PREVENZIONE DEI REATI E RICONOSCIMENTO FACCIALE: IL PARERE SFAVOREVOLE DEL GARANTE PRIVACY SUL SISTEMA SARI REAL TIME

Ariella Fonsi

Sommario: 1. Introduzione. – 2. I sistemi di riconoscimento facciale. - 3. Il quadro normativo: le Linee guida del Comitato Consultivo della Convenzione 108 e il Decreto 51/2018. – 4. Il sistema SARI. - 5. Il provvedimento del Garante privacy su SARI Enterprise – 6. Il Parere sfavorevole su SARI Real Time - 7. Osservazioni conclusive.

1. **Introduzione**

Con il provvedimento n. 127 del 25 marzo 2021, l'Autorità garante per la protezione dei dati personali (il "**Garante privacy**" o il "**Garante**"), ha espresso parere sfavorevole in merito all'utilizzo di SARI Real Time (il "**Parere**")[1], ossia il sistema di riconoscimento facciale implementato dal Ministero dell'Interno – Dipartimento di pubblica sicurezza, in grado di coadiuvare l'attività delle forze di polizia e di polizia giudiziaria.

Il Parere si inserisce in un contesto in cui l'utilizzo di sistemi biometrici e, nello specifico, di sistemi di riconoscimento facciale diventa sempre più strategico nella lotta alla criminalità, al terrorismo e, in generale, nell'ambito della tutela dell'incolumità nazionale.

Infatti, in una società in cui la criminalità evolve con il progredire della tecnologia, si è acuita l'esigenza di identificare i soggetti che accedono a luoghi pubblici, informazioni e/o servizi.

In tale contesto, laddove il fattore umano incontra dei limiti nell'effettuare controlli massivi e sistematici sulle persone, il ricorso a macchine "intelligenti" diventa un *asset* strategico per le autorità pubbliche e uno strumento di fondamentale importanza per la sicurezza dei cittadini.

2. I sistemi di riconoscimento facciale

Con l'aumentare del rischio di attacchi terroristici e, in generale, di una criminalità sempre più sofisticata e organizzata, si è ingenerata una crescente esigenza di garantire la sicurezza dei cittadini a fronte del clima di allarme dilagante in luoghi pubblici "ad alto rischio" (si pensi, per esempio, agli aeroporti e alle stazioni ferroviarie).

In tale contesto, come anticipato, l'utilizzo della biometria costituisce un valido alleato nell'individuazione di soggetti potenzialmente pericolosi per la collettività, misurando – mediante metodologie matematiche e statistiche – le variabili fisiologiche e comportamentali proprie di una persona[2].

In particolare, un sistema biometrico può essere definito come un dispositivo automatico per l'identificazione di una persona sulla base di caratteristiche biologiche, che possono essere fisiologiche (se si

riferiscono, ad esempio, ad impronte digitali, il disegno dell'iride, l'immagine del volto) ovvero comportamentali (si pensi al modo di "battere sulla tastiera" di un individuo).

I sistemi di riconoscimento facciale rappresentano, pertanto, una precipua branca della biometria fisiologica, che si occupa di sviluppare algoritmi capaci di confrontare due immagini di un volto umano.

Secondo il Working Party 29 (ora *Europoean Data Protection Board*)[3], il riconoscimento facciale può essere definito come un trattamento automatico di immagini digitali che contengono i volti di persone ai fini di identificazione, autenticazione, verifica o categorizzazione di tali persone e consta di un processo distinto nelle seguenti fasi:

- acquisizione dell'immagine, ossia il processo di rilevamento dei tratti del volto di una persona e la conversione in formato digitale;
- individuazione della presenza di un volto all'interno di un'immagine digitale;
- attenuazione delle variazioni all'interno delle regioni del volto individuate (si pensi alla conversione in una dimensione *standard* o all'allineamento delle distribuzioni del colore);
- estrazione di caratteristiche dell'immagine digitale di una persona;
- registrazione dell'immagine e/o del modello di riferimento per un successivo confronto;
- misurazione delle somiglianze tra una serie di caratteristiche del modello con quelle già registrate nel sistema.

