzione contenente i dati biometrici, che vanno resi inintelligibili al di fuori del contesto in cui se ne prevede l'uso tramite l'adozione di accorgimenti crittografici. Il titolare del trattamento svolto con sistemi elettronici è tenuto ad adoperarsi, utilizzando i mezzi tecnici che lo stato dell'arte nel settore informatico rende disponibili, per proteggere i dati personali mentre per quanto la scelta dei processi biometrici si deve privilegiare l'uso di quelli che richiedono la cooperazione consapevole dell'interessato. Laddove tecnicamente possibile, vanno utilizzati modelli biometrici con la minore quantità di informazioni, in modo da ridurre o annullare il rischio di ricostruzione del campione biometrico originario in qualunque fase del trattamento. I dati biometrici grezzi (*raw data)* generati nel corso del procedimento di acquisizione biometrica (*biometric capture*) andranno cancellati da aree di memoria temporanea, centrale e secondaria e dal *filesystem* del sistema utilizzato per l'acquisizione immediatamente dopo la generazione del campione biometrico. Il dato biometrico andrà possibilmente cifrato al momento della sua acquisizione dal sensore per ridurre il rischio di acquisizione fraudolenta con attacchi di tipo di *third in the middle* sul sensore o sui suoi canali di comunicazione con il sistema biometrico. La trasmissione del dato andrà comunque effettuata, sia in fase di *enrolment* sia in fase di riconoscimento, su canali di comunicazione cifrati tra il dispositivo di acquisizione e il sistema su cui sono effettuati i confronti biometrici o l'eventuale conservazione dei campioni o dei modelli biometrici di riferimento. I campioni o i modelli biometrici, laddove indispensabile per consentire i confronti, andranno conservati in aree di *filesystem* protette con strumenti crittografici o in database che supportino la cifratura a livello di *record* o di colonna. Laddove il sistema biometrico renda non praticabile l'utilizzo di tecniche crittografiche a chiave pubblica o la partecipazione di un soggetto terzo fiduciario, la cifratura dovrà comunque garantire elevati standard di sicurezza con lunghezza delle chiavi adeguate alla dimensione e alla criticità della banca dati. I dati identificativi degli utenti andranno conservati separatamente dai relativi dati biometrici. Se il dato biometrico si trova nella disponibilità del titolare del trattamento ed è conservato in un'unica banca dati, nelle postazioni di lavoro informatiche oppure su dispositivi di acquisizione biometrica, il titolare deve sempre prendere le massime precauzioni e implementare tutti i presidi necessari alla tutela del dato, riducendo al minimo il rischio di accesso non autorizzato, il furto, la sostituzione o la compromissione dei dati biometrici. Nei casi eventuali di conservazione centralizzata dei dati biometrici in un server devono essere adottati sistemi idonei alla registrazione degli accessi da parte dei soggetti specificatamente abilitati

a svolgere mansioni tecniche connesse alla manutenzione e alla gestione del server medesimo, che dovranno essere designati quali amministratori di sistema. Tali registrazioni devono comprendere i riferimenti temporali e avere caratteristiche di completezza, integrità, inalterabilità e durata della conservazione analoghe a quelle richieste per i log degli accessi di cui al provvedimento del Garante del 27 novembre 2008 sugli amministratori di sistema. I dati biometrici rilevati, riferiti al dato grezzo d'origine, al campione biometrico, oppure ai dati ottenuti tramite elaborazione di quelli precedentemente citati (modelli o riferimenti biometrici), saranno oggetto di trattamento per il periodo di tempo strettamente necessario a perseguire gli scopi per i quali sono stati raccolti e trattati, fatta salva l'eventuale applicabilità di specifiche disposizioni in casi particolari. In particolare, i campioni biometrici impiegati nella realizzazione del modello biometrico possono essere trattati solo durante le fasi di registrazione e di acquisizione necessarie al confronto biometrico, e non devono essere memorizzati se non per il tempo strettamente necessario alla generazione del modello stesso. Venuta meno la necessità di trattare il dato questo deve essere cancellato in modo sicuro anche dalle aree di memoria volatile oltre che dai supporti di memorizzazione.[25]

5.6. Conclusioni

La normativa europea ed italiana in tema di protezione dei dati personali reca disposizioni specifiche circa l'utilizzo di sistemi di biometria e del trattamento di dati particolari ex art. 9 GDPR come i dati derivanti dal riconoscimento facciale, sia per quanto riguarda l'utilizzo di tali tecnologie nell'ambito della prevenzione dei reati quali terrorismo, sia per quanto fuoriesce da tale perimetro coinvolgendo diverse categorie di interessati.

