Videosorveglianza: il quadro normativo in Italia (parte I)

Author : Giovanni Villarosa

Date : 5 Novembre 2019

Nell'anno accademico 2016-2017 ho frequentato, presso il dipartimento di **Giurisprudenza dell'Università di Roma Tre**, il master di II livello per **"Responsabile della protezione dei dati personali: *data protection officer* e *privacy expert*";** un corso di formazione specialistica multi-settoriale patrocinato dall'Autorità Garante per la protezione dei dati personali, dove si è approfondito il mutato quadro generale nella protezione dei dati personali, tanto in ambito pubblico quanto in quello privato, alla luce del nuovo **Regolamento europeo GDPR 2016/679.**

La parte conclusiva del master prevedeva la discussione di un elaborato che prendesse in considerazione, integrandoli, diversi insegnamenti qualificanti del corso. Il mio lavoro di tesi ha tentato di analizzare una problematica oggi molto sentita: ***l'impatto privacy dei sistemi di videosorveglianza nelle attività di pubblica sicurezza, sicurezza urbana, sicurezza privata,*** argomento studiato minuziosamente sotto la fondamentale guida della relatrice dott.ssa Ferola, funzionaria dell'Autorità Garante, dal risultato decisamente interessante, discusso poi nella commissione presieduta dalla Prof.ssa Califano, componente del collegio del Garante.

Sappiamo, ad esempio, come all'interno della cd. società *tecnocratica* determinate scelte politiche vengano prese anche utilizzando la *sommatoria* di analisi provenienti da esperti qualificati, da strumenti scientifici e da tecnologie che *acquisiscono ed elaborano* dati personali. Ebbene, la **videosorveglianza** è una tematica che influenza fortemente certi indirizzi politici, perché rappresenta due componenti fondamentali di certe scelte, per qualità e quantità: una componente fa capo alle *politiche sociali* sulla sicurezza urbana e controllo del territorio, mentre l'altra tenta di realizzare, nel concreto, *la fusione* tra le *smart city* e le *smart technology*.

Il mio breve lavoro di ricerca ha messo in risalto come la richiesta da parte degli enti locali per il controllo del territorio, del traffico e la sicurezza dei cittadini, mediante l'utilizzo dei sistemi di videosorveglianza, sia cresciuta considerevolmente nel nostro Paese proprio negli ultimi venti anni; difatti, già nella newsletter del 28 febbraio 2000, il Garante espliciterà la necessità, per le amministrazioni interessate, *di adeguare la ripresa delle immagini alle norme sulla privacy adottando le necessarie cautele -già sancite dal DPR n.318/1999 Privacy misure minime di sicurezza-, quali informare gli interessati, limitare la possibilità di ingrandimento delle immagini e*

il livello di dettaglio sui tratti somatici.

In buona sostanza l'Autorità ribadisce come *il cittadino interessato al trattamento*, debba sempre essere informato quando si trovi *oggetto di un trattamento dati*, dunque in prossimità di aree *video controllate*: l'amministrazione dovrà farlo attraverso l'affissione di appositi cartelli/avvisi, ma soprattutto, dovrà rispettare il *principio di non eccedenza* dei dati raccolti in relazione agli *scopi perseguiti*.

Ho scritto più volte sui sistemi di videosorveglianza, pubblica o privata, e sul perché costituiscono *uno dei sistemi di sicurezza fisica più innovativi* utilizzati in questi ultimi anni; abbinati alla registrazione, alla visione *live o real time* da remoto, diventano un'interessante quanto importante fonte di dati personali e informazioni (metadati) utili per le *analisi di sicurezza (safety e security), investigative e di intelligence*.

Rileggendo oggi il mio elaborato e trovandoci a due anni di distanza, ma soprattutto a vent'anni dalla *nascita definitiva* del videocontrollo – fino a quel momento praticamente e tecnicamente in uno stato embrionale -, possiamo *ragionevolmente* considerare l'anno 2019 quale primo *step temporale*, *il primo gradino di una scala di riferimento* necessario per **misurare l'impatto** che i sistemi di videosorveglianza hanno prodotto, in questo intervallo, sulla sfera privacy e nell'ambito del trattamento dei dati personali.

Venti anni di evoluzione tecnologica e normativa credo che rappresentino *la pietra miliare* del settore; un arco temporale che impone oggi una riflessione attenta sulla reale efficacia del binomio *sicurezza=tecnologie* e sull'impatto creato nella società, giacché i *device* tecnologici sono diventati ormai una *centralità quotidiana* dei giuristi, chiamati costantemente a formulare risposte tangibili ai quesiti posti sul rischio del ***trattamento dati con dispositivi elettronici*** per l'acquisizione e registrazione dei file video, perché le attività di **sorveglianza elettronica** rappresentano realmente un trattamento di dati personali, operazioni che vanno condotte sempre con le dovute garanzie.

Peraltro, *deontologia e buona condotta* ce la ricordava l'**art. 134** del **Codice della Privacy** (**D.Lgs 196/2003 novellato dal D.Lgs 101/2018**), definendo la videosorveglianza come ***il trattamento effettuato con strumenti elettronici di rilevamento immagini***.

