



Parere su uno schema di d.P.R. ai sensi dell'art. 57 del Codice, in tema di modalità attuative dei principi di protezione dei dati personali relativamente ai trattamenti effettuati per finalità di polizia da Organi, Uffici e Comandi di polizia - 2 marzo 2017

Registro dei provvedimenti
n. 86 del 2 marzo 2017

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti e del dott. Giuseppe Busia, segretario generale;

Vista la richiesta di parere del Ministero dell'Interno;

Visto l'art. 154, comma 4, del d.lgs. 30 giugno 2003, n. 196 recante Codice in materia di protezione dei dati personali (di seguito Codice);

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore la dott.ssa Augusta Iannini;

PREMESSO

Il Ministero dell'interno ha chiesto il parere del Garante in ordine a uno schema di decreto del Presidente della Repubblica concernente l'individuazione delle modalità attuative dei principi di protezione dei dati personali relativamente ai trattamenti effettuati per finalità di polizia da Organi, Uffici e Comandi di polizia, con il quale viene data attuazione all'articolo 57 del Codice. Il provvedimento è inteso ad introdurre una disciplina di carattere generale, applicabile a tutti i trattamenti di dati effettuati per le finalità sopra indicate dalle suddette autorità.

Il Ministero ha predisposto un ulteriore provvedimento, sempre da emanarsi in attuazione dell'art. 57, sul quale il Garante si accinge a rendere parere, finalizzato a disciplinare le procedure di raccolta, accesso, correzione e cancellazione dei dati e delle informazioni registrate negli archivi magnetici del centro elaborazione dati (C.E.D.) del Ministero dell'Interno.

In tal modo, considerando anche il decreto che sarà adottato ai sensi dell'art. 53 del Codice, che individua i trattamenti non occasionali di dati personali svolti per finalità di polizia con strumenti elettronici ed i relativi titolari, su cui il Garante ha appena reso parere, il Titolo II della Parte II del Codice risulterà finalmente attuato.

RILEVATO

1. Il Ministero dell'Interno nella Relazione illustrativa rappresenta che lo schema si pone quale normativa di riferimento per tutti i trattamenti di dati personali, attuali e futuri, direttamente correlati, ai sensi dell'articolo 53 del Codice, «... all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e la repressione dei reati ...», configurandosi quale cornice giuridica - coerente con la normativa comunitaria di settore - entro la quale potranno adottarsi, ove necessarie, le disposizioni di dettaglio relative ai singoli trattamenti.

Rappresenta inoltre che la molteplicità ed eterogeneità dei trattamenti oggetto di disciplina, come evidenziato anche nei trattamenti censiti ai fini della predisposizione dello schema di decreto attuativo dell'articolo 53, comma 3 del Codice, hanno reso necessario prevedere norme di ampio respiro applicabili a tutte le tipologie di trattamento e a tutti gli organi, uffici e comandi di polizia, rinviando a un diverso livello regolatorio l'adozione di normative di dettaglio, anche di natura tecnica, o di misure organizzative attuative della disciplina regolamentare.

2. In relazione al secondo decreto attuativo dell'art. 57 del Codice - ai sensi del quale, secondo quanto riportato Ministero dell'Interno nella Relazione illustrativa, verranno disciplinate le modalità di applicazione dei principi del Codice ai trattamenti di dati personali effettuati, per le finalità di polizia, dal Centro Elaborazione Dati di cui all'art. 8 della legge n. 121/1981 - si rappresenta che i principi e le modalità di trattamento enucleati nel decreto oggetto del presente parere potranno essere ivi tenuti presenti, senza essere rielaborati nel dettaglio, attraverso una o più semplici norme di rinvio. Ciò nell'ottica di semplificare e facilitare l'attuazione degli adempimenti previsti dal Codice.

L'articolo 57 elenca in particolare alcuni istituti che dovranno essere disciplinati nel provvedimento attuativo dell'articolo stesso.

L'elencazione non è peraltro da considerarsi esaustiva, tenuto presente che l'art. 53 esclude dall'applicazione anche, tra l'altro, disposizioni del Codice relative alle modalità di esercizio dei diritti dell'interessato (art. 9), al riscontro reso dal titolare del trattamento alla richiesta di accesso, rettifica, cancellazione (art. 10), all'informativa da rendere a questi (art. 13), alla cessazione del trattamento (art. 16), che vanno disciplinate nello schema di decreto sottoposto al Garante.

