I webinar di AnciRisponde

BODYCAM, DASH CAM, FOTOTRAPPOLE, DRONI E INTELLIGENZA ARTIFICIALE: LE NOVITÀ IN MATERIA DI TRATTAMENTO DATI

Dott. Marco MASSAVELLI

27 febbraio 2025

anciDigitale

DI CHE COSA PARLIAMO

- L'importanza della protezione dei dati personali nell'uso di tecnologie di raccolta video e dati
- Bodycam - Dash Cam - Fototrappole – Droni: come gestirli nel rispetto delle disposizioni in materia di protezione dei dati personali
- Intelligenza artificiale e analisi dei dati: normative emergenti in materia di AI e trattamento dati.
- Best practice e strategie di conformità: come condurre una valutazione d'impatto (DPIA) efficace.

anciDigitale

LE QUESTIONI DI MAGGIOR INTERESSE

Con l'evoluzione tecnologica, strumenti come bodycam, dashcam, fototrappole, droni e intelligenza artificiale stanno trasformando il modo in cui raccogliamo e utilizziamo i dati. Tuttavia, il loro utilizzo solleva questioni cruciali legate alla protezione dei dati personali e alla conformità normativa.

Questo webinar esplora le ultime novità e normative in materia di trattamento dati, fornendo approfondimenti pratici e indicazioni su come rispettare il GDPR e altre normative di riferimento, garantendo al contempo sicurezza ed efficacia nell'utilizzo di questi strumenti innovativi.

NORMATIVA DI RIFERIMENTO

- **REGOLAMENTO (UE) 2016/679** DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

- **DECRETO LEGISLATIVO 30 giugno 2003, n.196** recante il "Codice in materia di protezione dei dati personali" integrato con le modifiche introdotte dal **DECRETO LEGISLATIVO 10 agosto 2018, n. 101**, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679

Articolo 35

Valutazione d'impatto sulla protezione dei dati

1.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, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

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.

VALUTAZIONE DI IMPATTO PER VIDEOSORVEGLIANZA

Provvedimento GARANTE 11 ottobre 2018

Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione di impatto:

- *Trattamenti automatizzati finalizzati ad assumere decisioni che producono effetti giuridici oppure tali da incidere in modo significativo sull'interessato*
- *Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati*

L’adozione della valutazione di impatto sulla protezione dei dati personali

La valutazione di impatto è un **documento di competenza del titolare del trattamento**.

In nessun caso questo documento dovrebbe essere redatto dal responsabile della protezione dei dati personali, che si limita a svolgere attività di consulenza nel corso della redazione e ad esprimere un parere finale sul documento redatto.

Per quanto attiene ai trattamenti effettuati a mezzo videosorveglianza in ambito urbano, il titolare è da individuare nel Comune, inteso come Pubblica Amministrazione.

All’interno dell’Ente locale, quindi, a chi spetta la redazione e l’adozione di questo documento?

La redazione deve avvenire sicuramente in ambito gestionale e deve quindi essere effettuata dal dirigente interessato – titolare del trattamento in quota parte – o, laddove manchino le necessarie competenze tecnico-giuridiche, questo dovrà affidare l’incarico ad un esperto o comunque a un soggetto esterno all’Amministrazione, che presenti il necessario e adeguato profilo professionale.

L’adozione della valutazione di impatto sulla protezione dei dati personali

Una volta predisposta la valutazione, **il documento dovrà essere adottato dall’Ente, attraverso un atto tipico dell’espressione dell’autonomia amministrativa.**

Non vi è una risposta certa su quale sia il soggetto nel contesto organizzativo del Comune, deputato a svolgere questo compito.

In via generale, si può tuttavia ritenere opportuno adottare la valutazione di impatto sulla protezione dei dati personali **attraverso una deliberazione della Giunta comunale**, capace di esprimere la potestà in materia di indirizzo e controllo politico-amministrativo e, in via residuale, ogni altro compito non specificamente assegnato al Consiglio o alla dirigenza, a norma degli artt. 48 e 107 del D.Lgs. 18 agosto 2000, n. 267.