Appare chiaro fin qui come la videosorveglianza, dal punto di vista normativo, sia un'attività *licitus*; una legittimità confermata anche in ambito **penale**, estrapolandola *a contrario* proprio dal codice penale, che all'**art. 615 bis** punisce *l'indebita acquisizione d'immagini mediante l'uso di strumenti di ripresa visiva nell'abitazione altrui o in altro luogo di privata dimora*; da qui l'ovvia *estrapolazione*, che ***la videosorveglianza è consentita in luogo pubblico o aperto al pubblico***.

Orbene, nel marzo 1999 l'Autorità garante guidata dal Prof. Rodotà, all'interno di una sua newsletter, affrontava il tema del trattamento dati per mezzo di strumenti elettronici in ambito videosorveglianza pubblica, pronunciandosi così: "*La videosorveglianza è un tema di grande rilievo e interesse per l'opinione pubblica: non esiste ancora una normativa specifica in materia, ma la legge sulla privacy, nel recepire i principi sanciti in sede europea, definisce dato*

personale qualsiasi informazione che permette l'identificazione della persona compresi i suoni e le immagini.
Anche una semplice installazione di videocamera, o una registrazione sonora per esempio, deve essere conforme alle disposizioni sulla privacy: a quale tipo di funzione o per quale finalità viene realizzata, la sicurezza e la conservazione delle immagini e delle riproduzioni, l'uso appropriato rispetto alla finalità, l'informazione agli interessati.
L'Autorità ha avviato in collaborazione con il Dipartimento di Sociologia dell'Università di Roma "La Sapienza" un'indagine sulle diverse forme di videosorveglianza, che ne monitorizzi l'uso valutandone anche l'impatto sociale.
L'utilizzo delle telecamere si sta sempre più diffondendo a scopi di sicurezza sociale, di accesso ai centri storici, di controllo in luoghi pubblici, esercizi commerciali, o di vigilanza all'interno delle strutture sanitarie per un'assistenza continua ai pazienti.
Per quest'ultimo caso, trattandosi di dati sensibili relativi a persone che necessitano di cure e controlli, rientra nelle finalità degli organismi sanitari raccogliere informazioni anche in modo non tradizionale e sempre nel contesto delle regole di base in materia: informazione agli interessati e individuazione del personale autorizzato in esclusiva all'uso dei dati, che devono essere strettamente necessari e conservati per un periodo determinato".

Una *riflessione* interessante a supporto dei potenziali rischi che tali sistemi generano per la privacy e che poggia le sue fondamenta sulla fattiva collaborazione del dipartimento di Sociologia della Sapienza, che analizzando le diverse forme di videosorveglianza ne misurerà contemporaneamente l'impatto sociale, determinando così un approccio nei confronti della tematica di studio impostato ***ab origine**,* e in modalità non esclusivamente *giuridica,* ma con una particolare considerazione sulle potenziali ricadute *sociali*.

Un Garante illuminato che ben capì, sin da subito, come le dimensioni assunte dal fenomeno - sommate e/o sottratte alle sue positive e/o negative potenzialità - di lì a pochi anni si trasformasse da mero strumento *tecnico* a vera *arma sociale*: *l'illusione che la talcosa tecnologica fosse **la risoluzione di tutti i mali**, e dai poteri taumaturgici!*

Ma comprese ancor meglio un altro aspetto importante della questione, sul come questa tecnologia, sommata ad un utilizzo sconsiderato, potesse andare ben oltre il solo ambito giuridico, ingenerando allarmanti problematiche sociali con ricadute negative in termini di costi e impatto sulla sfera privacy.

Un'analisi perfetta che lo spingerà successivamente, nel **quinquennio 1999/2004**, a regolamentare il settore con diversi atti di indirizzo ben specifici.

Una sorta di *anno zero* nell'ambito del trattamento dei *dati video*, che dimostrerà nel contempo due cose: una, l'attenzione da parte dell'istituzione al crescente fenomeno degli impianti di videocontrollo, del loro impatto privacy e soprattutto le vulnerabilità che questo processo di acquisizione dati comporterà; l'altra, invece, equivale ad uno *Zero-Day* - passatemi il forzato concetto - che tali sistemi rappresenteranno per il Titolare del trattamento e lo stesso Garante che, sollecitato negli anni a continui richiami in materia, adotterà nel novembre 2000 un ***Decalogo delle regole per non violare la privacy,*** documento in dieci punti contenente adempimenti, garanzie e tutele in merito, che va letto alla luce delle numerose note inviate -

soprattutto dagli enti pubblici - all'Autorità per l'accertamento della *conformità* degli impianti alle disposizione normative contenute all'interno della **Legge n° 675/1996** (legge di recepimento della direttiva 95/46/CE, cd. direttiva madre).

Ci troviamo di fronte a un decalogo innovativo, senza eguali nel resto dell'unione, antesignano del primo vero e proprio ***Provvedimento generale sulla videosorveglianza*** – pubblicato poi nell'aprile 2004 -, *illuminante* per le considerazioni generali sul tema, contenente una disciplina più compiuta ed organica che conforma, sostanzialmente, i trattamenti dei dati personali al nuovo **D.Lgs n° 196/2003** (***Codice in materia di protezione dei dati personali*****,** cd. **CdP**) entrato nel frattempo in vigore il 1 gennaio 2004.

Nei prossimi articoli approfondiremo le dimensioni applicative della normativa esaminata e i conseguenti profili di criticità.

Articolo a cura di **Giovanni Villarosa**