3. Il quadro normativo a livello di diritto dell'Unione europea si è negli anni arricchito, pervenendo all'adozione della Decisione quadro 2008/977/GAI ed oggi della Direttiva (UE) 2016/680 (che tra l'altro abroga la Decisione quadro). La Direttiva è in vigore dal 5 maggio 2016 e, pur non essendo ancora trascorso il termine entro il quale dovrà essere trasposta nell'ordinamento nazionale (il 5 maggio 2018), occorre che eventuali disposizioni introdotte nel frattempo non siano in conflitto con quanto dalla stessa previsto.

Per tale ragione quindi è apprezzabile che il Ministero, abbia convenuto di inserire un riferimento alla Direttiva (UE) 2016/680 nel preambolo e si sia ispirato a disposizioni della stessa in taluni casi, come indicato nella relazione illustrativa. Ciò da un lato consente un'applicazione dell'art. 57 che tenga conto del lasso di tempo trascorso dall'approvazione del Codice e della progressiva attrazione nell'orbita della normativa dell'Unione europea di settori prima ricadenti esclusivamente nelle competenze degli Stati, con l'introduzione di norme e "standard" comuni in materia di protezione dei dati personali, dall'altro consente di rendere più stabili nel tempo le disposizioni che si intendono adottare, da considerare, con gli accorgimenti e le specificazioni che il Garante si appresta ad indicare nel presente parere, in linea con le disposizioni della Direttiva.

4. Il presente parere si riferisce a una versione aggiornata dello schema che tiene conto degli approfondimenti svolti nell'ambito di alcuni incontri tenutisi presso quest'Autorità e che in parte recepisce le indicazioni da questa formulate al fine di conformare pienamente il trattamento dei dati ai principi del Codice ed agli standard europei in materia. In particolare i suggerimenti del Garante hanno riguardato: l'opportunità di adeguare l'articolato alle disposizioni della Direttiva (UE) 680/2016 in modo da evitare disposizioni con essa contrastanti o non in linea e di inserire un riferimento alla stessa nel preambolo dello schema; la necessità di dare compiuta attuazione agli specifici aspetti indicati dall'articolo 57, tenendo presente la Raccomandazione 87 (15) e la Decisione quadro 2008/977/GAI, nel rispetto dei principi del Codice, segnatamente dell'articolo 11, in relazione alla finalità dei trattamenti ed al trattamento ulteriore dei dati, ai trattamenti effettuati per finalità di analisi e per esigenze temporanee, alla comunicazione e diffusione dei dati, all'utilizzo di particolari tecniche (videosorveglianza, apparecchi a pilotaggio remoto), alla sicurezza dei dati e dei sistemi, ai termini di conservazione dei dati. Le osservazioni formulate in seguito saranno limitate agli aspetti tuttora irrisolti ovvero a specifici punti dello schema ritenuti meritevoli di ulteriori affinamenti in modo da rendere il testo pienamente conforme al quadro normativo di riferimento.

RITENUTO

5.1. - CAPO I - Disposizioni generali

Art. 1 - Oggetto e ambito di applicazione

Il comma 1, individua l'oggetto del regolamento riprendendo alla lettera il testo dell'articolo 57, comma 1, del Codice, del quale costituisce attuazione.

Riguardo all'ambito di applicazione soggettiva, ed in relazione a specifica richiesta su cui infra in relazione all'articolo 12, relativo alla comunicazione dei dati tra forze di polizia, la relazione illustrativa precisa che la locuzione «organi, uffici e comandi di polizia» utilizzata dal regolamento (mutuata dall'articolo 57, comma 1, del Codice), fa riferimento a un'area di operatività circoscritta rispetto a quella desumibile dalla nozione di «organi di pubblica sicurezza o altri soggetti pubblici», ai quali, ai sensi dell'articolo 53, comma 2, del Codice, è consentito il trattamento dei dati personali acquisiti per finalità di polizia usufruendo dello speciale regime derogatorio. Lo schema di d.P.R., quindi, non si applica direttamente ai trattamenti effettuati, ad esempio, dalle Prefetture, dagli uffici dell'Agenzia delle Dogane, ecc., difettando per essi l'attributo "di polizia" né alla polizia municipale, cui l'articolo 1 della legge 7 marzo 1986, n. 65, recante «Legge-quadro sull'ordinamento della polizia municipale», attribuisce il compito istituzionale di «svolgere funzioni di polizia locale». Tale "funzione di polizia locale", prosegue la relazione illustrativa, in base alle disposizioni legislative (art. 159, d.lgs. 112 del 1998) e costituzionali (art. 117, comma 1, lett. h, Cost.) e anche alle indicazioni offerte dalla Corte Costituzionale, sarebbe riconducibile ad attività meramente amministrative, finalizzate ad assicurare l'osservanza di norme pubblicistiche collocate in materie di competenza regionale (sanità, turismo, ecc.). La "polizia amministrativa locale" (polizia sanitaria, polizia urbanistica, ecc.), quindi, si esplica con lo svolgimento di attività non assimilabili affatto al mantenimento dell'ordine pubblico e della sicurezza in senso stretto e di prevenzione dei reati, la quale, al contrario, contraddistingue l'attività delle forze di polizia (ex articolo 16 della legge n. 121 del 1981), svolta sotto la guida del Ministero dell'interno.

