UNIONE POLIZIA LOCALE ITALIANA
Articolo disponibile all'indirizzo: www.unionepolizialocaleitaliana.it/2020-57/

VIDEOSORVEGLIANZA, FOTOTRAPPOLE E OBBLIGO DI VALUTAZIONE D'IMPATTO

di Massimiliano Mancini[1]

ABSTRACT: *La videosorveglianza e le fototrappole si stanno diffondendo ovunque, nei piccoli comuni come nelle città metropolitane, eppure esse sono tra le attività specificatamente soggette all'obbligo della preventiva redazione della valutazione d'impatto o DPIA(Data Privacy Impact Assessment). Tuttavia in molti casi questo obbligo è assolto in maniera meramente formale o addirittura omesso nonostante sia punito, senza alcun trattamento di favore per gli enti pubblici, con sanzioni sino a 10 milioni di euro, importi in grado di determinare il dissesto.*

KEYWORDS: #privacy #GDPR #valutazionedimpatto #dpia #pia #trattamentodatipersonali #DPO #DataProtectionOfficer #RPD #responsabileprotezionedati #PoliziaGiudiziaria #PoliziaAmministrativa #MassimilianoMancini #EspertiUPLI #UPLI #UnionePoliziaLocaleItaliana

INDICE

PREMESSA

In Italia si registra una scarsa sensibilità alle tematiche della privacy anche e soprattutto in ambito pubblico e ciò è ancor più grave poiché gli enti territoriali sono il simbolo concreto della legalità dello Stato e poi, su un piano più pragmatico, le sanzioni, che colpiscono allo stesso modo e senza differenze gli enti pubblici e le aziende private, sono così elevate da mandare facilmente in dissesto molte amministrazioni.

La videosorveglianza pubblica, ad esempio, è in forte espansione su tutti i territori, dai comuni più piccoli alle città metropolitane, ed è uno dei casi tipici per i quali la normativa sovranazionale del Regolamento Europeo 2016/679, noto con l'acronimo GDPR (General Data Protection Regulation), prescrive senza eccezioni la necessità di una valutazione d'impatto.

Eppure molte amministrazioni affidano la redazione a soggetti privi di competenza, convinti che sia sufficiente rispettare l'obbligo solo su un piano formale, oppure addirittura omettono del tutto la valutazione d'impatto, convinti che nessuno agirà contro gli Enti pubblici o che comunque le sanzioni in fondo siano trascurabili.

---

[1] *Segretario Generale UPLI, già comandante dirigente di Polizia Locale e Provinciale, consulente privacy per enti pubblici (Mancini Privacy Firm) e DPO.*

Tutto ciò è dimostrazione di come sia ancora diffusamente poco conosciuta la rivoluzione introdotta in tutt'Europa con il GDPR e del suo valore di norma sovraordinata all'intero ordinamento nazionale e che quindi nessun organo, nemmeno il parlamento, può derogare o modificare in alcun modo.

L'inosservanza degli obblighi concernenti la DPIA può comportare anche per gli Enti Pubblici l'imposizione di sanzioni pecuniarie da parte delle Autorità garanti elevatissime.

Il mancato svolgimento dell'analisi nei casi il trattamento è soggetto alla valutazione d'impatto, lo svolgimento non corretto o la mancata consultazione dell'Autorità di controllo competente ove ciò sia necessario, possono comportare l'applicazione di una sanzione amministrativa fino a un massimo di 10 milioni di euro.

LA VALUTAZIONE D'IMPATTO

La valutazione d'impatto è una procedura, nota anche con l'acronimo DPIA (Data Protection Impact Assessment) o PIA (Privacy Impact Assessment), come si indicherà nel seguito, è prevista dall'articolo 35 del Regolamento UE/2016/679 (GDPR) e ha lo scopo di descrivere un trattamento di dati per valutarne la necessità e la proporzionalità così come tutti gli altri principi fondamentali del GDPR.

Il processo di PIA può riguardare un singolo trattamento anche più trattamenti che presentino analogie per natura, ambito, finalità e rischi[a].

Dalla descrizione del trattamento ne consegue la valutazione e quindi la predisposizione di idonee misure per affrontarlo.

La PIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare a rispettare le prescrizioni normative ma attesta anche di aver adottato idonee misure per garantirne il rispetto.