Tali tecnologie, com'è evidente, possono apportare un contributo prezioso all'attività delle forze di polizia, a cui è demandato il compito di identificare un soggetto nel caso in cui ci siano dubbi sulla sua identità, attualmente svolgendo *brevi manu* i rilievi tecnici all'uopo necessari (ad esempio, rilievi descrittivi, dattiloscopici e fotografici svolti nel corso del fermo identificativo).

3. Il quadro normativo: le Linee guida del Comitato Consultivo della Convenzione 108 e il Decreto 51/2018

Come anticipato, il riconoscimento facciale consiste nell'elaborazione automatica di immagini digitali contenenti i volti degli individui per l'identificazione o la verifica di tali individui utilizzando modelli di volti.

Alla luce di quanto precede, emerge chiaramente che tale attività costituisce un trattamento di dati personali e, nello specifico, di dati biometrici, ossia dati relativi a caratteristiche fisiche, fisiologiche o comportamentali di una persona.

In tale contesto, lo scorso 28 gennaio il Comitato Consultivo della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di carattere personale 108/1981 (la "**Convenzione 108**") ha adottato le "*Guidelines on Facial Recognition*" (in italiano, "*Linee guida sul Riconoscimento Facciale*", le "**Linee guida**")[4], individuando specifici orientamenti in materia di riconoscimento facciale e fornendo ad enti quali governi, produttori di sistemi di riconoscimento facciale e pubbliche amministrazioni che utilizzano tali tecnologie le misure idonee a proteggere i diritti e le libertà degli interessati.

In particolare, ai sensi dell'art. 6 della Convenzione 108, il trattamento di speciali categorie di dati - nei quali rientrano i dati biometrici - può essere svolto solo se legittimato da una precipua base giuridica e se nel diritto dello Stato membro in cui è implementato siano previste garanzie adeguate rispetto ai rischi per gli interessati.

Con specifico riferimento al riconoscimento facciale nel settore pubblico, poi, il Comitato Consultivo della Convenzione 108 espressamente sancisce che, dato lo squilibrio di poteri tra i cittadini e le autorità pubbliche, la base giuridica per il trattamento dei dati biometrici deve essere individuata esclusivamente in norme specifiche che garantiscano sia che l'uso di tali tecnologie sia strettamente necessario e proporzionato alle finalità per le quali tale uso è implementato (per esempio, ordine pubblico o emergenza sanitaria) sia le necessarie garanzie da rispettare.

Infine, l'impiego di tali tecnologie per l'identificazione in un ambiente controllato o incontrollato dovrebbe essere limitato, in generale, a fini di sicurezza e dovrebbe essere effettuato esclusivamente dalle autorità competenti in tale settore.

L'impostazione delineata nelle Linee guida trova riscontro nel D.lgs. 51/2018 attuativo della Direttiva UE 680/2016 (il "**Decreto**"), che detta una disciplina per i trattamenti di dati personali per finalità di prevenzione di reati e minacce alla sicurezza pubblica e, anche su delega dell'Autorità Giudiziaria, di indagine, accertamento e perseguimento di reati, configurandosi a tal fine come *lex specialis* rispetto al Regolamento UE 679/2016 ("**GDPR**").

In particolare, il Decreto evidenzia che i trattamenti in commento determinano una forte interferenza con la vita privata delle persone e, pertanto, devono trovare "giustificazione" in un'adeguata base normativa.

L'art. 5 del Decreto, infatti, dispone che i trattamenti di dati personali[5] da parte degli organi di polizia devono basarsi su disposizioni di legge ovvero di regolamento.

Inoltre, il successivo art. 7 sancisce che il trattamento dei dati particolari di cui all'articolo 9, GDPR[6] (nello specifico dati biometrici intesi a identificare in modo univoco una persona fisica) da parte di pubbliche autorità a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali può essere effettuato "*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 ad oggetto dati resi manifestamente pubblici dall'interessato".

