Sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici in luoghi pubblici o aperti al pubblico
A.C. 3009

Dossier n° 441 - Progetti di legge
25 maggio 2021

Informazioni sugli atti di riferimento

A.C.	3009
Titolo:	Sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici in luoghi pubblici o aperti al pubblico
Iniziativa:	Parlamentare
Iter al Senato:	No
Date:	
presentazione:	12 aprile 2021
trasmissione alla Camera:	13 aprile 2021
assegnazione:	20 aprile 2021
Commissione competente :	I Affari costituzionali
Sede:	referente
Pareri previsti:	II (ai sensi dell'art. 73 reg. Camera), V, Questioni regionali

La proposta di legge A.C. 3009 prevede la sospensione temporanea dell'utilizzo di sistemi di riconoscimento facciale con uso di dati biometrici nei luoghi pubblici o aperti al pubblico, in considerazione dei rischi per la privacy e per i diritti civili dei cittadini legati all'uso di queste tecnologie ed in attesa di una normativa specifica che disciplini in modo uniforme "i requisiti di ammissibilità, le condizioni e le garanzie relativi all'impiego di sistemi di riconoscimento facciale", sulla base di quanto disposto dal regolamento (UE) 2016/679, dalla direttiva (UE 2016/680) e nel rispetto del principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'UE.

Riconoscimento facciale e dati biometrici: le norme di riferimento

Regolamento UE

L'art. 4, par. 1, n. 14) del Regolamento UE 2016/679 definisce i **dati biometrici** come quei "dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici".

Per questi dati, il Regolamento (art. 9) sancisce in linea generale **il divieto di trattamento**, superabile in presenza, tra gli altri, di uno dei seguenti presupposti:

- il consenso esplicito dell'interessato prestato in relazione a una o più finalità specifiche (lett. a);
- la necessità del trattamento di tali dati per l'assolvimento degli obblighi e l'esercizio dei diritti specifici (del titolare del trattamento o dell'interessato) in materia di **diritto del lavoro**, nella misura in cui il **trattamento** stesso sia **autorizzato "dal diritto degli Stati membri"**, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi del soggetto passivo (lett. b);
- la necessità del **trattamento per motivi di interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (lett. g).

Inoltre, il par. 4 dell'art. 9, prevede che gli Stati membri possano mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati biometrici.

Codice privacy

Nell'ordinamento nazionale, il Codice della privacy (d.lgs. n. 196 del 2003), così come modificato dal d.lgs. n. 108/2018, ha specificato, all'art. 2-sexies, che il trattamento dei dati biometrici può essere legittimato da motivi di interesse pubblico rilevante solo qualora il trattamento sia previsto 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, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Inoltre, fermi i presupposti dell'art. 9 del Regolamento, il Codice detta all'art. 2-septies specifiche misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute, richiedendo il rispetto di **misure di garanzia disposte dal Garante**, ed adottate con un provvedimento a cadenza almeno biennale.

Nell'emanazione delle misure il garante deve tenere conto:

- delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali;
- dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure;
- dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.

Le misure di garanzia possono individuare ulteriori condizioni sulla base delle quali il trattamento di tali dati è consentito, individuano misure di sicurezza (es. tecniche di cifratura e di pseudonomizzazione), misure di minimizzazione e specifiche modalità per l'accesso selettivo ai dati e le misure necessarie a garantire i diritti degli interessati.
Infine, l'art. 2-septies esclude che i dati personali biometrici possano essere diffusi.

Prevenzione e repressione dei reati

Per quanto riguarda in particolare il trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati (in attuazione della direttiva (UE) 2016/680), anche l'art. 7 del d.lgs. n. 51 del 2018 autorizza i trattamento di dati biometrici 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.

I **presupposti di legittimità del trattamento dei dati biometrici** attengono dunque alla sussistenza di una previsione normativa specifica, alla necessità del trattamento per la realizzazione dei legittimi fini perseguiti, nonché al rispetto di garanzie appropriate.

Ultimi provvedimenti del Garante

L'assenza di una una base giuridica idonea a legittimare il trattamento dei dati biometrici è stata più volte evidenziata da **provvedimenti del Garante** (si vedano, tra i più recenti, per quanto riguarda il trattamento di tali dati per finalità di sicurezza pubblica il parere sul sistema Sari Real Time del 25 marzo 2021 e per quanto riguarda il trattamento nell'ambito del rapporto di lavoro l'ordinanza ingiunzione nei confronti di Azienda sanitaria provinciale di Enna del 14 gennaio 2021).

La necessità di una regolamentazione per evitare i grandi rischi per la **privacy e la protezione dei dati** posti dall'utilizzo crescente delle **tecnologie di riconoscimento facciale** è stata di recente proposta dal **Consiglio d'Europa** attraverso una serie di Linee guida adottate il 28 gennaio 2021, che forniscono una serie di misure di riferimento che governi, sviluppatori di sistemi di riconoscimento facciale, produttori, aziende e pubbliche amministrazioni dovrebbero adottare per garantire che l'impiego di queste tecnologie non pregiudichi la dignità della persona, i diritti umani e le libertà fondamentali.

