Transizione Digitale

La videosorveglianza nelle P.A.

Avv. Alessio Cicchinelli – 15 maggio 2024

Ambito trasversale di incidenza della videosorveglianza

Ambito trasversale di incidenza della videosorveglianza

FAQ GARANTE della Privacy in tema di videosorveglianza: https://www.garanteprivacy.it/faq/videosorveglianza

1) Quali sono le regole da rispettare per installare sistemi di videosorveglianza?

L'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili: ad esempio, le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, o in materia di controllo a distanza dei lavoratori. Va sottolineato, in particolare, che l'attività di videosorveglianza va effettuata nel rispetto del cosiddetto principio di minimizzazione dei dati riguardo alla scelta delle modalità di ripresa e dislocazione e alla gestione delle varie fasi del trattamento. I dati trattati devono comunque essere pertinenti e non eccedenti rispetto alle finalità perseguite.

E' bene ricordare inoltre che il Comitato europeo per la protezione dei dati (EDPB) ha adottato le "*Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*" allo scopo di fornire indicazioni sull'applicazione del Regolamento in relazione al trattamento di dati personali attraverso dispositivi video, inclusa la videosorveglianza.

Videosorveglianza e privacy

Videosorveglianza e privacy – principi del GDPR

Liceità

Perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato o su altra base legittima prevista per legge dal presente regolamento o dal diritto dell'Unione o degli Stati membri, come indicato 4.5.2016 IT Gazzetta ufficiale dell'Unione europea L 119/7 nel presente regolamento, tenuto conto della necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso

Videosorveglianza e privacy – principi del GDPR

Liceità

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; (…) e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore

Correttezza e trasparenza

Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano

Limitazione della finalità del trattamento

Il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti.

Minimizzazione dei dati

Il principio di minimizzazione esprime il concetto in base al quale i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento.

Applicazione dei principi GDPR – I soggetti

Individuazione delle figure soggettive e dei ruoli rilevanti al fine del rispetto della normativa sul trattamento dei dati personali.

Garante privacy – provvedimento del 18.7.23, n. 9920664

3) Le persone che transitano nelle aree videosorvegliate devono essere informate della presenza delle telecamere?

Sì. Gli interessati devono sempre essere informati (ex art. 13 del Regolamento) che stanno per accedere in una zona videosorvegliata, anche in occasione di eventi e spettacoli pubblici (ad esempio, concerti, manifestazioni sportive) e a prescindere dal fatto che chi tratta i dati sia un soggetto pubblico o un soggetto privato.

Applicazione dei principi GDPR - Informativa

Nel rispetto del principio di "liceità, correttezza e trasparenza", il titolare del trattamento deve adottare misure appropriate per fornire all'interessato, prima di iniziare il trattamento, tutte le informazioni richieste dal Regolamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (artt. 5, par. 1, lett. a), 12 e 13 del Regolamento).

Applicazione dei principi GDPR - Informativa

CARTELLO VIDEOSORVEGLIANZA - Modello semplificato [65 k, docx]

Applicazione dei principi GDPR - Informativa

Allorquando siano impiegati dispositivi video, il titolare del trattamento, oltre a rendere l'informativa di primo livello mediante apposizione di segnaletica di avvertimento in prossimità della zona sottoposta a videosorveglianza, deve fornire agli interessati anche delle "informazioni di secondo livello", che devono "contenere tutti gli elementi obbligatori a norma dell'articolo 13 del [Regolamento]" ed "essere facilmente accessibili per l'interessato, ad esempio attraverso un pagina informativa completa messa a disposizione in uno snodo centrale [...] o affissa in un luogo di facile accesso"

Applicazione dei principi GDPR - Informativa

Le informazioni di primo livello (cartello di avvertimento) "dovrebbero comunicare i dati più importanti, ad esempio le finalità del trattamento, l'identità del titolare del trattamento e l'esistenza dei diritti dell'interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento" (Linee guida del Comitato, cit., par. 114). Inoltre, la segnaletica deve contenere anche quelle informazioni che potrebbero risultare inaspettate per l'interessato. Potrebbe trattarsi, ad esempio, della trasmissione di dati a terzi, in particolare se ubicati al di fuori dell'Unione europea, e del periodo di conservazione. Se tali informazioni non sono indicate, l'interessato dovrebbe poter confidare nel fatto che vi sia solo una sorveglianza in tempo reale (senza alcuna registrazione di dati o trasmissione a soggetti terzi) (Linee guida del Comitato, cit., par. 115). La segnaletica di avvertimento di primo livello deve contenere un chiaro riferimento al secondo livello d'informazioni, ad esempio indicando un sito web sul quale è possibile consultare il testo dell'informativa estesa.