Le previsioni contenute del Decreto risultano inoltre coerenti con i principi generali stabiliti dal diritto unionale e, in particolare, dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (la "**CEDU**") e dalla Carta dei Diritti Fondamentali dell'Unione Europea (la "**Carta**").

Con riferimento alla prima, l'art. 8, CEDU prevede che ogni persona ha diritto al rispetto della propria vita privata e familiare e che "*non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*".

Infine, l'art. 52 della Carta stabilisce che eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla stessa (quali il rispetto della vita privata[7] e la protezione dei dati personali[8]) devono essere previste dalla legge e devono, altresì, rispettare il contenuto essenziale di detti libertà e diritti.

4. Il sistema SARI

Nel febbraio 2017, il Ministero dell'Interno – Dipartimento di pubblica sicurezza aveva bandito una procedura volta alla fornitura di una soluzione per l'allestimento di un Sistema Automatico di Riconoscimento d'Immagini ("**SARI**"), volto a gestire due diversi scenari operativi.

Da un lato, il Ministero aveva previsto uno scenario *enterprise* ("**SARI Enterprise**"), con un sistema in grado di ricercare un volto presente in un'immagine in modo automatico, per mezzo di algoritmi di riconoscimento facciale, all'interno di una banca dati di soggetti fotosegnalati (nello specifico, il *database Automatic Fingerprint Identification System*, "**AFIS**")

Dall'altro, è stato specificamente richiesto uno scenario *real-time* ("**SARI Real Time**") - che doveva impiegare come *engine* principale quello dello scenario *enterprise* - in cui il sistema analizza in tempo reale i volti dei soggetti ripresi da telecamere installate in un'area geografica circoscritta e delineata, per poi confrontarli con i dati presenti in una banca dati ristretta e predefinita denominata "*watch-list*" (della grandezza dell'ordine di migliaia di immagini), con generazione di un *alert* per gli operatori in caso di confronto positivo.

5. Il provvedimento del Garante privacy su SARI Enterprise

Con riferimento al primo scenario, all'esito della fase si sperimentazione del sistema SARI terminato nel settembre 2018[9], il Garante - con il provvedimento n. 440/2018 – aveva avuto modo di osservare che il trattamento di dati personali realizzato tramite SARI Enterprise non presenta criticità sotto un profilo privacy[10].

In particolare, SARI Enterprise affianca il sistema AFIS-SSA[11], che consente di effettuare ricerche nell'archivio AFIS tramite l'opera manuale di un addetto, il quale, a tal fine, deve inserire nella maschera di interrogazione informazioni quali anagrafiche, connotati e segni di vario genere (per esempio, colore dei capelli e degli occhi).

In tale contesto, il sistema SARI Enterprise si limita ad automatizzare le operazioni di cui sopra, consentendo un'elaborazione automatica della ricerca nel *database* di soggetti fotosegnalati e, pertanto, costituisce un trattamento di dati personali già previsto e disciplinato dalle fonti normative e, nello specifico, da quelle individuate nel Decreto del Ministro dell'interno del 24 maggio 2017 (recante l'individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da forze di polizia effettuati con strumenti elettronici, in attuazione dell'art. 53, comma 3, del D.lgs 196/2003).

Inoltre, a parere del Garante privacy, il requisito della stretta necessità del trattamento risulta confermato dalla connessione di tale sistema rispetto alle attività di identificazione svolte dalle forze di polizia, costituendo "*un mero ausilio all'agire umano, avente lo scopo di velocizzare l'identificazione, da parte dell'operatore di polizia, di un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato*".

In conclusione, con riferimento al trattamento dell'immagine facciale per mezzo del sistema SARI Enterprise, il requisito della necessaria previsione normativa del trattamento di cui all'art. 7 del Decreto deve ritenersi soddisfatto dalle numerose disposizioni legislative e regolamentari citate nella scheda 19 del summenzionato Decreto del Ministro dell'interno[12], che recano, altresì, le necessarie garanzie per l'interessato.

