Videosorveglianza: dimensione applicativa, criticità emergenti e cautele necessarie (parte I)

Author : Giovanni Villarosa

Date : 27 Novembre 2019

Abbiamo analizzato nei precedenti articoli come i sistemi di videosorveglianza rappresentino una tra le *misure di sicurezza* – pubblica e privata - e *controllo* tra le più usate; ne è testimonianza, ad esempio, *l'accento* posto sull'uso di tali sistemi all'interno dei *Protocolli e Patti per la sicurezza urbana.*

Abbiamo osservato come venti anni fa la visibilità delle forze dell'ordine fosse considerata *centrale,* da parte dei cittadini, e come oggi i nuovi strumenti elettronici messi a disposizione dalle nuove tecnologie, invece, ci permettano di attuare servizi di sicurezza, osservazione e prevenzione esercitando *un controllo di polizia tecnologicamente a distanza*, piuttosto che *fisicamente* in presenza.

L'esponenziale crescita della videosorveglianza permette oggi alle istituzioni preposte alla *sicurezza pubblica* un monitoraggio *puntuale* del luogo del disordine, o del reato, tenendo costantemente sotto controllo la situazione, pur non essendo presenti *umanamente*.

Di contro però, **non c'è stato l'effetto deterrente sperato**, o il risultato più atteso, motivo per cui erano stati inizialmente pensati tali sistemi; infatti il lavoro di tesi ha messo in risalto, piuttosto, come tali sistemi di *raccolta dati* si siano rivelati molto più *determinanti nelle analisi investigative post evento* (riconoscimenti dei responsabili a posteriori, ricostruzione temporale dei fatti delittuosi o di pericolo, etc), anziché come vero e proprio *strumento tipicamente preventivo*.

Si è analizzato come la sfera della riservatezza individuale, i dati personali trattati di ogni singolo cittadino, possano essere compromessi *dall'invasività* creata dalle innovative tecnologie video, dagli usi non conformi utilizzati nelle attività di sicurezza, che si sono dimostrati di forte e negativo impatto della sfera privacy.

Analisi condotta partendo dai *principi cardini* della materia: **la privacy *by design* e *by default*, il *privacy impact assessment*, l'*accountability*, l'analisi dei rischi,** tutti assiomi introdotti dal

nuovo **Regolamento UE 2016/679** a protezione del corretto, e non eccedente, trattamento dei dati personali.

Un Regolamento che prevede specifiche prescrizioni, a differenza della **Direttiva 95/46/CE** (cd "direttiva madre"), circa le modalità di analisi del rischio ed il ruolo assunto sia dal titolare del trattamento dei dati che dalle autorità di controllo preposte, e a fronte di tale progresso normativo, ci siamo chiesti: ma tutto questo sarà sufficiente?

È davvero soddisfacente una trasformazione prescrittiva per rendere un Regolamento (presente già nel perimetro concettuale delineato all'interno della direttiva, ovvero, centralità dell'interessato, principio di finalità, minimizzazione, etc) conforme a rispondere alle nuove minacce, ai rischi posti in gioco dal nuovo modello di trattamento dati per mezzo di sistemi video basati su performanti algoritmi matematici, sviluppati nei software di analisi video?

Quello che è sembrato mancare, come *garanzia*, sono gli specifici strumenti per valutare e tenere in debita considerazione le possibili conseguenze *etiche, sociali* sui modelli di trattamento e sulla tutela dei dati.

L'approccio basato sulla prevenzione del *rischio,* scelto dal legislatore nel nuovo Regolamento, appare decisamente distante dall'idea di una valutazione molteplice dei rischi correlati nell'uso dei *dati video* raccolti dai sistemi di videosorveglianza.

Un timido supporto normativo, in tal senso, lo si può ritrovare all'interno del **considerando 75**, dove tra i tanti, viene riconosciuto che *i rischi per i diritti e le libertà delle persone fisiche possono anche consistere in danni fisici… effetti discriminatori… o di danno sociale significativo;* linearmente ai principi tipici dell'analisi dei rischi, secondo il **considerando 84**, l'obbligo di adottare misure atte a mitigare il rischio è sempre valutato alla luce della *tecnologia disponibile* e dei *costi di attuazione*.

Ma tali parametri, presenti anche nelle disposizioni in materia di sicurezza (art. 32 e considerando 83) e *data protection by design* (art. 25 e considerandi 75-78), costituiscono un elemento importante per attuare il **principio di proporzionalità** nell'insieme della gestione del rischio, e sulle misure di protezione da adottare alla luce del nuovo Regolamento, che supererà l'inadeguatezza di un modello di a*nalisi obsoleto* alle nuove tecnologie e tipologie di minaccia, contenuto nell'**allegato B** del Codice.

Nella seconda parte del lavoro è stato approfondito come nel campo della sicurezza, pubblica e privata, nella sfera della protezione privacy, il fenomeno sociale ed etico della videosorveglianza rappresenti due tendenze contrastanti tra loro: la tendenza della sicurezza "ad ogni costo", contro quella della riservatezza personale "nonostante tutto", analizzando come si sia passati da tecnologie (hardware e software) tipicamente *analogiche*, limitate tecnicamente a registrare **tutto e comunque**, a tecnologie *digitali* con la capacità di *apprendere* (hardware) secondo metodi *deduttivi* (software), e una potenzialità di acquisizione dei dati mediante il principio del ***solo quelli necessari*.**

Ora, a latere di un *interesse di carattere generale*, come viene definita la pubblica sicurezza e la

sicurezza urbana, ne resiste uno diverso, contrapposto e fondamentale: *la riservatezza delle persone*, declinata, come si è analizzato, in diverse forme, che vanno dal diritto alla privacy, alla tutela dei dati personali del privato cittadino.

L'obiettivo perseguito dai sistemi di videosorveglianza (installati da soggetti pubblici o privati) è quello del contenimento dei fenomeni criminali, sia mediante l'azione *repressiva* (individuazione degli autori dei reati) sia *preventiva* (effetto deterrenza): la teoria sociologica delle cd ***opportunità criminali*** rappresenta proprio la finalità della deterrenza, secondo cui l'azione criminale può essere prevenuta riducendo l'opportunità di delinquere.

È proprio la necessità di equilibrare queste tendenza tipica della videosorveglianza, quella di far convivere le necessità di sicurezza, da una parte, e la tutela dei diritti degli interessati dall'altra, che obbligò il Garante a disciplinare la materia pubblicando, a partire dal 2000, ben tre diversi decaloghi/provvedimenti generali (anni 2000, 2004, 2010) di settore - più tutta una serie documentale prescrittiva, specifica e complementare - che esamineremo, a conclusione di questa panoramica, in un successivo articolo.

Articolo a cura di **Giovanni Villarosa**