OBBLIGO DELLA PIA

Il PIA (Privacy Impact Assessment) è obbligatorio in tutti i casi previsti dall'articolo 35 comma 1 del EUE 2016/679 GDPR[b] ossia quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche e questo può avvenire per varie ragioni:

- per l'implementazione di nuove tecnologie;
- a causa della natura, dell'oggetto, del contesto o delle finalità del trattamento.

Lo stesso articolo 35 del Reg.UE 2016/679 GDPR al comma 3[c] cita anche alcune ipotesi specifiche che rendono sempre obbligatoria la PIA che sono:

---

[a] Regolamento UE/2016/679 GDPR, articolo 35 (Valutazione d'impatto sulla protezione dei dati) c.1 "*…Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi…".*

[b] Reg.UE/2016/679 GDPR, art.35 c.1 (Valutazione d'impatto sulla protezione dei dati) "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, …".*

[c] Reg.UE/2016/679 GDPR, art.35 c.3 "*La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo*

- la valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche (art.35 c.3 p.a GDPR);
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10 (art.35 c.3 p.b GDPR);
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (art.35 c.3 p.c GDPR).

GLI ULTERIORI OBBLIGHI INTRODOTTI DAL GARANTE PER LA PRIVACY

Il GDPR ha previsto espressamente che l'autorità nazionale di controllo ha il potere e la facoltà di prevedere delle specifiche tipologie di trattamento per i quali è obbligatoria l'adozione del PIA (art.35 c.4 GDPR)[d], in questi casi ha l'obbligo di pubblicare il provvedimento e comunicarlo al comitato europeo per la protezione dei dati (art.35 c.6 GDPR)[e] che era Gruppo di lavoro art.29 o Working Party article 29 (noto anche con l'acronimo WP29), fino al 25 maggio del 2018 (data di entrata in vigore del RGPD) e aveva lo scopo di occuparsi di questioni relative alla protezione della vita privata e dei dati personali, ed è stato sostituito in seguito dal Comitato europeo per la protezione dei dati (art.68 GDPR).

Per specificare nel dettaglio e dare maggiore certezza è intervenuto il provvedimento del Garante per la Protezione dei Dati Personali che con la delibera 11 ottobre 2018, n.467 "*Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati, ai sensi dell'articolo 35, comma 4, del regolamento (UE) n. 2016/679*", che ha attuato le indicazioni del Working Party article 29 del 2017 fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018.

In questo modo si è stabilito l'obbligo di PIA nei casi in cui ricorrano almeno due di questi criteri anche se il titolare può deciderla anche quando ne ricorra uno solo in funzione delle implicazioni sulla sicurezza:

- trattamenti valutativi o di scoring, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es. assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es. videosorveglianza);

---

significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.".

[d] Reg.UE/2016/679 GDPR, art.35 c.4 "*L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.".*

[e] Reg.UE/2016/679 GDPR, art.35 c.6 "*Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.".*

- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es. informazioni sulle opinioni politiche);
- trattamento di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per differenti finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene ad esempio con i big data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es. riconoscimento facciale, devices Internet of Things, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es. screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

CASI DI ESCLUSIONE DELL'OBBLIGO DI PIA

Lo stesso articolo 35 del Reg.UE 2016/679 GDPR al punto 10[f] stabilisce che il PIA è esclusa quando si verificano contemporaneamente le seguenti condizioni:

1. Finalità del trattamento di interesse pubblico e specificatamente in uno dei seguenti casi:
   a. per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
   b. per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

2. Disciplina normativa esplicita della finalità di interesse pubblico contenuta in un atto normativo Europeo o dello Stato membro al quale il titolare del trattamento è soggetto.

3. Sia già stata eseguita una PIA nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione della disciplina giuridica di cui al punto precedente.

Il Garante per la Protezione dei Dati Personali, secondo quanto previsto dal Regolamento Europeo (art.35 c.5 GDPR)[g], ha stabilito che il PIA non è necessario per i trattamenti che:

- non presentano rischio elevato per i diritti e le libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata svolta una PIA;
- sono stati già sottoposti a verifica da parte di un'autorità di controllo prima del maggio 2018 e le cui condizioni (es. oggetto, finalità, ecc.) non hanno subito modifiche;

---

[f] Reg.UE/2016/679 GDPR, art.35 c.10 "*Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.*".