La circostanza che la polizia municipale possa anche svolgere "funzioni di polizia giudiziaria" limitate («... nell'ambito territoriale dell'ente di appartenenza e nei limiti delle proprie attribuzioni ...») non contraddice l'anzidetta esclusione soggettiva; si tratta, infatti, di circoscritte attività di cooperazione con l'autorità giudiziaria penale, quando, in occasione dello svolgimento delle attività amministrative istituzionali, si renda necessario l'accertamento e la repressione dei reati.

Art. 4 - Qualità dei dati trattati

Il comma 1, esplicita i principi riguardanti le caratteristiche dei dati personali oggetto di trattamento, come individuati dall'articolo 11, comma 1, del Codice: esattezza, aggiornamento (se necessario), completezza, pertinenza e non eccedenza.

Il comma 2, richiama l'obbligo per gli organi, uffici e comandi di polizia di assicurare la verifica degli anzidetti requisiti, con le modalità di cui all'articolo 54, comma 4, del Codice, ove materialmente possibile, in occasione dell'utilizzo dei dati personali nell'ambito di un'attività informativa, di sicurezza o di indagine di polizia giudiziaria.

Il comma 3, inserito a seguito delle interlocuzioni avute, prevede che il titolare o il responsabile del trattamento diano notizia al Garante delle direttive eventualmente impartite in merito alle verifiche di cui al comma 2.

Al riguardo appare necessario sopprimere la parola "eventualmente", in quanto la presenza di direttive è indispensabile per garantire l'effettuazione della verifica della qualità dei dati.

Art. 5 - Configurazione dei sistemi informativi e dei programmi informatici

L'articolo riprende il principio, enunciato nell'articolo 3 del Codice - riferibile ai trattamenti automatizzati - secondo il quale i sistemi informativi devono essere configurati in modo da ridurre al minimo l'utilizzo dei dati personali. Dispone, inoltre, al comma 2, che i nuovi sistemi informativi siano progettati in modo che i dati personali possano essere cancellati o resi anonimi con modalità automatizzate allo scadere dei termini di conservazione previsti dal successivo articolo 10 ed, inoltre, in modo da consentire la registrazione in appositi registri, degli accessi e delle operazioni effettuati dagli operatori abilitati nei casi in cui ciò sia previsto dall'ordinamento. Nel valutare positivamente l'inserimento di questa ultima disposizione, si fa presente, tuttavia, che andrebbero soppresse le parole "nei casi in cui ciò sia previsto da disposizioni di legge o di regolamento, da atti normativi dell'Unione europea o dal diritto internazionale".

Ciò in quanto l'art. 25 della Direttiva (UE) 2016/680 già prevede che gli Stati membri dispongano che siano registrati in sistemi di trattamento automatizzato almeno i seguenti trattamenti: raccolta, modifica, consultazione, comunicazione, inclusi i trasferimenti, interconnessione e cancellazione, e pertanto il riferimento indicato sopra appare come una limitazione rispetto all'obbligo introdotto dalla Direttiva.

Art. 6 (Trattamenti che presentano rischi specifici) e art. 7 (Uso di particolari tecniche di elaborazione delle informazioni)

L'articolo 6, al comma 1, prevede che ai trattamenti di dati personali che implicano maggiori rischi di un danno alla persona interessata e, in particolare, alle banche di dati genetici e biometrici, alle tecniche basate su dati relativi all'ubicazione, alle banche dati basate su particolari tecniche di elaborazione delle informazioni o su particolari tecnologie, si applicano le previsioni dell'articolo 55 del Codice riguardanti peculiari garanzie per l'interessato. Dei trattamenti in questione, pertanto, dovrà essere data preventiva comunicazione al Garante anche ai fini della prescrizione di particolari misure e accorgimenti a tutela della riservatezza degli interessati.

Il comma 2, stabilisce per i dati in esame, ove trattati con l'ausilio di strumenti elettronici, la registrazione degli accessi e delle operazioni effettuati dagli operatori abilitati ed il comma 3, a tutela della riservatezza degli operatori abilitati, definisce le specifiche finalità per le quali è consentito l'accesso ai registri degli accessi e delle operazioni (file di log).