Con la **risoluzione 2020/2013 (INI) del 20 gennaio 2021** relativa a questioni in materia di intelligenza artificiale, il Parlamento europeo ha invitato la Commissione a **valutare le conseguenze di una moratoria** sull'utilizzo dei sistemi di riconoscimento facciale e, in funzione dell'esito di tale valutazione, a prendere in considerazione l'introduzione di una moratoria sull'utilizzo di tali sistemi da parte delle autorità dello Stato nei luoghi pubblici e nei locali destinati all'istruzione e all'assistenza sanitaria, come pure di una moratoria sull'utilizzo dei sistemi di riconoscimento facciale da parte delle autorità di contrasto in spazi semi-pubblici come gli aeroporti, fino a quando le norme tecniche non saranno considerate pienamente conformi ai diritti fondamentali, i risultati ottenuti non saranno privi di distorsioni e di discriminazioni e non vi saranno rigorose garanzie contro gli utilizzi impropri in grado di assicurare la necessità e la proporzionalità dell'utilizzo di tali tecnologie.

Contenuto della proposta di legge

La proposta si compone di due articoli.

L'**articolo 1**, al comma 1, dispone la **sospensione** dell'installazione e dell'utilizzazione, da

parte delle autorità pubbliche o di soggetti privati, di **impianti di videosorveglianza con sistemi di riconoscimento facciale** operanti attraverso l'uso di **dati biometrici** in luoghi pubblici o aperti al pubblico.

La **sospensione** ha efficacia dall'entrata in vigore della legge sino all'entrata in vigore di una disciplina legislativa della materia e, in ogni caso, **non oltre il 31 dicembre 2021**.

Moratoria fino al 31 dicembre 2021

In relazione al campo di applicazione oggettivo della disposizione, due sono gli elementi da considerare.

In primo luogo, come anticipato, deve trattarsi di impianti di videosorveglianza che utilizzino tecnologie di riconoscimento facciale basate su dati biometrici (si v. *supra*).

In secondo luogo vengono in rilievo solo gli impianti che operano in **luoghi pubblici o aperti al pubblico**.

In proposito, si ricorda che ai fini della definizione del carattere pubblico, privato o aperto al pubblico del luogo rileva non la proprietà del luogo stesso, ma l'uso che ne venga fatto. In generale si intende per **luogo pubblico** un luogo che per definizione e natura è accessibile a tutti senza particolari limitazioni e può consistere in un'area, una piazza ovvero una via, un giardino ecc.., mentre l'espressione "**luogo aperto al pubblico"**, individua qualsiasi luogo nel quale l'accesso è consentito a particolari condizioni soltanto dopo l'espletamento di particolari formalità (quali il pagamento di un biglietto di ingresso, l'esibizione di un invito, l'obbligo di iscrizione ad un'associazione che lo gestisca, ecc.).

Ai fini della proposta, non rileva invece che l'installazione o l'utilizzazione di tali sistemi siano svolte da **un'autorità pubblica o** da **un soggetto privato**.

Dalla sospensione sono esclusi, come esplicitato dal **comma 2**, i sistemi di videosorveglianza che non presentano le caratteristiche di cui al comma 1 e che siano conformi alla normativa vigente. Pertanto sembrerebbero **non rientrare** nel campo di applicazione della proposta:

- gli impianti di videosorveglianza privi di un sistema di riconoscimento facciale;
- gli impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici, installati e utilizzati in luoghi privati.

Norme che autorizzano regimi di videosorveglianza

Sono molteplici e con differenti ambiti e finalità le norme previste nell'ordinamento che consentono ad autorità pubbliche e soggetti privati l'installazione di sistemi di videosorveglianza.
Uno dei settori che negli ultimi anni ha registrato una crescita rilevante è il ricorso alla **videosorveglianza da parte degli enti locali** per rispondere alla domanda di sicurezza urbana. Si ricorda, in proposito, che il decreto legge n. 11 del 2009 (art. 6, commi 7 e 8) ha autorizzato i comuni, ai fini della **tutela della sicurezza urbana**, ad impiegare sistemi di videosorveglianza nei luoghi pubblici o aperti al pubblico, mentre prima tali finalità non erano perseguibili in quanto di competenza delle autorità di polizia. In questo caso la norma prevede che i dati raccolti mediante tali sistemi possono essere conservati sino al settimo giorno successivo alla loro rilevazione, salvo particolari esigenze di ulteriore conservazione.
Il potenziamento e l'installazione dei sistemi di videosorveglianza è uno degli strumenti da utilizzare nell'ambito dei patti per la sicurezza urbana a fini di prevenzione della criminalità diffusa e predatoria (si cfr. D.L. n. 14 del 2017, articolo 5, comma 2, lett. a)). La relativa attività di installazione e di esercizio dei sistemi di videosorveglianza da parte degli enti locali è considerata attività libera e non soggetta ad autorizzazione generale (art. 38, co. 3, D.L. n. 76 del 2020).