[g] Reg.UE/2016/679 GDPR, art.35 c.5 "*L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.*".

- sono compresi nell'elenco facoltativo del trattamento per i quali non è necessaria provvedere alla PIA;
- fanno riferimento a norme o regolamenti, Ue o di uno Stato membro, per la cui definizione è stata condotta una PIA.

CHI DEVE SVOLGERE LA PIA

Il titolare del trattamento ha la responsabilità di valutare la necessità del Privacy Impact Assessment (art.35 c.2 GDPR)[h] e, laddove si renda necessaria, l'obbligo di provvedere alla realizzazione sovrintendendo sempre ogni fase pur se la realizzazione materia sia demandata ad altro soggetto (consulente esterno o dipendente).

Nella decisione sulla realizzazione e nello svolgimento si consulta con il DPO/RDP (Data protection officer/Responsabile per la protezione dei dati) inoltre, se il trattamento lo richiede, può acquisire pareri di esperti, tecnici e in particolare del responsabile della sicurezza dei sistemi informativi (noto anche come Chief Information Security Officer, acronimo CISO) e del responsabile IT (acronimo di Information Technology), laddove presenti, da allegare alla PIA.

Se lo ritiene necessario, il titolare può acquisire anche il parere degli interessati o dei loro rappresentanti purché ciò non pregiudichi gli interessi commerciali o pubblici dell'azienda o ente che procede e purché non si mettano a rischio i trattamenti stessi che si vogliono valutare con la PIA (art.35 c.9 GDPR)[i].

AGGIORNAMENTO DEL PIA

Il PIA non è un documento statico ma proprio per le sue finalità generali richiede un processo costante di verifica ed eventuale aggiornamento perlomeno quando insorgono variazioni del rischio, secondo il contesto e le evoluzioni tecnologiche, ovvero mutino o si evolvano le attività relative al trattamento.

In questi casi il titolare del trattamento procede a un riesame per valutare se dalle variazioni delle procedure del trattamento che sono intervenute e/o dalle mutate condizioni del contesto ne scaturisca un pregiudizio, anche solo potenziale, sulla sicurezza del trattamento dei dati personali e se le previsioni contenute nel PIA siano ancora valide e attuali (art.35 c.11 GDPR)[j].

---

[h] Reg.UE/2016/679 GDPR, art.35 c.2 "*Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.*".

[i] Reg.UUE/2016/679 GDPR, art.35 c.9 "*Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.*".

[j] Reg.UE/2016/679 GDPR, art.35 c.11 "*Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.*".

SONO ESCLUSE LE FOTOTRAPPOLE?

In via generale il GDPR esclude le attività effettuate a fini di prevenzione indagine accertamento o perseguimento di reati o esecuzione di sanzioni penali, che concretamente sono le attività di polizia giudiziaria e di esecuzione di provvedimenti penali (GDPR art.1 c.2)[k].

Quindi se le fototrappole o in via generale i sistemi di videosorveglianza sono impiegati in indagini penali non vi è alcun bisogno della PIA, tuttavia deve esserci preventivamente un fascicolo di indagine aperto.

Viceversa tutte le informazioni acquisite in violazione degli obblighi della PIA rappresentano una violazione di legge e quindi un vizio del processo sanzionatorio insanabile, ad esempio laddove le fototrappole fossero utilizzate per contrastare le violazioni ambientali punite con sanzioni amministrative, e inoltre impongono all'autorità che ne abbia conoscenza, come ad esempio il sindaco, il presidente della provincia, il Giudice di Pace che sia chiamato a decidere del ricorso, a segnalare la violazione al Garante per la Privacy per l'applicazione della sanzione, facoltà che ha anche qualsiasi privato.

[k] Regolamento UE 2016/679 art.1 c.2: « 2. Il presente regolamento non si applica ai trattamenti di dati personali: a) effettuati per autorità che non rientrano nell'ambito di applicazione del diritto dell'Unione; b) effettuati dagli Stati membri nell'esercizio di autorità che rientrano nell'ambito di applicazione del titolo V capo 2 TUE; c) effettuati da una persona fisica per l'esercizio di autorità a carattere esclusivamente personale o domestico; d) effettuati dalle autorità competenti a fini di prevenzione indagine accertamento o perseguimento di reati o esecuzione di sanzioni penali incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.»