2) Occorre avere una autorizzazione da parte del Garante per installare le telecamere?

No. Non è prevista alcuna autorizzazione da parte del Garante per installare tali sistemi.

In base al principio di responsabilizzazione (art. 5, par. 2, del Regolamento), spetta al titolare del trattamento (un'azienda, una pubblica amministrazione, un professionista, un condominio...) valutare la liceità e la proporzionalità del trattamento, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Il titolare del trattamento deve, altresì, valutare se sussistano i presupposti per effettuare una valutazione d'impatto sulla protezione dei dati prima di iniziare il trattamento (cfr. FAQ n. 7).

Applicazione dei principi GDPR – Responsabilizzazione e DPIA

7)Quali sistemi di videosorveglianza necessitano di valutazione d'impatto preventiva?

La valutazione d'impatto preventiva è prevista se il trattamento, quando preveda 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 le persone fisiche (artt. 35 e 36 del Regolamento) (per approfondimenti si vedano le "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 del 4 ottobre 2017).

Può essere il caso, ad esempio, dei sistemi integrati - sia pubblici che privati - che collegano telecamere tra soggetti diversi nonché dei sistemi intelligenti, capaci di analizzare le immagini ed elaborarle, ad esempio al fine di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli.

La valutazione d'impatto sulla protezione dei dati è sempre richiesta, in particolare, in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico (art. 35, par. 3, lett. c) del Regolamento) e negli altri casi indicati dal Garante (cfr. "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679" dell'11 ottobre 2018).

Art. 35, GDPRP

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.

Art. 35, GDPRP

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 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.

Applicazione dei principi GDPR – Responsabilizzazione e DPIA

Art. 35, GDPRP

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Applicazione dei principi GDPR – Conservazione

5) Quali sono i tempi dell'eventuale conservazione delle immagini registrate?

Le immagini registrate non possono essere conservate più a lungo di quanto necessario per le finalità per le quali sono acquisite (art. 5, paragrafo 1, lett. c) ed e), del Regolamento). In base al principio di responsabilizzazione (art. 5, paragrafo 2, del Regolamento), spetta al titolare del trattamento individuare i tempi di conservazione delle immagini, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Ciò salvo che specifiche norme di legge non prevedano espressamente determinati tempi di conservazione dei dati (si veda, ad esempio, l'art. 6, co. 8, del D.L. 23/02/2009, n. 11, ai sensi del quale, nell'ambito dell'utilizzo da parte dei Comuni di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, *"la conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione"*).

In via generale, gli scopi legittimi della videosorveglianza sono spesso la sicurezza e la protezione del patrimonio. Solitamente è possibile individuare eventuali danni entro uno o due giorni. Tenendo conto dei principi di minimizzazione dei dati e limitazione della conservazione, i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve a rilevare atti vandalici) – cancellati dopo pochi giorni, preferibilmente tramite meccanismi automatici. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione.

Ad esempio, normalmente il titolare di un piccolo esercizio commerciale si accorgerebbe di eventuali atti vandalici il giorno stesso in cui si verificassero. Un periodo di conservazione di 24 ore è quindi sufficiente. La chiusura nei fine settimana o in periodi festivi più lunghi potrebbe tuttavia giustificare un periodo di conservazione più prolungato.

6) È possibile prolungare i tempi di conservazione delle immagini?

In alcuni casi può essere necessario prolungare i tempi di conservazione delle immagini inizialmente fissati dal titolare o previsti dalla legge: ad esempio, nel caso in cui tale prolungamento si renda necessario a dare seguito ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria in relazione ad un'attività investigativa in corso.

Videosorveglianza nei luoghi di lavoro

9) Il datore di lavoro pubblico o privato può installare un sistema di videosorveglianza nelle sedi di lavoro?

Sì, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, nel rispetto delle altre garanzie previste dalla normativa di settore in materia di installazione di impianti audiovisivi e altri strumenti di controllo (art. 4 della l. 300/1970).

Art. 37 Statuto dei lavoratori

Le disposizioni della presente legge si applicano anche ai rapporti di lavoro e di impiego dei dipendenti da enti pubblici che svolgono esclusivamente o prevalentemente attività economica. Le disposizioni della presente legge si applicano altresì ai rapporti di impiego dei dipendenti dagli altri enti pubblici, salvo che la materia sia diversamente regolata da norme speciali.