Vi è tuttavia da dire che il comma 3, lett. i), del citato art. 107, attribuisce ai dirigenti anche ogni altro atto previsto dallo statuto, dai regolamenti comunali o, in base a questi, delegati dal Sindaco.

È quindi evidente che qualora lo statuto comunale preveda l’adozione di documenti analoghi in capo alla dirigenza o, meglio ancora, lo stesso regolamento comunale sulla disciplina della videosorveglianza disponga espressamente che la valutazione di impatto sulla protezione dei dati personali sia adottata dal dirigente, spetterà a questo adottarla con proprio provvedimento o determinazione.

L’adozione della valutazione di impatto sulla protezione dei dati personali

Di particolare rilievo è la questione inerente la pubblicazione di informazioni concernenti la dislocazione e gli aspetti tecnici relativi agli impianti di videosorveglianza in uso o condivisi con le Forze di polizia, per finalità di controllo del territorio e tutela dell’ordine e della sicurezza pubblica.

Sul punto si è espresso il **TAR Lazio, sez. I, sentenza 1° agosto 2022, n. 10825**, censurando la divulgazione di informazioni di questo tipo “che, pur non costituendo segreto d’ufficio in senso proprio, per la loro particolare riservatezza”, in funzione delle finalità di prevenzione e repressione dei reati, “**costituiscono certo notizie che non possono essere rese di dominio pubblico**”.

Su questa scorta il giudice amministrativo individua tali informazioni tra quelle inaccessibili e quindi sottratte ad ogni tipo di ostensione a norma dell’**art. 3, comma 1, lett. d), del D.M. 10 maggio 1994, n. 415 (**atti e documenti concernenti l'organizzazione ed il funzionamento dei servizi di polizia) e, quindi, escluse anche dalle procedure di accesso civico e di accesso civico generalizzato, rispettivamente previste dagli artt. 5 e 5-bis del D.Lgs. 14 marzo 2013, n. 33

DISPOSITIVI MOBILI

- FOTOTRAPPOLE
- BODY CAM
- DASH CAM
- DRONI

Immagini memorizzate su schede di memoria o trasmesse via rete dati, grazie a una SIM

E’ necessario prevedere concrete modalità di protezione dei dati registrati: l’immagazzinamento di immagini su comuni supporti di memoria POTREBBE causare la perdita accidentale di informazioni o la sottrazione de dati /data breach)

DISPOSITIVI MOBILI

- ***Art. …….. - Utilizzo di particolari sistemi mobili.***

1. *Il Comando di Polizia Locale può dotarsi di telecamere riposizionabili, anche del tipo foto-trappola, con generazione di allarmi da remoto per il monitoraggio attivo.*

2. *Le modalità di impiego dei dispositivi in questione saranno disciplinate con apposito provvedimento da parte del Comandante della Polizia Locale.*

3. *Gli apparati di videosorveglianza modulare riposizionabili vengono installati secondo necessità, nei luoghi ove sia più sentita l'esigenza di tutela del decoro urbano e ambientale; possono essere utilizzati per accertare illeciti penali ed anche amministrativi, solo qualora non siano altrimenti accertabili con le ordinarie metodologie di indagine. Qualora non sussistano finalità di sicurezza o necessità di indagine previste dal D.Igs. 51/2018 che esimono dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica, per l'informativa agli utenti frequentatori di dette aree.*

- **…….**

DISPOSITIVI MOBILI

1. *Il Comando di Polizia Locale, per lo svolgimento delle attività di competenza può dotarsi di ogni altra tecnologia di ripresa video e di captazione di immagini necessaria al raggiungimento delle finalità istituzionali.*
2. *In particolare può dotarsi di Sistemi Aeromobili a Pilotaggio Remoto — droni — sia per l'esecuzione di riprese ai fini di tutela della sicurezza urbana, sia per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali: in ogni caso, i dispositivi e il loro utilizzo devono essere conformi alla normativa vigente, con particolare riferimento alla regolamentazione adottata dall'Ente Nazionale per l'Aviazione Civile e al Codice della Navigazione.*

- *Le modalità di impiego dei dispositivi in questione saranno disciplinate con apposito provvedimento del Comandante della Polizia Locale.*