Il Regolamento europeo GDPR, la Direttiva 680/2016, il Decreto Legislativo 51/2018 ed il Decreto Legislativo 101/2018 creano un quadro di applicazione particolare che pone al centro la doverosa tutela da riconoscere agli interessati ed obblighi e misure di sicurezza tecniche ed organizzative da adottare al fine di poter lecitamente utilizzare gli strumenti di rilevazione biometrica, sia che si tratti di Autorità competenti alla prevenzione di crimini sia che si tratta di altri titolari del trattamento. È obbligatorio quindi, nel progettare un siffatto sistema, tener presente l'art. 25 del GDPR e la *data protection by design*. È obbligatorio, inoltre, procedere ad una valutazione d'impatto ex art. 35 GDPR (DPIA). È altresì obbligatorio nominare un DPO, mantenere un registro dei trattamenti, adottare una *policy* circa la gestione e segnalazione al Garante ed agli interessati in caso di *data breach* ed adottare le misure e tecniche adeguate, da un punto di vista relativo alla sicurezza informatica, come delineate dai provvedimenti futuri e presenti del Garante e secondo il principio di *accountability* delineato

25 Linee guida in materia di riconoscimento biometrico e firma grafometrica - Allegato A al Provvedimento del Garante del 12 novembre 2014 - Provvedimento Generale prescrittivo in tema di biometria

dall'art. 32 del GDPR. Non ultimo, per le Autorità competenti sarà necessario consultare il Garante ex art. 55 del Codice e, genericamente, i titolari del trattamento di un sistema di riconoscimento biometrico dovranno, a seguito di una valutazione d'impatto (DPIA) che abbia dato esito negativo rispetto ai rischi potenziali per diritti e libertà degli interessa, chiedere il parere del Garante per la Protezione dei Dati Personali.

6
INDIRIZZO PROGRAMMATICO

6.1. Adempimenti e *privacy by design*

All'interno del GDPR, per invitare al rispetto del principio di *data protection-by-design*, l'art. 25 parla esplicitamente di "Protezione dei dati fin dalla progettazione". La predetta disposizione, letta in combinato con il Considerando 78 dello stesso GDPR, prevede che i produttori dei prodotti, dei servizi e delle applicazioni basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, in fase di sviluppo, progettazione, selezione e utilizzo di tali strumenti, dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati in modo da adempiere ai loro obblighi di protezione dei dati. È evidente, dunque, come il Considerando 78 del GDPR combini lo sviluppo e la progettazione di prodotti e servizi da parte dei produttori con il principio di *accountability* del Titolare o del Responsabile che utilizzeranno quelle tecnologie, rendendo così la *data protection-by-design* un criterio di valutazione della responsabilità stessa di questi soggetti.

Si noti che il valore dell'introduzione del principio di *data protection-by-design* (e della protezione dei dati come opzione predefinita – cd. d*ata protection-by-default*), di cui all'art. 25, è esplicitato non solo nell'inclusione del predetto articolo tra le circostanze che possono essere valutate dall'Autorità di controllo competente al momento di comminare una sanzione amministrativa, ma soprattutto nell'inclusione della mancata applicazione dei principi di cui all'art. 25 tra le condotte passibili di sanzione da parte della Autorità di controllo, ex art. 83.4.a) – cioè fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato globale se superiore.

Tenuto conto dell'obbligatorietà del rispetto del principio di *data protection-by-design* che emerge dalle disposizioni del GDPR, si illustrano di seguito delle brevi linee guida relative all'applicazione della *data protection-by-design* in processi e prodotti o servizi.