Videosorveglianza nei luoghi di lavoro – Statuto dei lavoratori e dipendenti pubblici

Art. 42, D.Lgs. n. 165/01

1. Nelle pubbliche amministrazioni la libertà e l'attività sindacale sono tutelate nelle forme previste dalle disposizioni della legge 20 maggio 1970, n. 300, e successive modificazioni ed integrazioni. Fino a quando non vengano emanate norme di carattere generale sulla rappresentatività sindacale che sostituiscano o modifichino tali disposizioni, le pubbliche amministrazioni, in attuazione dei criteri di cui all'articolo 2, comma 1, lettera b) della legge 23 ottobre 1992, n. 421, osservano le disposizioni seguenti in materia di rappresentatività delle organizzazioni sindacali ai fini dell'attribuzione dei diritti e delle prerogative sindacali nei luoghi di lavoro e dell'esercizio della contrattazione collettiva.

Videosorveglianza nei luoghi di lavoro – Statuto dei lavoratori e dipendenti pubblici

Art. 37 Statuto dei lavoratori

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. *In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.*

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.

Circolare Ispettorato n. 2 del 2016

Ciò posto, è pertanto necessario individuare quando l'installazione di apparecchiature di localizzazione satellitare GPS sia strettamente funzionale a "...rendere la prestazione lavorativa...", tenuto conto che l'interpretazione letterale del disposto normativo porta a considerare quali strumenti di lavoro quegli apparecchi, dispositivi, apparati e congegni che costituiscono il mezzo indispensabile al lavoratore per adempiere la prestazione lavorativa dedotta in contratto, e che per tale finalità sia stati posti in uso e messi a sua disposizione. In linea di massima, e in termini generali, si può ritenere che i sistemi di sistemi di geolocalizzazione rappresentino un elemento "aggiunto" agli strumenti di lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa ma, per rispondere ad esigenze ulteriori di carattere assicurativo, organizzativo, produttivo o per garantire la sicurezza del lavoro. Ne consegue che, in tali casi, la fattispecie rientri nel campo di applicazione di cui al comma 1 dell'art.4 L. n. 300/1970 e pertanto le relative apparecchiature possono essere installate solo previo accordo stipulato con la rappresentanza sindacale ovvero, in assenza di tale accordo, previa autorizzazione da parte dell'Ispettorato nazionale del lavoro (art. 4, comma 1, della L. n. 300/1970 come modificato dall'art. 5, comma 2, D.Lgs. n. 185/2016).

Circolare Ispettorato n. 2 del 2016

Si evidenzia tuttavia, che solo in casi del tutto particolari - qualora i sistemi di localizzazione siano installati per consentire la concreta ed effettiva attuazione della prestazione lavorativa (e cioè la stessa non possa essere resa senza ricorrere all'uso di tali strumenti), ovvero l'installazione sia richiesta da specifiche normative di carattere legislativo o regolamentare (es. uso dei sistemi GPS per il trasporto di portavalori superiore a euro 1.500.000,00, ecc.) – si può ritenere che gli stessi finiscano per "trasformarsi" in veri e propri strumenti di lavoro e pertanto si possa prescindere, ai sensi di cui al comma 2 dell'art. 4 della L. n. 300/1970, sia dall'intervento della contrattazione collettiva che dal procedimento amministrativo di carattere autorizzativo previsti dalla legge.

Provvedimento del 21 dicembre 2023 - Documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" [9978728]

Le predette garanzie non trovano invece applicazione "agli strumenti di registrazione degli accessi e delle presenze", così come "agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" (art. 4, comma 2, l. n. 300/1970). Tale disposizione introduce un'eccezione, rispetto al più restrittivo regime previsto dal comma 1, e deve, pertanto, essere oggetto di stretta interpretazione, considerate le responsabilità anche sul piano penale che possono derivare dalla violazione del predetto quadro normativo. Per scelta espressa del legislatore, solo gli strumenti preordinati, anche in ragione delle caratteristiche tecniche di configurazione, alla "registrazione degli accessi e delle presenze" e allo "svolgimento della prestazione" non soggiacciono quindi ai limiti e alle garanzie di cui al primo comma, in quanto funzionali a consentire l'assolvimento degli obblighi che discendono direttamente dal contratto di lavoro, vale a dire, la presenza in servizio e l'esecuzione della prestazione lavorativa.

Provvedimento n. 138 del 16.3.2017 a firma del Garante Privacy italiano [doc. web n. 6275314] ("...il sistema di localizzazione dei veicoli non è direttamente preordinato all'esecuzione della prestazione lavorativa con conseguente applicazione del menzionato articolo 4, comma 1...") , e Provvedimento n. 139 dell'8.3.2018 a firma del Garante Privacy italiano [doc. web n. 8163433].