Il nuovo testo tiene conto delle interlocuzioni avute e, ai fini dell'attuazione del criterio indicato in particolare alla lettera f) (ed in parte alla lettera a) dell'articolo 57 del Codice, nell'articolo è stato anche inserito l'articolo 7, inteso a disciplinare l'uso, anche per finalità di analisi, di particolari tecniche di elaborazione delle informazioni, inclusi i sistemi di indice, indicando le particolari cautele necessarie per garantire la correttezza e liceità del trattamento.

Al riguardo, sembra opportuno prevedere che le due disposizioni siano meglio articolate e pertanto si ritiene di suggerire di sostituire all'art. 6, comma 1 le parole "banche dati basate su particolari tecniche" con le seguenti: "banche dati e trattamenti di cui all'art. 7 basati su particolari tecniche"; conseguentemente all' art. 7, comma 1, eliminare le parole "fuori dai casi previsti dall'art. 6".

La modifica è richiesta in quanto anche trattamenti di cui l'art. 7 presentano rischi specifici, per cui il testo degli articoli 6 e 7 va armonizzato nel modo indicato.

5.2 – CAPO II - Termini di conservazione dei dati

Il Capo II, composto dal solo articolo 10, intende dare attuazione all'articolo 11, comma 1, lettera e) del Codice – secondo il quale i dati personali sono «conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati» (tutela del "diritto all'oblio") – come pure dell'articolo 57, comma 1, lett. d), del Codice per il quale l'«individuazione di specifici termini di conservazione dei dati in relazione alla natura dei dati o agli strumenti utilizzati per il loro trattamento, nonché alla tipologia dei procedimenti nell'ambito dei quali essi sono trattati o i provvedimenti sono adottati», rappresenta un fondamentale aspetto da disciplinare con il presente schema di regolamento, individuando i tempi di conservazione delle diverse categorie di dati trattati per le finalità "di polizia".

Il comma 2 dell'art. 10, allo scopo di contemperare le finalità di polizia con le esigenze di tutela della riservatezza degli interessati relativamente ai dati personali soggetti a trattamento automatizzato, prevede, in ossequio ai principi di "necessità" e "proporzionalità", che, trascorsa la metà del tempo massimo di conservazione di cui al comma 3 (se pari o superiore a trent'anni), ad essi possano accedere solo gli operatori incaricati del trattamento ai sensi dell'articolo 30 del Codice, a ciò autorizzati per il compimento di specifiche operazioni nell'ambito di attività informative, di sicurezza o di indagine di polizia giudiziaria. Tuttavia questa previsione non consente di sopperire alle criticità rappresentate nel corso degli incontri avuti, in relazione a tempi di conservazione, la cui durata non appare adeguatamente giustificata.

I termini massimi di conservazione indicati al comma 3, sono nella relazione illustrativa, raggruppati come segue:

"- con riferimento ai dati personali correlati a provvedimenti restrittivi della sfera giuridica dell'interessato adottati a seguito di sentenza di condanna o di procedimento cautelare - lett. a), b), h), p) e q) – sono stati individuati tempi di conservazione compresi tra 50 e 80 anni, in considerazione della necessità di poter reperire i dati e le informazioni personali, non solo durante il periodo di esecuzione della misura restrittiva (che potrebbe essere molto lungo), ma anche successivamente per un tempo congruo alle esigenze primarie di tutela dell'ordine e della sicurezza pubblica nonché di prevenzione e repressione dei reati;

- con riferimento ai dati personali relativi ad attività informative ed ispettive – lett. e) – e di prevenzione generale – lett. k) e lett. j) – sono stati individuati tempi di conservazione rispettivamente pari a 50, 30 e 15 anni - graduati in ragione della tipologia di dati - ritenuti congrui con riferimento all'arco temporale (parametrato sull'aspettativa media di vita), entro il quale potrebbero emergere evidenze significative per le finalità di polizia; per coerenza, in 30 anni è stato fissato il termine massimo di conservazione dei dati, strumentalmente correlati a quelli soprarichiamati, relativi alla gestione delle attività operative, lett. r);

- in relazione ai dati correlati ad attività di polizia giudiziaria conclusa con provvedimento di archiviazione e di assoluzione – lett. f) e lett. g) – sono stati individuati tempi di conservazione pari a 50 anni, ritenuti congrui con precipuo riferimento alle esigenze investigative. Il provvedimento di archiviazione è, infatti, l'atto conclusivo di un procedimento penale nell'ambito del quale non è stato possibile acquisire elementi idonei a sostenere l'accusa in giudizio, con la possibilità, tuttavia, di una riapertura delle indagini (c.d. cold case) che implica normalmente una rivisitazione delle attività già svolte. La sentenza di assoluzione anche sottende un processo che non si è concluso con la condanna dell'autore del reato e, pertanto, non esclude una riapertura delle indagini per quello stesso fatto, anche a distanza di tempo, rendendo necessario un riesame delle attività già svolte;