Integrare la *data protection-by-design* nelle procedure intraprese significa proteggere i dati personali attraverso misure sia tecniche che organizzative, adottate *ex ante* rispetto al verificarsi dell'evento dannoso. In tal senso, gli ambiti che necessitano di includere, sin dalla loro progettazione, la protezione dei dati sono sostanzialmente tre: obblighi e adempimenti in materia di sicurezza; obblighi e adempimenti di garanzia nei confronti dei diritti dell'interessato; collaborazione con soggetti preposti al controllo. Dal punto di vista tecnico, è necessario integrare le misure di sicurezza direttamente in applicazioni, servizi e prodotti,

sin dalla fase di loro sviluppo e progettazione. Seguendo le disposizioni dell'art. 32 GDPR, infatti, prodotti, servizi e applicazioni dovrebbero prevedere *ex ante* misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che possono comprendere la pseudonimizzazione e la cifratura dei dati personali, nonché assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento attraverso procedure tecniche che consentano di «ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico» (ex art. 32 GDPR).

Beninteso, integrare la *data protection-by-design* nelle misure di sicurezza non significa dare per assodate e immutabili le misure inserite in fase di progettazione. È infatti necessario, ai sensi dell'art. 32.d) GDPR stabilire una procedura interna volta a «testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento». Sul punto, si predispone al proprio interno *audit* periodici, tecnologici, documentali e organizzativi, nonché svolge regolarmente, per esempio, prove di penetrazione nel perimetro informatico aziendale sulle misure di sicurezza adottate nei diversi sistemi di Trattamento con strumenti informatici.

Nel valutare l'adeguato livello di sicurezza, infine, per integrare il principio di *data protection-by-design* nelle misure di sicurezza, si "tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati" (cfr. art. 32 (2) GDPR) attraverso una procedura sull'analisi dei rischi IT.

Con riferimento agli obblighi in materia di sicurezza, è necessario prevedere sin dalla progettazione di applicazioni, prodotti e servizi, delle contromisure organizzative effettive e tempestive al fine di procedere alla notificazione all'Autorità di contratto competente (ex art. 33 GDPR) e alla comunicazione all'Interessato (ex art. 34 GDPR) in caso di violazione dei dati personali. A ben vedere, in effetti, il ripristino della sicurezza *ex post* rispetto al verificarsi della violazione, passa per l'integrazione sin dalla progettazione sia di misure di sicurezza adeguate, sia di sistemi di risposta efficienti che a seguito della violazione consentano di adempiere agli obblighi di collaborazione con l'Autorità di controllo e di garantire all'interessato il rispetto dei suoi diritti.

È bene precisare che tra le misure intraprese *ex ante*, introdotte sin dalla progettazione di prodotti e servizi, non rientrano solo quelle tecniche (ad es. pseudonimizzazione) o organizzative (ad es. Procedura per la gestione dei *data breach*) messe in atto per gestire le informazioni, la loro salvaguardia e difesa in caso di intrusioni e alterazioni non autorizzate. Infatti, vi sono anche tutte quelle misure organizzative che riguardano il sistema delle autorizzazioni relative all'accesso ai dati; i contratti per il trattamento di dati personali l'esecuzione

della valutazione di impatto sulla protezione dei dati, di cui si dirà più avanti, e tutte quelle ulteriori misure organizzative funzionali a custodire e controllare i dati.

Procedendo con ordine, il sistema delle nomine appare necessario nel rispetto del principio di riservatezza intesa nel senso introdotto dal Considerando 83, il quale menziona esplicitamente la riservatezza come adeguato strumento di sicurezza dei dati, proprio perché l'obiettivo del Titolare deve essere quello di impedire anche l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento (cfr. Considerando 39). Alla luce di questa considerazione, la presenza di mansionari e lettere di incarico a persona autorizzata al trattamento diventano necessarie in quanto definiscono i profili di autorizzazione e impongono ai Responsabili del trattamento di attenersi alle istruzioni impartite dal Titolare evitando *by design* che vi sia accesso ai, o utilizzo non autorizzato dei, dati personali.