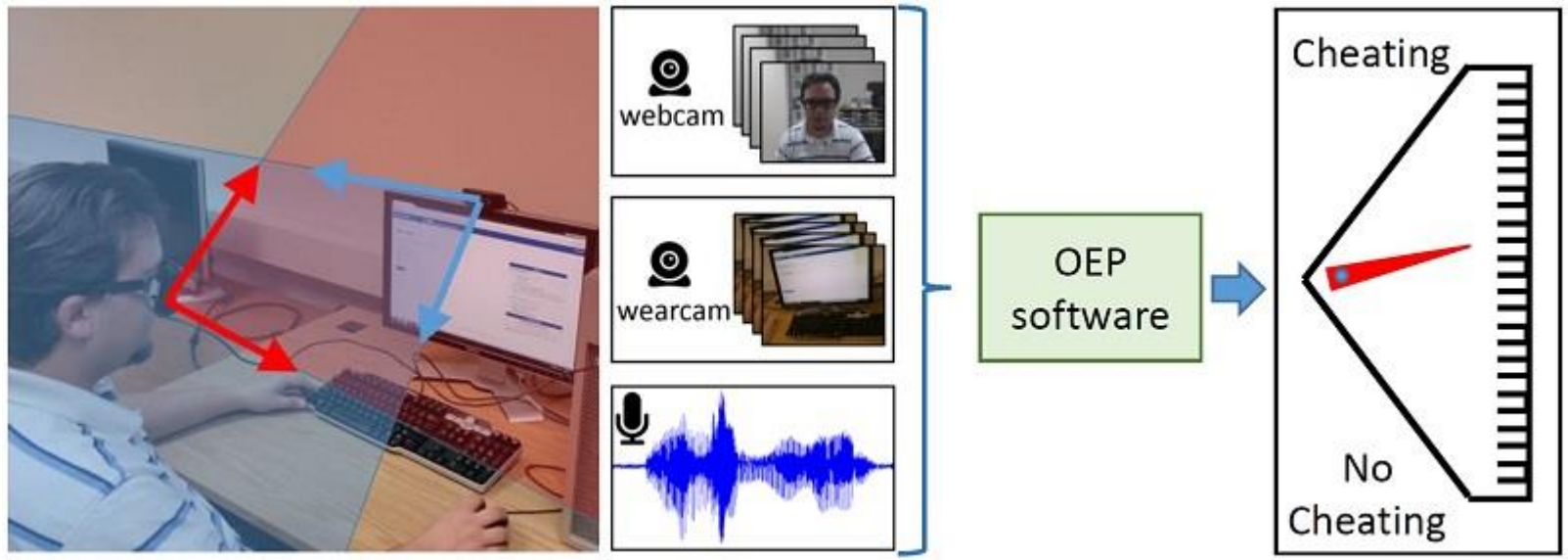
in tale nozione – infatti – e con riferimento agli strumenti oggetto del presente provvedimento, vale a dire servizio di posta elettronica e navigazione web – è da ritenere che possano ricomprendersi solo servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza. Da questo punto di vista e a titolo esemplificativo, possono essere considerati "strumenti di lavoro" alla stregua della normativa sopra citata il servizio di posta elettronica offerto ai dipendenti (mediante attribuzione di un account personale) e gli altri servizi della rete aziendale, fra cui anche il collegamento a siti internet. Costituiscono parte integrante di questi strumenti anche i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore (ad esempio: sistemi di logging per il corretto esercizio del servizio di posta elettronica, con conservazione dei soli dati esteriori, contenuti nella cosiddetta "envelope" del messaggio, per una breve durata non superiore comunque ai sette giorni; sistemi di filtraggio anti virus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso).

Provvedimento n. 138 del 16.3.2017 a firma del Garante Privacy italiano [doc. web n. 6275314] ("...il sistema di localizzazione dei veicoli non è direttamente preordinato all'esecuzione della prestazione lavorativa con conseguente applicazione del menzionato articolo 4, comma 1..."), e Provvedimento n. 139 dell'8.3.2018 a firma del Garante Privacy italiano [doc. web n. 8163433].