- valutazioni analoghe a quelle di cui al punto precedente sono state poste a fondamento dell'individuazione dei tempi di conservazione dei dati di cui alla lettera i), con la precisazione che in questi casi l'attività investigativa non ha avuto un esito positivo sfociato in un'informativa all'autorità giudiziaria;

- con riferimento ai dati raccolti per l'analisi criminale – lett. l) – il tempo massimo di conservazione, 20 anni, è stato individuato in considerazione della rilevanza strategica che tali dati rivestono nello svolgimento delle analisi che per loro natura possono riguardare archi temporali anche molto lunghi;

- quanto ai dati relativi ai provvedimenti di espulsione e rimpatrio, il termine di conservazione – 50 anni - è stato parametrato in relazione ai tempi di conservazione previsti dalla normativa archivistica dettata dal Ministero per i beni e le attività culturali per il documento cartaceo;

- con riferimento ai dati correlati a provvedimenti autorizzatori – lett. n) - il termine di conservazione, 10 anni, è stato determinato in considerazione della rilevanza che possibili abusi posti in essere nell'esercizio dell'attività "autorizzata" potrebbero assumere per le finalità di polizia."

I termini di conservazione dei dati personali in argomento indicati nello schema di d.P.R. appaiono, infatti, estremamente lunghi, anche se sono stati inseriti alcuni temperamenti indicati sopra, come limitazioni all'accesso ai dati conservati per un tempo pari o superiore ai 30 anni, quando sia decorsa la metà del termine di conservazione.

Il Ministero dell'interno non ha ritenuto di accogliere l'auspicio del Garante di introdurre una differenziazione dei termini di conservazione in relazione alla tipologia o gravità di reato, da individuare, eventualmente, in base alla pena edittale.

Parrebbe, comunque, necessario stabilire termini di conservazione sostanzialmente più brevi, con possibilità di prolungarli nei casi in cui ciò sia effettivamente necessario.

Con riferimento ai trattamenti di cui alle lettere e, i, j, k, q, occorre specificare che i dati relativi a soggetti nei cui confronti non è emerso alcun rilievo siano conservati per un tempo inferiore e che, comunque, nel caso in cui si ritenga necessario conservare tali dati per un periodo maggiore, questo non superi 90 giorni.

Il termine indicato rappresenta un bilanciamento tra le esigenze rappresentate dal Ministero dell'interno, anche in diverse riunioni informali, e tutela dei dati personali.

A tale proposito, si ricorda che il Garante ha avuto occasione di esprimere un parere su un progetto di sperimentazione di "microcamere individuali del personale della Polizia di Stato impiegato nell'attività di controllo del territorio", nel quale, tra l'altro, con riferimento al periodo di conservazione delle immagini registrate dalle microcamere, era previsto che le immagini che non davano evidenza di aspetti rilevanti sarebbero state cancellate dopo sette giorni dalla loro acquisizione, periodo ritenuto necessario per verificare il contenuto delle immagini. Tale periodo di conservazione è stato ritenuto dal Garante congruo, in relazione al contesto organizzativo nel quale le immagini vengono esaminate ed ai diversi profili per i quali esse possono essere rilevanti.

Pertanto, un periodo di conservazione di 90 giorni per le immagini "neutre", appare congruo, in quanto ben più lungo di quello prospettato dalla stessa Amministrazione dell'interno con riferimento al progetto sperimentale delle microcamere individuali ed è inoltre funzionale a corrispondere alle esigenze, rappresentate dal Ministero dell'interno nel corso dei precedenti incontri informali, riferite a casi, che si sarebbero effettivamente verificati, in cui immagini acquisite da sistemi di videosorveglianza e cancellate in breve tempo perché apparentemente irrilevanti, avrebbero assunto rilievo in ordine a vicende criminali avvenute poco tempo dopo.

5.2.1 Termini di conservazione dei dati di video sorveglianza e riprese fotografiche, audio e video.

Con riferimento ai termini di conservazione dei dati raccolti mediante i sistemi di video sorveglianza e delle riprese fotografiche, audio e video, fissati in 5 anni nell'art. 10, comma 3, lettera r, occorre prevedere, in coerenza con quanto sopra precisato, che, i dati relativi a coloro che sono casualmente oggetto di controllo da parte delle forze di polizia e nei cui confronti non è emerso alcun rilievo la conservazione è limitata al massimo a 90 giorni.