Le designazioni, in sostanza, consentono di distribuire sin da subito, prima che avvenga il trattamento, le responsabilità tra Titolare e Responsabile, attribuendo a quest'ultimo una serie di obblighi, affinché non solo egli operi soltanto su istruzioni del Titolare ma anche applichi una serie di misure tecniche e organizzative volte al trattamento lecito dei dati, coadiuvando così il Titolare nell'esecuzione degli obblighi a lui attribuiti.

Parimenti, la nomina di un Responsabile per la protezione dei dati (DPO) costituisce una misura organizzativa che consente di rispettare il principio di *data protection-by-design,* in quanto tale figura svolge diversi compiti tra cui la sorveglianza sull'applicazione del GDPR e il rispetto «delle politiche del titolare del trattamento o del responsabile». La sua funzione è proprio quella di garantire l'implementazione della protezione dei dati *ab origine,* assicurando agli interessati una tutela che va oltre la semplice applicazione della norma, grazie alla maggiore consapevolizzazione del Titolare e del Responsabile rispetto ai rischi del trattamento e agli strumenti per mitigarli.

Le politiche (*policy*, procedure, linee guida interne, circolari), a loro volta, vanno annoverate tra le misure organizzative che implementano la protezione dei dati sin dalla progettazione di prodotti, servizi o applicazioni, in quanto consentono di modellare il trattamento dei dati personali su regole dettate in principio. Da non sottovalutare è, poi, la formazione di ogni persona autorizzata a trattare i dati personali, che ricade tra le misure di natura organizzativa, grazie alla quale è possibile assicurarsi che chi materialmente tratta i dati personali conosca regole e potenziali rischi di tale attività.

Con riferimento al profilo della garanzia dei diritti dell'interessato e i relativi obblighi e adempimenti, si noti che, se da un lato i dati personali divengono sempre più preziosi per il Titolare, dall'altro anche gli interessati sono più consapevoli della loro rilevanza. Ciò

implica la necessità di applicare *by design* misure tecniche, ma soprattutto organizzative, che non solo riducano al minimo i rischi, ma che consentano di sviluppare un rapporto di fiducia con gli interessati e di mantenere una buona relazione con essi. In tal senso, a ciascun interessato dovrebbe pervenire l'informativa *privacy* prevista dagli artt. 13 e 14 GDPR in cui sono indicate le condizioni di liceità del trattamento e deve essere anche progettato un sistema di CRM che implichi la stratificazione del database, in modo tale da poter registrare e conservare le informative, le domande di consenso e le risposte date da ciascun interessato, tenendo traccia nel tempo anche degli eventuali cambiamenti di volontà dell'Interessato con riferimento ad uno o più trattamenti di dati personali. Altrettanto fondamentale è la definizione *ex ante* di una idonea organizzazione per fornire riscontro tempestivo alle istanze dell'interessato (art. 12.3 GDPR) nonché per permettere al medesimo l'esercizio dei diritti a lui riconosciuti dagli artt. 15-22 GDPR.

Il DPIA o Valutazione d'impatto sulla protezione dei dati personali è il cuore applicativo del principio di *data protection-by-design,* è disciplinato dall'art. 35 del GDPR e ha l'obiettivo non solo di garantire la sicurezza dei dati personali, ma soprattutto di individuare i rischi specifici del trattamento. Il legame tra DPIA e *data protection-by-design* risiede proprio nel fatto che esso è prodromico rispetto all'adozione delle adeguate misure di sicurezza che vanno implementate nei prodotti e servizi che trattano dati personali. Il concetto di sicurezza, dunque, riguarda la protezione dei dati sin dalla progettazione di applicazioni, prodotti e servizi in quanto essa dipende proprio dal rapporto tra trattamento e diverse tipologie di dati trattati. Inoltre, il DPIA consente di affrontare gli aspetti di protezione dei dati prima che il prodotto o il servizio vengano messi sul mercato. Ciò fa sì che si riduca l'incertezza giuridica rispetto ai rischi, generando vantaggi sia per gli Interessati sia per le filiere di soggetti attivi del trattamento di dati.

In ultimo, con riferimento alla collaborazione con i soggetti preposti al controllo la *data protection-by-design* può essere individuata come essenziale nella progettazione di tutte quelle procedure che consentono la conservazione delle prove relative alla compliance con le disposizioni del GDPR: il Registro dei trattamenti ex art. 30, gli esiti del DPIA, gli archivi di nomine, incarichi e contratti.

