



I.s.e.c. Srl

Taggia, li 13 dicembre 2022

Spett.le Ente  
Per C.C. Spett.le RPCT

**IL GARANTE INTERVIENE IN MERITO AI SISTEMI DI VIDEOSORVEGLIANZA NON CONFORMI ALLA NORMATIVA IN TEMA DI PROTEZIONE DATI PERSONALI**

La videosorveglianza rappresenta uno dei trattamenti più invasivi che un ente pubblico possa fare nei confronti della raccolta di dati personali di potenziali soggetti ripresi, i cosiddetti "interessati".

Si può comprendere quindi come il Garante sia sempre più attento nel segnalarci che l'installazione e l'utilizzo di tali sistemi, ove non corretti sia dal punto di vista della finalità che dal punto di vista della mancanza di idonea documentazione a riguardo, può portare a gravi conseguenze per i diritti e le libertà dei soggetti interessati. L'invasività dei sistemi di videosorveglianza dipende, tra l'altro, anche dal posizionamento delle telecamere e dalla qualità delle immagini.

Queste prime considerazioni generali, non esaustive senz'altro come analisi, dovrebbero essere fatte SEMPRE a monte, cioè in anticipo rispetto al posizionamento stesso delle telecamere. Una ulteriore analisi da sviluppare deve riguardare il rispetto del principio di necessità, che richiede, ad esempio, di non eccedere nelle riprese, definendo con accortezza le inquadrature in base alla corretta individuazione delle aree di pertinenza che si ritiene utile sorvegliare.

Queste analisi dovrebbero essere ricomprese e affrontate in una corretta valutazione d'impatto dei trattamenti sui dati personali, definita **DPIA** dalla normativa, da farsi, come si è sopra accennato, PRIMA dell'avvio di una qualsivoglia ripresa. (*art. 35 Reg UE 2016/679 e Linee guida in tema di DPIA, WP 248/2017*)

Una corretta DPIA dovrà ragionare sul rispetto dei principi generali contenuti nell'art. 5 del Regolamento UE 2016/679 (RGDP), tra cui il principio di trasparenza previsto, tra l'altro, al punto 3.1 del provvedimento in materia di videosorveglianza pubblicato dal Garante nel 2010, che presuppone che gli interessati debbano essere sempre informati, nel caso di una ripresa, circa il fatto che stanno per accedere in una zona videosorvegliata. Sussiste altresì il principio di minimizzazione che presuppone che i dati raccolti siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Si potrà, dunque, comprendere il motivo per cui il Garante ha sanzionato con 2.000 euro un esercizio commerciale per avere installato una telecamera che riprendeva, oltre alle zone di sua pertinenza, anche proprietà di altri e la pubblica via adiacente.



I.s.e.c. Srl

A FRONTE DI UN RECLAMO PRESENTATO, il Garante si è, infatti, attivato per verificare la conformità rispetto al trattamento eseguito da una telecamera girevole che riprendeva non solo l'ingresso dell'esercizio ma la pubblica via, oltre all'ingresso pedonale e il passo carraio dell'abitazione del reclamante.

L'elemento più grave, segnalato dal Garante, è stata la TOTALE ASSENZA di cartellonistica informativa al riguardo. Operativamente l'Autorità, attivando il Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di Finanza, ha avviato un'istruttoria preliminare (doc. n. 9809504 del 28.07.2022 – link: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9809504> ). L'accertamento ispettivo ha rilevato la telecamera segnalata, priva di cartello che ne desse informativa, sottolineando anche la mancata applicazione del principio di minimizzazione, visto che la telecamera, dotata di dispositivo rotante, poteva riprendere ampie aree dei marciapiedi e della carreggiata delle due vie pubbliche adiacenti, oltre a finestre e porte di accesso degli immobili privati che si affacciavano sulle predette strade.

Il Garante, dunque, oltre che attestare l'assenza della dovuta informativa prevista, ha ritenuto che il trattamento fosse in ogni caso eccedente rispetto al legittimo interesse del titolare.

Per tali motivi ha ingiunto al titolare della telecamera di provvedere a circoscrivere alle sole aree di stretta pertinenza le riprese della telecamera, oltre che di fornire agli interessati l'informativa prevista, mediante l'apposizione di specifici cartelli. In aggiunta a ciò, ha inflitto all'attività commerciale una sanzione amministrativa pecuniaria di 2.000,00 euro per la violazione dell'*art. 5, par.1 lett. a) e c) del RGPD* e ha inoltre ritenuto necessaria anche l'applicazione della sanzione accessoria, consistente nella pubblicazione del provvedimento d'ingiunzione sul sito internet del Garante (*art. 166, c. 7 D.Lgs.196/2003*).

Appare dunque necessario, non foss'altro che per il livello di attenzione e di monitoraggio in costante crescita da parte dell'Autorità Garante, porre sempre più attenzione ai componenti che formano un sistema di videosorveglianza pubblico, controllando che le analisi da fare in merito siano state fatte, e che la eventuale documentazione necessaria sia presente, a norma, aggiornata e revisionabile in tempi medio rapidi. Solo così si potrà attestare, a seguito di un possibile controllo e rilievo, che tutto è stato svolto seguendo le direttive della norma.

Ricordiamo, infine, che oltre al sopracitato provvedimento del Garante del 2010, nel 2019 sono state emanate le *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video* (link: [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_201903\\_video\\_devices\\_it.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_it.pdf)) mentre per quanto riguarda la valutazione d'impatto è certamente utile la conoscenza delle Linee guida in materia, adottate nel 2017 (*Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248rev.01* – link: [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=611236](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236))

Restiamo a disposizione per tutti gli approfondimenti in merito.

Il Data Protection Officer (DPO)