6. Il Parere sfavorevole su SARI Real Time

Nel 2021 il Garante privacy ha avuto modo di esprimersi anche sul secondo scenario, a valle della descrizione del sistema SARI Real Time inoltrato dal Ministero dell'Interno, unitamente alla valutazione di impatto ai sensi dell'art. 23 del Decreto.

Vale la pena di precisare che l'articolo in commento pone in capo al titolare del trattamento[13] l'onere di effettuare una valutazione d'impatto sulla protezione dei dati personali tutte le volte in cui "*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*".

In particolare, il secondo comma dell'art. 23 richiede che la valutazione contenga:

- una descrizione generale dei trattamenti previsti;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare tali rischi;
- le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e il rispetto Decreto.

Quanto alla descrizione dei trattamenti, dalla documentazione prodotta emergeva che SARI Real Time – attualmente non ancora in uso – consentirebbe, da un lato, di analizzare i volti dei soggetti ripresi con le modalità descritte nel precedente paragrafo 4 e, dall'altro, registrare i flussi video delle telecamere, fungendo, pertanto, da attività di videosorveglianza.

All'interno della valutazione d'impatto, il Ministero richiamava numerose disposizioni che avrebbero dovuto legittimare il trattamento in oggetto, tra cui alcuni articoli del Codice di procedura penale, del Testo unico delle leggi di pubblica sicurezza ("**TULPS**") e del D.P.R. 15/2018 recante l'individuazione delle modalità di attuazione dei principi del Codice relativamente al trattamento dei dati effettuato per le finalità di polizia.

Con riferimento alle summenzionate disposizioni di legge, il Garante ha avuto modo di osservare nello specifico che:

- l'art. 1 del TULPS[14] prevede i compiti generali dell'attività dell'Autorità di pubblica sicurezza, senza operare alcun riferimento al trattamento di dati biometrici; e partimenti
- gli artt. 134 comma 4, 234, 266 e 431 comma 1, lett. b), del Codice di procedura penale - relativi alla documentazione degli atti per riproduzione audiovisiva, l'acquisizione di documenti mediante fotografia ed altri mezzi e l'intercettazione di flussi di comunicazioni telematiche o tra presenti mediante dispositivi elettronici portatili - non possono costituire precipua base giuridica per trattamenti di dati biometrici diretti all'identificazione personale; e ancora
- gli artt. 55, 348, 354 e 370 del Codice di procedura penale, che attengono alle funzioni di polizia giudiziaria nell'assicurare le fonti di prova e nel condurre accertamenti su luoghi o persone, di iniziativa o su delega dell'Autorità giudiziaria, non prevedono il trattamento dei dati biometrici; infine
- il Capo V del D.P.R. 15/2018 prevede e disciplina il trattamento dei dati attraverso sistemi di videosorveglianza e di ripresa fotografica, audio e video, "*sistemi ontologicamente diversi da quelli dei*

dati biometrici"[15].

Alla luce di quanto precede, le suddette fonti normative non risultano soddisfare - a parere del Garante - i requisiti di specificità richiesti dal Decreto per il trattamento dei dati biometrici per finalità di sicurezza pubblica e repressione dei reati, che, tra l'altro, "*non può considerarsi, di per sé, fonte normativa idonea a legittimarli, in quanto è diretto a specificare le condizioni che ne consentono l'effettuazione, tra le quali individua, appunto, la sussistenza di una norma del diritto dell'Unione o dello Stato nazionale che lo autorizzi specificamente*".

Pertanto, conclude il Garante privacy, allo stato non è possibile individuare alcuna base giuridica ai sensi dell'art. 7 del Decreto, idonea a consentire il trattamento dei dati biometrici per le finalità in argomento, diverso e ulteriore rispetto a quelli individuato con riferimento a SARI Enterprise.

7. Osservazioni conclusive

Come osservato dal Garante, il trattamento di immagini volte ad identificare soggetti nell'ambito della pubblica sicurezza è un argomento di estrema delicatezza e, pertanto, necessita di un'attenta ponderazione d'insieme, al fine di evitare che singole iniziative, sommate tra loro, definiscano un nuovo modello di sorveglianza e "*introducano, di fatto, un cambiamento non reversibile nel rapporto tra individuo ed autorità*".