DISPOSITIVI MOBILI

DISCIPLINARE DELLE ATTIVITA' DI MONITORAGGIO DEL TERRITORIO COMUNALE CON FOTO-VIDEOTRAPPOLE E MICROTELECAMERE e UTILIZZO BODYCAM

- Situazioni e operatori cui è permesso portare e utilizzare i dispositivi
- Indicazione delle circostanze in cui è ammessa l'attivazione delle bodycam
- Quali devono essere le modalità di impiego dei dispositivi nell'esecuzione di riprese in situazioni che richiedono particolari cautele (presenza di minori, vittime di reato, area privata…)
- Quali sono i soggetti autorizzati e preposti a verificare che le riprese siano effettivamente attinenti a situazioni che rientrano nelle finalità perseguite dal trattamento, nonché i soggetti incaricati del prelievo dati e con quali procedure e modalità debbano essere eseguite l'estrapolazione delle riprese
- ……

DISPOSITIVI MOBILI

- Prevedere opportune misure finalizzate ad impedire accessi abusivi e perdita di informazioni, nonché ogni altra misura necessaria al fine di garantire il corretto trattamento dei dati personali

STOP!!!!!!

DISPOSITIVI MOBILI

DRONI

Sono dotati di potenti sistemi di videoripresa di alta qualità con la possibilità di registrare immagini, scattare fotografie e trasmettere direttamente le riprese ad un device

Finalità: controllo del territorio – sicurezza urbana (GDPR) / polizia giudiziaria (illeciti ambientali, edilizi, spaccio) (DLGS 51/2018) IMMODIFICABILITA' FILMATO / protezione civile

DPIA DISPOSITIVI MOBILI

FOTOTRAPPOLE

Caratteristiche tecniche dell'impianto di videosorveglianza

- Il sistema prevede l'installazione di telecamere ad alta risoluzione con ottica varifocale e visione notturna con IR o a colori grazie a sensori ampi ed ampie aperture di diaframma. Per ogni installazione sono possibili molteplici punti di ripresa grazie anche alla capacità di trasmissione wireless (cifrata) tra box centrale e telecamere periferiche (dette satelliti).

- La postazione contiene una memoria, che consente la registrazione delle immagini riprese dalle telecamere. Il periodo di registrazione viene impostato, prevedendo l'automatica sovrascrittura delle immagini oltre il termine richiesto dal Comune.

DPIA DISPOSITIVI MOBILI

- La memoria è contenuta all'interno di una apparecchiatura disposta ad altezza superiore a 2.8 metri su un palo. Tutti i dispositivi e loro accessori sono protetti fisicamente da un contenitore con serratura chiusa a chiave, le cui chiavi vengono detenute esclusivamente da Alma Sicurezza, oppure sono protetti mediante altra forma di impedimento fisico all'accesso.

- L'apparecchiatura è protetta da password e username, i filmati registrati sono in formato proprietario e la trasmissione dati è criptata.

- Al presentarsi di un evento di abbandono il sistema lo rileva mediante un algoritmo basato sulla tecnica di "Background Subtraction", appositamente tarato per l'installazione specifica con indicazioni dimensionali e di orientamento eseguite da personale specializzato.

DPIA DISPOSITIVI MOBILI

- L'evento genera un "allarme" ed il pacchetto video relativi a tale allarme vengono inviati tramite cloud al Comune.
- Tutti i sistemi installati prevedono un codice di identificazione univoco, pertanto non è possibile "confondere" un sistema con un altro. All'atto dell'invio dei pacchetti video la struttura stessa del pacchetto identifica senza possibilità di errore il sistema da cui proviene.
- Il servizio/sistema memorizza su cloud GDPR compliant **con server in Italia o EU selezionabili**. Il fornitore di tale servizio è certificato ISO 9001 ed ISO 27001. E' inoltre qualificato dall'Agenzia per la Cybersicurezza Nazionale.

DPIA DISPOSITIVI MOBILI

Sicurezza del prodotto e controllo degli accessi

- I dispositivi sono forniti di sistema di logging, che registra sia gli accessi che i malfunzionamenti. In casi di tentativi di accessi non autorizzati o malfunzionamenti, i dispositivi inviano una notifica.
- I dispositivi prevedono la possibilità di creare utenti con diritti diversi, es: admin/user. Ogni accesso è tracciato nei logs e anche in caso di tentativi di accesso non riusciti, l'evento viene segnalato nei logs.