5.3 -CAPO III – Raccolta, comunicazione e diffusione dei dati

Art.11 - Limitazioni alla raccolta dei dati

L'articolo intende disciplinare il trattamento dei dati sensibili e dei dati atti a definire profili e personalità dell'interessato, mantenendo il divieto come principio ed indicando le deroghe al comma 2.

Il comma 3, richiama il divieto di basare sul solo trattamento automatizzato di dati, decisioni che implicino una valutazione del comportamento umano.

In tale quadro, appare opportuno inserire, nell'elencazione di cui al comma 1 della norma, anche i dati genetici o biometrici, in coerenza con l'art. 10 della Direttiva (UE) 2016/680, che include tali peculiari informazioni nelle categorie particolari di dati personali. Ciò consentirà di allineare fin da adesso il sistema alle disposizioni europee, che dovranno comunque essere recepite nell'ordinamento entro il 6 maggio 2018.

Art. 12 - Comunicazioni dei dati tra forze di polizia

Al riguardo, come già ricordato al punto 6.1 in relazione all'articolo 1, si rileva la mancata inclusione, tra le Forze di polizia che comunicano tra loro dati personali in argomento, della Polizia locale, pur nel ristretto ambito delle sue competenze.

Il Ministero ha rappresentato che la polizia municipale non può assimilarsi alla categoria degli "organi, uffici e comandi di polizia", in quanto le funzioni da questi svolte sono riconducibili ad attività meramente amministrative.

Art. 13 - Comunicazione dei dati a pubbliche amministrazioni o enti pubblici e a privati

Il comma 3, prevede ulteriori ipotesi nelle quali la comunicazione di dati personali, sia a pubbliche amministrazioni sia a privati, può avvenire.

Al riguardo sembra opportuno espungere il riferimento al consenso della persona interessata, in quanto il consenso non rappresenta elemento condizionante le attività di polizia. Le parole "e questa ha fornito il proprio consenso o, in mancanza, ricorrono circostanze che consentono, in modo inequivoco, di ritenere tale consenso" andrebbero pertanto espunte dal testo.

Art. 14 - Diffusione dei dati e delle immagini personali

Il comma 3 del nuovo testo prevede che siano comunicate al Garante le eventuali direttive adottate in ambito nazionale in materia di diffusione dei dati o delle immagini personali.

La parola "eventuali" andrebbe eliminata, poiché la diffusione in parola può recare sensibile pregiudizio all'interessato. Impartire a tal fine direttive appare necessario per un corretto esercizio di tale attività, e la conoscenza, sia pure ex post, di tali direttive, consente lo svolgimento delle funzioni di garanzia.

5.4 - CAPO IV - Trattamento dei dati nell'ambito dell'attività di cooperazione internazionale di polizia

Il Capo IV disciplina lo scambio di dati con Stati membri e organismi comunitari (articolo 16) e la comunicazione di dati alle autorità competenti degli Stati terzi e ad organismi internazionali, nonché il trattamento dei dati da questi trasmessi (articoli da 17 a 21).

Art. 16: Il comma 1, fa riferimento allo scambio di dati personali con le autorità competenti degli Stati membri e con organismi comunitari, consentendolo nei casi, alle condizioni e con le modalità, stabilite da disposizioni di legge o di regolamento o da atti normativi dell'Unione europea. Il comma 2 fa salvi gli accordi e le intese ratificati e resi esecutivi con Stati membri o con organismi comunitari, a condizione che non siano in contrasto con la normativa nazionale e comunitaria.

La normativa di riferimento, allo stato, è, a livello di diritto dell'Unione europea, la Decisione quadro 2006/960/GAI del Consiglio, del 10 dicembre 2006, relativa allo scambio di informazioni e intelligence tra le Autorità degli Stati membri dell'Unione Europea incaricate dell'applicazione della legge; a livello nazionale, il decreto legislativo 23 aprile 2015, n. 54, recante attuazione nell'ordinamento interno dell'anzidetta Decisione quadro.

Nel corso dei precedenti incontri informali l'Ufficio aveva chiesto al Ministero dell'interno di prevedere che un elenco degli accordi o delle intese sottoscritti e resi esecutivi con Stati terzi o con organismi internazionali che prevedano lo scambio di dati per finalità di polizia sia comunicato al Garante entro 60 giorni dall'entrata in vigore del d.P.R. e tempestivamente aggiornato nonché pubblicato sul sito istituzionale del Ministero dell'Interno.

Il Ministero dell'interno ha eccepito la "possibile natura riservata degli accordi che, peraltro, ai sensi del DM n. 415/1994 (art. 2, comma 1, lett. a) sono sottratti all'accesso per motivi attinenti alla sicurezza, alla difesa nazionale ed alle relazioni internazionali".