In tale contesto, il sistema SARI Real Time determinerebbe un'evoluzione dell'attività di sorveglianza, passando da adempimento mirato nei confronti di specifici individui ad osservazione *tout court* per finalità di pubblica sicurezza, generando modelli di tutti i consociati per confrontarli con quelli delle persone incluse nella citata *watch-list*.

Lo scenario delineato - in Italia ancora ipotetico - è già in alcuni Paesi del mondo una realtà che ha costituito una svolta nella repressione dei reati.

Si pensi, per esempio, alla Cina e alla Russia che, con un approccio centralizzato e ingenti investimenti pubblici, hanno già "sdoganato" un sistema di controllo basato su tecnologie di riconoscimento facciale in ambito di sicurezza e prevenzione dei reati.

E ancora, si guardi agli USA che - nell'ottica di una politica liberale - danno ampio spazio alla ricerca privata, con scarsi interventi pubblici, affrontando i grandi temi etici, politici e legali solo a seguito di istanze da parte di specifici gruppi di interesse.

La via europea, differentemente da USA, Cina e Russia, è orientata ad una cooperazione tra gli Stati membri improntata a favorire uno sviluppo tecnologico "umanocentrico"[16].

Tale attenzione è confermata - *inter alia* - dalle Linee guida che, nell'ambito dell'utilizzo di tecnologie di riconoscimento facciale per finalità di prevenzione, segnalano l'"intrusività" che tale utilizzo comporta per il diritto alla vita privata e alla privacy degli individui e, in generale, per i diritti e le libertà fondamentali.

Ciò si traduce nell'esigenza a che i singoli Stati membri assicurino - con un impegno costante e proporzionato - le necessarie garanzie normative volte a rendere adeguatamente prevedibile l'uso di tali sistemi e a non conferire un'eccessiva discrezionalità alla pubblica autorità sull'utilizzo degli stessi, determinando, altresì, i limiti dei sistemi in oggetto e stimando (e quindi attenuando) le conseguenze per gli interessati in caso di errori (si pensi, ad esempio, ai falsi positivi).

In Italia, molti sono ancora gli interrogativi - invero già portati all'attenzione del Parlamento in una recente interrogazione – a cui il legislatore dovrà dare una chiara e precisa risposta normativa, prevedendo sia l'*an* (ossia la possibilità di effettuare il trattamento di dati biometrici con le anzidette modalità) sia il *quomodo*, disciplinando, ad esempio, i *database* a cui il sistema SARI può eventualmente attingere oltre all'AFIS e i cittadini inclusi in tali banche dati, nonché i controlli **svolti sugli accessi al sistema di riconoscimento.**

[1] Il provvedimento n. 127 adottato dall'Autorità garante per la protezione dei dati personali il 25 marzo 2021 è disponibile al seguente

URL: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877.

[2] Sul punto, "*Riconoscimento dei volti: un sistema orientato all'uso di metodologie neurali*", di F. Perrone e S. Di Iorio, in IISFA Memberbook 2017 DIGITAL FORENSICS.

[3] Si legga, nello specifico, il "*Parere 2/2012 relativo al riconoscimento facciale nell'ambito dei servizi online e mobili*" adottato dal Working Party 29 il 22 marzo 2012.

[4] Le "*Guidelines on Facial Recognition*" adottate il 28 gennaio 2021 dal Comitato Consultivo della Convenzione *sulla protezione delle persone rispetto al trattamento automatizzato di carattere personale* 108/1981 sono disponibili al seguente URL: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.

[5] Per "trattamento" s'intende "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, 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*" (art. 2, par. 1, lett. b), Decreto).

[6] L'art. 9 GDPR annovera, in particolare, tra le particolari categorie di dati personali quelli che rivelano

"*l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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*".

[7] Il diritto alla vita privata di cui all'art. 7 della Carta recita: "*ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni*".