DPIA DISPOSITIVI MOBILI

BODY CAM

Risorse di supporto al trattamento dei dati.

- I dati trattati sono crittografati nei siti di memorizzazione e, anche durante la fase di trasferimento, *LA DITTA* mantiene le procedure di gestione delle chiavi di crittografia attuali e controllate.
- Crittografia dei dati in transito: i dati di prova vengono crittografati durante il trasferimento tramite SSL con chiave RSA a 2048 bit, crittografie a 256 bit, TLS 1.2, *Perfect Forward Secrecy*.
- Utenze granulari: per rispondere alle diverse esigenze degli utilizzatori, le utenze sono create con livelli di autorizzazioni e accessi alle riprese videoregistrate differenti. Tale modalità consente di poter attribuire autorizzazioni differenti ai vari operatori di centrale operativa ovvero operanti sul campo, ed avere il controllo di tutti gli accessi alla piattaforma per la visione del "*live streaming*" ovvero la consultazione delle videoregistrazioni effettuate dalle telecamere indossabili (*bodycam*).

DPIA DISPOSITIVI MOBILI

Nessun utilizzatore ha l'accesso diretto ai filmati dagli apparecchi di registrazione (*bodycam*) ma deve necessariamente visionarli e trasferirli solo dalla piattaforma informatica ".....", dopo essersi accreditato, potendo compiere solo le operazioni consentite rispetto al profilo di assegnazione.

DPIA DISPOSITIVI MOBILI

MISURE PREVISTE PER AFFRONTARE I RISCHIO PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI

Mitigazione del rischio derivante da sottrazione illecita, ovvero distruzione o smarrimento dei dispositivi di registrazione

- I dispositivi sono assicurati in maniera stabile all'uniforme degli operatori, adeguatamente addestrati alla gestione di situazioni ad alto impatto, pertanto la probabilità della sottrazione dei dispositivi, come pure la loro distruzione o smarrimento, può reputarsi "*poco probabile*".
- Tutte le registrazioni sono protette da crittografia, le videoriprese sono visionabili solo ed esclusivamente dal portale informatico "……." dopo il trasferimento dei dati criptati tramite apposito dispositivo "*dock station*" ed accredito personalizzato alla piattaforma "…….". Inoltre, per trasferire i dati contenuti occorre il tramite della "dock station" utilizzabile solo se in possesso delle necessarie chiavi informatiche, vale a dire codice identificativo di autorizzazione e password. La dannosità per la protezione dei dati in caso di sottrazione dei dispositivi di registrazione è pertanto pari a "*poco dannoso*".

DPIA DISPOSITIVI MOBILI

Ne consegue che il rischio per il trattamento dei dati in caso di sottrazione illecita, smarrimento o distruzione dei dispositivi è "*irrilevante*" poiché tale evento risulta "*poco probabile*" e "*poco dannoso*".

Mitigazione del rischio derivante da violazione dell'integrità dei dati

- Le videoregistrazioni, criptate, sono salvate su "*cluod dedicato*" fornito e gestito dalla Società, nominata formalmente responsabile esterno del trattamento dati; le videoriprese sono visionabili ed estrapolabili esclusivamente dalla piattaforma informatica "". La piattaforma è in possesso delle necessarie certificazioni di sicurezza informatica che ne garantiscono l'inviolabilità. La probabilità che possa verificarsi una violazione dell'integrità dei dati trattati nel server è pari a "*poco probabile*" mentre il responsabile esterno di trattamento dei dati, tramite il possesso delle certificazioni in argomento, fornisce le sufficienti garanzie per poterlo ritenere in grado di risolvere la criticità contenendo tempi di reazione ed effetti dannosi: l'evento ha il grado di "dannoso". Il rischio di violazione dei dati trattati è pertanto di grado "*Tollerabile*".