6.2. DPIA

Una DPIA è un processo volto a descrivere il trattamento, valutare la necessità e la proporzionalità dello stesso, per gestirne i rischi per i diritti e le libertà delle persone fisiche che ne derivano, attraverso la loro analisi, determinando le misure per farvi fronte.

Il DPIA è un importante strumento di *accountability* in quanto aiuta i titolari non solo

a soddisfare i requisiti del GDPR, ma anche a dimostrare che siano state adottate misure adeguate per garantirne il rispetto. La DPIA deve essere effettuata prima del trattamento ex art. 35 e c. 90 e 92 coerentemente con i principi di *privacy by design e by default ex* art. 25 e c. 78; deve essere avviata già in fase di progettazione delle operazioni di trattamento, anche se il progetto non è definitivo; ne deriva che potrebbe essere necessario ripetere singole fasi di valutazione durante la progressione del progetto stesso. Come chiarito dal Gruppo di lavoro articolo 29 nelle linee guida di recente elaborate in materia, la DPIA è uno strumento di gestione dei rischi per i diritti delle persone fisiche e quindi, prende il loro punto di vista, mentre la analisi dei rischi richiesta ex art. 32 è più focalizzata sull'organizzazione. Una DPIA può riguardare una sola operazione di trattamento dei dati; tuttavia, ex art. 35.1 e c.92 una singola valutazione può affrontare una serie di operazioni di trattamento simili che presentano rischi simili elevati; inoltre, l'oggetto di una valutazione d'impatto sulla protezione dei dati può essere più ampio di un singolo progetto, come nel caso in cui più titolari prevedono di introdurre una comune applicazione o ambiente di elaborazione attraverso un settore industriale o segmento o per un'attività orizzontale ampiamente utilizzata; inoltre, se un prodotto tecnologico, come per esempio, un componente *hardware* o *software*, è suscettibile di essere utilizzato da altri titolari per effettuare diversi trattamenti, ciascun titolare rimane obbligato a svolgere la propria DPIA per quanto riguarda l'attuazione specifica. La DPIA ex art. 35 e ss. del GDPR è richiesta obbligatoriamente, solo per i trattamenti che possono presentare un alto rischio per i diritti e le libertà delle persone fisiche; il titolare del trattamento, prima di procedere allo stesso, deve effettuare una valutazione di impatto dei trattamenti previsti sulla protezione dei dati. Ne deriva, in via preliminare, la necessità di stabilire, in concreto, se il trattamento/i in oggetto, presenta o meno un rischio elevato per i diritti e le libertà delle persone fisiche; il Regolamento individua alcuni trattamenti che presentano alti rischi intrinsechi quali una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; il trattamento, su larga scala, di categorie particolari di dati personali ex art. 9.1, o di dati relativi a condanne penali e a reati ex art. 10; la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Nel sistema preso sinora in considerazione gli ambiti di applicazione sono presenti in tutte e tre le casistiche. Tale elencazione non è esaustiva, pertanto, i Garanti Europei, hanno fornito i seguenti criteri correlati da esempi concreti, per individuare tipologie altamente rischiose di trattamento, che vanno a meglio specificate le indicazioni più generali di cui all'art. 35 e c.71,75 e 91 del GDPR quali alcuni particolarmente rilevanti nella valutazione del sistema in questione come quelli relativi alle decisioni automatiche con effetti giuridici o similmente significativi, un'elaborazione che mira a prendere decisioni su soggetti inte-

ressati e che produce effetti giuridici riguardanti la persona fisica o che allo stesso modo sia determinante per la persona fisica art. 35.3.a.

Ad esempio, il trattamento può comportare l'esclusione o la discriminazione di singoli; controllo sistematico inteso come trattamento utilizzato per osservare, monitorare o controllare soggetti interessati, inclusi i dati raccolti attraverso un controllo sistematico di una zona accessibile al pubblico ex art. 35.3.c.,questo tipo di monitoraggio è considerato rischioso perché i dati personali possono essere raccolti in circostanze in cui gli interessati potrebbero non essere a conoscenza di chi sta raccogliendo i loro dati e di come saranno utilizzati.