Poiché, comunque, la conoscenza di tali accordi è necessaria per lo svolgimento dei controlli di competenza, si invita il Ministero a prevedere la pubblicazione nel sito degli accordi non riservati, in modo che gli interessati abbiano adeguata contezza del quadro normativo, e la trasmissione al Garante di un elenco relativo a tutti gli accordi conclusi.

5.5 - CAPO V - Trattamento dei dati attraverso sistemi di videosorveglianza e di ripresa audio e video

Art. 23 - Sistemi di ripresa fotografica, video e audio

L'articolo si occupa del trattamento per finalità di polizia dei dati personali raccolti mediante riprese fotografiche, audio e video. Anche tale materia sfugge alla puntuale disciplina da parte del Codice, così che la regolamentazione in materia deve necessariamente ricavarsi dai principi e dalle regole generali del Codice, come pure dalle indicazioni fornite dal Garante.

Il comma 1, consente la raccolta e il trattamento dei dati personali mediante sistemi di ripresa fotografica, audio e video quando ciò sia necessario per documentare specifiche attività preventive e repressive di reati, situazioni dalle quali possano derivare minacce per l'ordine e la sicurezza pubblica o un pericolo per la vita o l'incolumità dell'operatore, attività poste in essere durante il servizio che siano espressione di poteri autoritativi.

Il comma 2, in ossequio ai principi di "pertinenza e non eccedenza", analogamente a quanto previsto in materia di videosorveglianza, stabilisce che dovranno essere raccolti solo i dati strettamente necessari per il raggiungimento delle finalità di cui all'articolo 2, registrando esclusivamente le immagini indispensabili.

Il comma 3, introduce una particolare cautela relativamente all'utilizzo di sistemi di ripresa fotografica, video e audio, installati su aeromobili a pilotaggio remoto, stabilendo che debba essere autorizzato al livello gerarchico non inferiore a quello di capo ufficio o comandante di reparto.

Con particolare riferimento agli apparecchi a pilotaggio remoto (APR), in considerazione della particolare invasività del trattamento, l'Ufficio ha rappresentato la necessità di prevedere una norma specifica.

Il Ministero dell'Interno non ritiene, invece, che il trattamento delle immagini acquisite mediante APR possa essere ricondotto sempre e comunque nell'ambito dei trattamenti che presentano rischi specifici, ai sensi dell'art. 5 dovendosi di volta in volta valutare se ricorrano le circostanze di cui all'art. 55 del Codice, richiamato dall'art. 5 citato.

Si ritiene, tuttavia, che il trattamento di dati per mezzo dell'APR costituisca un trattamento che di per sé, in considerazione della particolare tecnologia che utilizza, implica maggiori rischi di un danno all'interessato e si insiste pertanto per l'introduzione di una specifica regolamentazione, all'uopo integrando il comma 3 ed inserendo un riferimento all'articolo 5 dello schema di d.P.R..

5.6 - CAPO VIII - Diritti della persona interessata e controllo sui trattamenti

Art. 29: Il comma 1, richiama quanto disposto dall'art. 160 del Codice Il comma prosegue specificando che il procedimento può essere innescato dalla segnalazione della persona interessata ovvero iniziato d'ufficio.

Il comma 2, traendo ancora spunto dall'articolo 159 del Codice, infine, precisa che ai controlli presenziano il titolare o il responsabile del trattamento che possono farsi coadiuvare da personale di fiducia per gli aspetti di carattere tecnico e amministrativo.

Il comma 3 e il comma 4 prevedono che il Garante, ove accerti che il trattamento non è conforme, indichi al titolare gli interventi necessari e che questi o il responsabile del trattamento adottino le iniziative conseguenziali.

Al riguardo si ritiene che tale articolo possa essere limitato alla prima parte del primo comma, eliminando i commi 2 e 3 e mantenendo il comma 4.

5.7 - CAPO VIII - Disposizioni transitorie e finali.

L' Art. 30 (Disposizioni transitorie), prevede uno speciale regime transitorio inteso a consentire, con riferimento ai trattamenti automatizzati già in uso, l'applicazione delle disposizioni del d.P.R. in modo graduale.

Nella relazione illustrativa si evidenzia come "i sistemi informativi in uso costituiscono un insieme assai eterogeneo dal punto di vista tecnologico che necessita di un complessivo processo di reingegnerizzazione allo scopo di consentire la concreta applicazione delle nuove, più stringenti norme e, in particolare di quelle in materia di termini di conservazione dei dati personali e di registrazione degli accessi e delle operazioni" e che "la norma transitoria, pertanto, tiene conto dell'oggettiva difficoltà e dell'antieconomicità di operare interventi evolutivi in particolare sulle tecnologie legacy ancora in uso, del possibile impatto negativo di repentine modifiche dei sistemi sulle attuali condizioni di interoperabilità, ma soprattutto, attribuisce il necessario rilievo alle questioni finanziarie sottese agli interventi di adeguamento che dovranno essere attuati dalle singole Amministrazioni «senza nuovi o maggiori oneri a carico della finanza pubblica»".