DPIA DISPOSITIVI MOBILI

Mitigazione del rischio derivante da violazione della riservatezza dei dati (accesso abusivo, trattamento non conforme)

- L'accesso ai dati conservati nel *cloud* dedicato attraverso la piattaforma "" è consentito solo a soggetti determinati e secondo i vari livelli di autorizzazione, definiti a mezzo di specifico ordine di servizio. Ogni ingresso e trattamento dei dati custoditi nella piattaforma informatica viene registrato in apposito file log che viene conservato anche ai fini di verifica e controllo. Gli operatori autorizzati vengono abilitati all'ingresso e trattamento con chiavi informatiche strettamente personali. L'evento della violazione della riservatezza dei dati a causa di accessi abusivi o trattamenti non conformi viene stimato in "*poco probabile*" e le verifiche periodiche riguardo alle operazioni conseguenti all'accesso ed il trattamento, con le restrizioni adottate, consentono di considerare l'evenienza come "*poco dannosa*"; di conseguenza il rischio per la violazione della riservatezza dei dati dovuto ad accesso abusivo o trattamento non conforme può essere catalogato come "*irrilevante*".

DPIA DISPOSITIVI MOBILI

Informativa agli interessati del trattamento

- I dispositivi di registrazione fonografica ed audiovisiva indossabili (*bodycam*) sono indossati in modo visibile e riportano, evidenziato da colore fluorescente, il pittogramma relativo agli apparati di registrazione accompagnato dalla dicitura "*Video Audio*".
- Gli agenti sono tenuti ad avvertire verbalmente, qualora le circostanze lo permettano, dell'attivazione del sistema di registrazione

STOP!!!

AI e protezione dati personali

Nei casi d'uso dell'AI che implicano anche il trattamento di dati personali **è imprescindibile** per gli operatori dei sistemi di AI – dai fornitori agli utilizzatori – tenere conto delle intersezioni tra AI Act e GDPR e adottare tutti i presidi necessari affinché l'uso di tali tecnologie risulti lecito e sicuro.

L'AI Act, che regola il ciclo di vita di una specifica tecnologia, non pregiudica l'applicazione del GDPR, ma ne è complementare.

AI e protezione dati personali

Principali potenziali **area di rischio:**

- **controllo generalizzato di massa dei dati personali anche particolari (es., biometrici)**
- **privacy dei lavoratori.**
- **tracking online e profilazione.**

Nell'ottica di mitigare i rischi per i diritti fondamentali tutelati negli articoli 7 e 8 della Carta, l'AI Act rimanda alla disciplina dettata dal GDPR, tra cui:

- i principi di minimizzazione e privacy by design e by default, applicabili dalla fase di pianificazione e progettazione dei sistemi di AI fino a quella di dismissione
- misure che i fornitori di sistemi di AI possono utilizzare per garantire la compliance a tali principi, tra cui l'anonimizzazione, la cifratura e l'uso di tecnologie che consentano di inserire algoritmi nei dati e di addestrare i sistemi di AI senza trasmissione o copia dei dati.

AI e protezione dati personali

DPIA e FRIA (Valutazione di impatto sui diritti fondamentali impattanti dall'uso di AI)

- Nel caso di sistemi di AI ad alto rischio, l'AI Act impone agli utilizzatori di svolgere una DPIA sulla base delle istruzioni comunicate dal fornitore all'utilizzatore per informarlo sulle finalità previste e sull'uso corretto del sistema di AI.
- **L'AI Act introduce un'ulteriore valutazione d'impatto, centrata sui diritti fondamentali (FRIA)**, finalizzata alla valutazione degli effetti che un sistema di AI ad alto rischio può avere sui diritti fondamentali delle persone e all'individuazione delle misure da adottare al concretizzarsi di tali rischi.
- **La funzione principale** della FRIA è identificare preventivamente, attraverso una valutazione mirata alla conformità legale, i potenziali rischi derivanti dall'utilizzo della AI e mitigarli prima che si manifestino.

Per consultare la Banca dati di Anci Risponde

https://ancirisponde.ancidigitale.it/

Per richieste di informazioni sul Servizio Anci Risponde e/o sugli altri servizi:

- Tel. 06 83394257-2
- info@ancidigitale.it
- www.ancidigitale.it

Per informazioni sulle formule di abbonamento

- https://www.ancidigitale.it/servizi/