In relazione allo svolgimento di **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 repressione dei reati, l'articolo 22 del DPR 15 gennaio 2018, n. 15 consente l'utilizzo di sistemi di videosorveglianza ove necessario e a condizione che non comporti un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali delle persone interessate.
Alcuni provvedimenti recano disposizioni relative alla videosorveglianza in specifici luoghi aperti al pubblico: tra queste si ricorda in particolare, per la sua incidenza sulla tutela della sicurezza, l'art. 1-*quater*, comma 3, del decreto-legge 28/2003, con cui si dispone che gli impianti sportivi di capienza superiore alle 7.500 unità utilizzati per lo svolgimento di partite di calcio devono essere dotati di strumenti di videosorveglianza delle aree riservate al pubblico sia all'interno dell'impianto, sia nelle sue immediate vicinanze.

Per quanto riguarda l'uso dei sistemi di videosorveglianza **in ambito lavorativo**, l'articolo 4 della legge n. 300/1970 (cd. Statuto dei lavoratori), come modificato dall'articolo 23, comma 1, del D.Lgs. 151/2015, pone alcuni limiti all'**utilizzo degli impianti audiovisivi** e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori. Tali impianti e

strumenti, in particolare, possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla R.S.U. o dalle R.S.A. (nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale). In mancanza di accordo, i richiamati impianti e strumenti possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa (nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali) della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti presi in mancanza di accordo sindacale sono da considerarsi definitivi.

Nell'ambito delle **amministrazioni pubbliche**, i commi da 1 a 4 dell'articolo 2 della L. 56/2019 (c.d. legge concretezza) hanno previsto l'introduzione di sistemi di **verifica biometrica dell'identità e di videosorveglianza degli accessi per i dipendenti,** ai fini della verifica dell'osservanza dell'orario di lavoro. Dall'ambito di applicazione dei suddetti sistemi le citate disposizioni hanno escluso il personale in regime di diritto pubblico, i dipendenti titolari di un rapporto agile, nonché il personale degli istituti scolastici ed educativi e i dirigenti scolastici, mentre sono inclusi i dirigenti, fatta salva la summenzionata esclusione per le categorie in regime di diritto pubblico. Tale previsione è stata successivamente abrogata ad opera della legge di bilancio 2021 (art. 1, comma 958, legge n. 178 del 2020).

Si ricorda, infine, che nella legislatura in corso la Camera ha approvato una proposta di legge di iniziativa parlamentare volta a prevenire e contrastare condotte di maltrattamento e abuso in danno di minori, anziani e persone con disabilità, che a tal fine prevede la possibilità, **nei servizi educativi per l'infanzia, nelle scuole dell'infanzia e nelle strutture socio-sanitarie e socio-assistenziali** per anziani e persone con disabilità, a carattere residenziale, semi-residenziale o diurno, di installare sistemi di videosorveglianza a circuito chiuso. Il provvedimento è in corso di esame al Senato (A.S. 897). Nelle more dell'esame del provvedimento, il Parlamento, in sede di conversione del D.L. 32 del 2019 (art. 5-*septies*) ha previsto uno stanziamento per l'istallazione di sistemi di videosorveglianza presso le aule dei servizi educativi per l'infanzia e nelle scuole dell'infanzia statali e paritarie, nonchè nelle strutture socio-sanitarie e socio-assistenziali.

Sanzioni amministrative

L'**articolo 2** stabilisce che, in caso di violazione delle prescrizioni di cui all'articolo 1, salvo che il fatto costituisca reato, si applicano **sanzioni amministrative pecuniarie.**

In particolare, per quanto riguarda i trattamenti realizzati da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati (D.Lgs. n. 51 del 2018), si applica la sanzione amministrativa del pagamento di una somma da 50.000 a 150.000 euro (art. 42, comma 1); per tutti gli altri trattamenti operati in violazione della moratoria si applica invece una sanzione amministrativa pecuniaria fino a 10 milioni di euro, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 166, comma 1, Codice della privacy, che rinvia all'art. 83, par. 4, del Regolamento).

Relazioni allegate o richieste

La proposta di legge in commento, di iniziativa parlamentare, è corredata della relazione illustrativa.

Rispetto delle competenze legislative costituzionalmente definite

In generale l'installazione di impianti di videosorveglianza per finalità di sicurezza appare riconducibile alle materia «***ordine pubblico e sicurezza»,*** rimessa alla competenza legislativa esclusiva dello Stato, anche con riguardo alle possibili forme di coordinamento con le Regioni (artt. 117, secondo comma, lettera h), e 118, terzo comma, Cost.); si veda, in questo senso, la sentenza della Corte costituzionale n. 63 del 2016.

Viene altresì in rilievo la protezione dei dati personali, che è materia riservata alla potestà legislativa esclusiva dello Stato, in quanto riconducibile alla materia dell'«**ordinamento civile**» di cui all'articolo 117, comma secondo, lettera l), della Costituzione, come sancito dalla sentenza 271/2005 della Corte costituzionale, con profili di rilevanza anche, ex 117, primo comma, in termini di compatibilità con il diritto dell'UE.