Inoltre, potrebbe essere impossibile per le persone evitare di essere oggetto di tale trattamento in spazi pubblici abituali (o accessibili al pubblico); relativi a dati particolari, include le categorie particolari di dati ai sensi dell'art. 9, nonché i dati personali relativi alle condanne penali o ai reati ex art. 10, questo criterio include anche i dati che possono più in generale essere considerati come aggravanti del possibile rischio per i diritti e le libertà delle persone, come i dati relativi all'ubicazione; quelli relativamente ai dati elaborati su larga scala: il GDPR non definisce cosa costituisca larga scala ma i Garanti Europei specificano che riguarda un trattamento che coinvolge un criterio relativo al numero di persone interessate, come numero specifico o come percentuale della popolazione di riferimento, il volume dei dati e/o la gamma di diversi elementi di dati in corso di elaborazione, la durata, o la permanenza, dell'attività di elaborazione dati e l'estensione geografica delle attività di elaborazione; i trattamenti relativi ai dati di interessati vulnerabili ex. c 75, il trattamento di questo tipo di dati può richiedere una DPIA a causa del maggiore squilibrio di potere tra la persona e il titolare, cioè l'individuo non può essere in grado di consentire, od opporsi, al trattamento dei propri dati, ciò riguarda anche segmento più vulnerabile della popolazione che necessita di protezione speciale, come, ad esempio, i richiedenti asilo e in ogni caso in cui può essere identificato uno squilibrio nel rapporto tra la posizione della persona interessata e il titolare.

Al fine di rendere obbligatoria una valutazione d'impatto è sufficiente che solo due delle tipologie di trattamento sopra elencate ricorrano, nel caso di cui trattasi sembrano potenzialmente ricorrere tutte le casistiche delineate nell'elenco.

Se all'esito della valutazione d'impatto sulla protezione dei dati, risulta che il trattamento, considerate anche le eventuali misure aggiuntive per mitigare i rischi, presenta un livello di rischio alto o medio alto per i diritti e le libertà delle persone fisiche, il titolare, deve consultare l'autorità di controllo competente ex art. 36 GDPR prima dell'inizio delle attività di trattamento.

L'obbligo di consultazione preventiva all'autorità di controllo sussiste anche quando è la legge nazionale a richiederlo specificamente in relazione al trattamento per l'esecuzione, da

parte del titolare, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica ex art. 36.5

È necessario revisionare il progetto una volta operativo per verificare se i rischi identificati sono stati gestiti correttamente e che non sussistono ulteriori rischi che in una prima fase di analisi non si sono riscontrati o sopraggiunti in un secondo momento, poiché, quando una operazione di trattamento è dinamica, ossia soggetta a continui cambiamenti, la valutazione d'impatto deve considerarsi un processo continuo. Qualsiasi significativa modifica del progetto stesso o di una sua funzionalità comporteranno una revisione/aggiornamento del DPIA, inoltre, occorre revisionare il DPIA quando c'è un cambiamento del rischio presentato da tale trattamento oppure perché il contesto organizzativo o sociale per l'attività di trattamento è cambiato, per esempio perché gli effetti di determinate decisioni automatizzate sono diventati più significativi, nuove categorie di persone fisiche sono diventate vulnerabili alla discriminazione o i dati sono destinati a essere trasferiti a destinatari situati in un paese che ha lasciato l'Unione europea. In ogni caso è necessario procedere alla revisione del DPIA ogni tre anni, tuttavia, potrebbe rendersi necessario anche prima, a seconda della natura del trattamento e del tasso di variazione dell'operazione di trattamento e delle circostanze generali.