In analogia con quanto previsto dall'articolo 180 del Codice, pertanto, la disposizione introduce cautele intese a consentire il graduale adeguamento, anche in considerazione delle risorse disponibili, dei sistemi informatici, comunque salvaguardando, nella fase transitoria, l'esigenza di prevenire e contenere il rischio di utilizzo contra legem dei dati oggetto di trattamento.

Il comma 1, quindi, fermi restando gli obblighi imposti dall'articolo 5, comma 2, primo periodo, quanto alla progettazione di nuovi sistemi, prevede che gli organi, uffici e comandi di polizia che alla data di entrata in vigore del regolamento non dispongano di sistemi informativi e programmi informatici che consentano, in tutto o in parte, la cancellazione o l'anonimizzazione con modalità automatizzate dei dati personali oggetto di trattamento, o non consentono la segnalazione con modalità automatizzate del decorso del termine di cui all'art. 10, comma 2, adottano ogni possibile misura organizzativa, logistica e procedurale idonea, in relazione agli strumenti informatici detenuti, a prevenire o limitare il rischio di utilizzo oltre i termini di conservazione anzidetti dei dati, o di accesso ai dati in violazione della disposizione di cui all'art. 10, comma 2, curando nel contempo, con la gradualità consentita dalla complessità dell'infrastruttura tecnologica, dalle risorse disponibili e dall'esigenza di espletare le procedure di evidenza pubblica, e comunque entro il termine di 15 anni dalla data di entrata in vigore del regolamento, l'adeguamento dei medesimi strumenti informatici.

Specularmente dispone il comma 2 con riferimento all'ipotesi in cui gli organi, uffici e comandi di polizia, alla data di entrata in vigore del regolamento, non dispongano di sistemi informativi e programmi informatici che consentano, in tutto o in parte, l'immediata applicazione delle disposizioni in materia di registrazione degli accessi e delle operazioni.

In merito si osserva l'opportunità di prevedere una prima informativa al Garante sulle misure temporanee adottate prima dell'adeguamento definitivo dei sistemi, ove ragioni tecniche impediscano l'immediata applicazione delle disposizioni in materia di cancellazione o anonimizzazione dei dati, nonché in materia di registrazione degli accessi e delle operazioni, da fornire entro 6 mesi dall'entrata in vigore dell'emanando d.P.R. e, successivamente, periodiche informative sulla progressiva messa "a regime" dei sistemi informatici da parte del titolare del trattamento.

Va inoltre rilevato che il termine di adeguamento dei sistemi previsto dalla norma, corrispondente a 15 anni a decorrere dalla data di entrata in vigore dell'emanando d.P.R. appare sproporzionato e non in linea con i termini previsti dalla Direttiva (UE) 2016/680 per l'adeguamento dei sistemi di trattamento automatizzato. Si ritiene pertanto che tali tempi vadano allineati rispetto alle previsioni della Direttiva.

Pertanto, i termini vanno ridotti a:

- 5 anni i sistemi di trattamento automatizzato istituiti anteriormente al 6 maggio 2016, quando l'immediato adeguamento alle "comporti sforzi sproporzionati, i sistemi di trattamento automatizzato istituiti anteriormente al 6 maggio 2016"
- 8 anni, per specifici e particolari sistemi, "qualora ciò causi altrimenti gravi difficoltà per il funzionamento di tale particolare sistema di trattamento automatizzato".

In tale ultimo caso, occorre anche soddisfare l'obbligo previsto nella Direttiva, secondo cui " Lo Stato membro in questione comunica alla Commissione i motivi di tali gravi difficoltà e i motivi del termine specificato entro il quale rende tale particolare sistema di trattamento automatizzato conforme all'articolo 25, paragrafo 1. Il termine specificato non supera in ogni caso il 6 maggio 2026".

TUTTO CIO' PREMESSO IL GARANTE:

esprime parere favorevole nei termini di cui in motivazione sullo schema di decreto del Presidente della Repubblica concernente l'individuazione delle modalità attuative dei principi di protezione dei dati personali relativamente ai trattamenti effettuati per finalità di polizia da Organi, Uffici e Comandi di polizia, recante attuazione dell'articolo 57 del Codice, con le condizioni e le osservazioni formulate ai punti da 5.1 a 5.7.

Roma, 2 marzo 2017

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
Busia