[8] Il diritto alla protezione dei dati personali è stabilito di cui all'art. 8 della Carta recita: "*ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*".

[9] Si legga il comunicato del Ministero dell'Interno, disponibile al seguente URL:

https://www.interno.gov.it/it/notizie/sistema-automatico-riconoscimento-immagini-futuro-diventa-realta.

[10] Il provvedimento n. 440 adottato dall'Autorità garante per la protezione dei dati personali il 26 luglio 2018 è disponibile al seguente URL: https://www.garanteprivacy.it/web/guest/docweb/GarantePrivacy-9040256-1.6 (3).pdf.

[11] In particolare, il "Sotto Sistema Anagrafico" (SSA) è un sistema informatico in grado di effettuare ricerche avanzate nell'archivio di soggetti fotosegnalati, consentendo la piena fruizione del patrimonio informativo contenuto nella banca dati AFIS. Mediante tale sistema di ricerca (accessibile via web soltanto ad utenti autorizzati e da postazioni abilitate) è possibile interrogare anagraficamente gli archivi elettronici dell'AFIS sulla base dei diversi parametri (generalità, nazionalità, rilievi descrittivi, *etc.*) acquisiti all'atto della segnalazione. L'applicativo SSA permette quindi di visualizzare le fotosegnalatiche dei soggetti selezionati in base al tipo di ricerca, unitamente ai relativi *alias*, di esportarle in formato elettronico e di stamparle, nonché di mantenere un archivio delle ricerche effettuate, integrandole o affinandole successivamente sulla base di ulteriori elementi.

[12] Nello specifico, il trattamento dei dati biometrici ricavabili dall'immagine del volto di un individuo effettuato dalle forze di polizia a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, troverebbe idonea base giuridica in una pluralità di fonti normative, tra cui: l'art. 4 del Testo unico delle leggi di pubblica sicurezza; l'art. 349 del Codice di procedura penale; l'art. 11 del decreto legge 21 marzo 1978, n. 59, convertito in legge 18 maggio 1978, n. 191; l'art. 5 del decreto legislativo

25 luglio 1998, n. 286.

[13] Per "titolare del trattamento" s'intende "*l'autorità competente 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 europea o dello Stato, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere previsti dal diritto dell'Unione europea o dello Stato*" (art. 2, par. 1, lett. h), Decreto).

[14] In particolare, l'art. 1 del TULPS recita: "*l'autorità di pubblica sicurezza veglia al mantenimento dell'ordine pubblico, alla sicurezza dei cittadini, alla loro incolumità e alla tutela della proprietà; cura l'osservanza delle leggi e dei regolamenti generali e speciali dello Stato, delle provincie e dei comuni, nonché delle ordinanze delle Autorità; presta soccorso nel caso di pubblici e privati infortuni. Per mezzo dei suoi ufficiali, ed a richiesta delle parti, provvede alla bonaria composizione dei dissidi privati. L'autorità di pubblica sicurezza è provinciale e locale. Le attribuzioni dell'autorità provinciale di pubblica sicurezza sono esercitate dal prefetto e dal questore; quelle dell'autorità locale dal capo dell'ufficio di pubblica sicurezza del luogo o, in mancanza, dal Podestà*".

[15] Sul punto, si noti che il Considerando 51 del GDPR chiarisce che: "*meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali [...] Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica. Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito nei casi specifici di cui al presente regolamento, tenendo conto del fatto che il diritto degli Stati membri può stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del presente regolamento ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Oltre ai requisiti specifici per tale trattamento, dovrebbero applicarsi i principi generali e altre norme del presente regolamento, in particolare per quanto riguarda le condizioni per il trattamento lecito*".

[16] Sul punto, "*Intelligenza artificiale, cos'è, come funziona e le applicazioni in Italia ed Europa*", di M. Nicotra, in Agenda digitale, disponibile al seguente URL:

https://www.agendadigitale.eu/sicurezza/privacy/intelligenza-artificiale-la-via-delleuropa-su-regole-e-investimenti/.