INDICE DELLE FONTI

Fonti bibliografiche

AMATO S., CRISTOFARI F., *Biometria: i codici a barre del corpo,* Giappichelli, Torino, 2013 Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies*, 720/12/EN, 2012;

BADIA, C., *La biometria nei flussi di migrazione*, Edizioni Accademiche Italiane, 2015;

BOLOGNINI L., BISTOLFI C., PELINO E., *Il Regolamento Privacy Europeo*, Giuffrè 2016;

Centro informazioni sulla difesa degli Stati Uniti (CDI)*, Combattere il finanziamento del terrorismo: un aspetto chiave della guerra al terrorismo.;*

DI LAZZARO, M.A., *Reati di terrorismo internazionale. Prospettive di repressione.,* Milano, 2001;

MATERAL, M., *International Criminal Law,* 2009;

PANZERA, F., *Terrorismo - dir. internazionale - Enciclopedia del diritto vol. 154.*

REID, V., *The Human fetus preferentially engages with face-like visual stimuli,* Current Biology, 2017;

VACCA, J., *Biometric Technolgies and Verification Systems,* Elsevier, 2007;

VIGNA A.G., *La minaccia del terrorismo allo stato libero di diritto: i mezzi di difesa, in Critica Sociale, 1979, p. 60;*

WOODWARD, J., *Biometrics: Facing up to terrorism,* RAND Arroyo Center, 2001

Fonti normative

Article 29 Data Protection Working Party, *Working document on biometrics, 720/12/EN,* 2013;

Article 29 Data Protection Working Party, *Opinion 2/2012 on facial recognition in online and mobile devices, 727/12/EN,* 2012;

National Commission on Terrorist Attacks on United States, 384, 2004;

CGUE, *cause riunite C-293/12 e C-593/12,* 2014;

Dal sistema d'informazione Schengen (SIS 1+) al sistema d'informazione Schengen di seconda generazione (SIS II) - https://eur-lex.europa.eu/legal-content/IT/TXT/?URI=LEGISUMM%3Ajil0010I-dentification of Applicants - Migration and Home Affairs - ec.europa.eu;

Report on the proposal for a regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011 (COM(2017)0344 – C8-0217/2017 – 2017/0144(COD)) - http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2018 0018+0+DOC+XML+V0//EN;

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) - https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679;

Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle au-

torità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio - https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ITA;

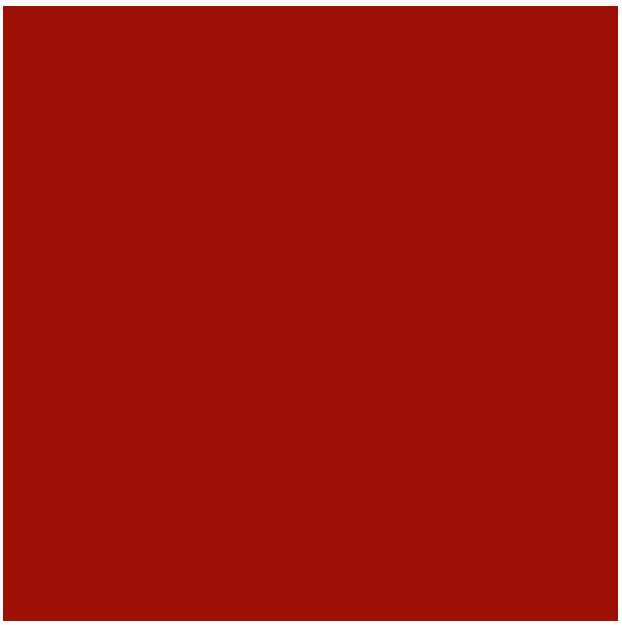
DECRETO LEGISLATIVO 18 maggio 2018, n. 51, Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonchÈ alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. (18G00080) (GU Serie Generale n.119 del 24-05-2018);

DECRETO LEGISLATIVO 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchÈ alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018);

Linee guida in materia di riconoscimento biometrico e firma grafometrica - Allegato A al Provvedimento del Garante del 12 novembre 2014 - Provvedimento Generale prescrittivo in tema di biometria.

NOTE SULL'AUTORE

Francesco Capparelli è Associate & Cyber-security Advisor presso ICT Legal Consulting di Luca Bolognini Paolo Balboni & Partners e Fellow presso l'Istituto Italiano per la Privacy e la Protezione dei Dati Personali.



FONDAZIONE MAGNA CARTA
Via Simeto, 64 ■ 00198 Roma
tel. +39 06 48 80 102 ■ fax +39 06 48 90 72 02
segreteria@magna-carta.it ■ www.magna-carta.it