Altri strumenti pure utili al conseguimento di una elevata sicurezza della rete aziendale, invece, non possono normalmente consentire controlli sull'attività lavorativa, non comportando un trattamento di dati personali dei dipendenti, e di conseguenza non sono assoggettati alla disciplina di cui all'art. 4 Stat. Lav. (ad es. sistemi di protezione perimetrale – firewall – in funzione di antintrusione e sistemi di prevenzione e rilevamento d'intrusioni – IPS/IDS – agente su base statistica o con il ricorso a sorgenti informative esterne) [...] i principi di necessità e proporzionalità impongono di privilegiare misure preventive ed, in ogni caso, gradualità nell'ampiezza del monitoraggio "che renda assolutamente residuali i controlli più invasivi, legittimandoli solo a fronte della rilevazione di specifiche anomalie" quali, ad esempio, la riscontrata presenza di virus e "comunque all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori

Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano – 16 settembre 2021

Registro dei provvedimenti
n. 317 del 16 settembre 2021



Videosorveglianza e pubblica sicurezza

Art. 6 D.L. 11/09, convertito con L. n. 38/09

Piano straordinario di controllo del territorio

7. Per la tutela della sicurezza urbana, i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico.

8. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione.

Art. 4 D.L. 14/17, convertito con L. n. 48/17

Definizione

1. Ai fini del presente decreto, si intende per sicurezza urbana il bene pubblico che afferisce alla vivibilità e al decoro delle città, da perseguire anche attraverso interventi di riqualificazione *anche urbanistica, sociale e culturale,* e recupero delle aree o dei *siti degradati*, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio, la promozione *della cultura* del rispetto della legalità e l'affermazione di più elevati livelli di coesione sociale e convivenza civile, cui concorrono prioritariamente, anche con interventi integrati, lo Stato, le Regioni e Province autonome di Trento e di Bolzano e gli enti locali, nel rispetto delle rispettive competenze e funzioni.

Art. 5 D.L. 14/17, convertito con L. n. 48/17

Patti per l'attuazione della sicurezza urbana

1. In coerenza con le linee generali di cui all'articolo 2, con appositi patti sottoscritti tra il prefetto ed il sindaco, nel rispetto di linee guida adottate, su proposta del Ministro dell'interno, con accordo sancito in sede di Conferenza Stato-città e autonomie locali, possono essere individuati, in relazione alla specificità dei contesti, interventi per la sicurezza urbana, tenuto conto anche delle esigenze delle aree rurali confinanti con il territorio urbano.

DECRETO LEGISLATIVO 18 maggio 2018, n. 51

Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonche' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. (18G00080) (GU Serie Generale n.119 del 24 05 2018)

DECRETO LEGISLATIVO 18 maggio 2018, n. 51

Art. 3
Principi applicabili
al trattamento di dati personali

1. I dati personali di cui all'articolo 1, comma 2, sono:

a) trattati in modo lecito e corretto;
b) raccolti per finalità determinate, espresse e legittime e trattati in modo compatibil con tali finalità;
c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati;
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragione per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per quali sono trattati;
e) conservati con modalità che consentano l'identificazione degli interessati per il ten necessario al conseguimento delle finalità per le quali sono trattati, sottoposti a es periodico per verificarne la persistente necessità di conservazione, cancellati o anonimizzati una volta decorso tale termine;
f) trattati in modo da garantire un'adeguata sicurezza e protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali, mediante l'adozione di misure tecniche e organizzative adeguate.

DECRETO LEGISLATIVO 18 maggio 2018, n. 51

Art. 4

Conservazione e verifica della qualità dei dati, distinzione tra categorie di interessati e di dati

1. Il titolare del trattamento, tenuto conto della finalità del trattamento e per quanto possibile, distingue i dati personali in relazione alle diverse categorie di interessati previste dalla legge e i dati fondati su fatti da quelli fondati su valutazioni. La distinzione in relazione alle diverse categorie di interessati si applica, in particolare, alle seguenti categorie di interessati: persone sottoposte a indagine; imputati; persone sottoposte a indagine o imputate in procedimento connesso o collegato; persone condannate con sentenza definitiva; persone offese dal reato; parti civili; persone informate sui fatti; testimoni.

DECRETO LEGISLATIVO 18 maggio 2018, n. 51

Art. 6

Condizioni di trattamento specifiche

1. I dati personali raccolti per le finalità di cui all'articolo 1, comma 2, non possono essere trattati per finalità diverse, salvo che tale trattamento sia consentito dal diritto dell'Unione europea o dalla legge.

DECRETO LEGISLATIVO 18 maggio 2018, n. 51

Art. 7

Trattamento di categorie particolari di dati personali

1. Il trattamento di dati di cui all'articolo 9 del regolamento UE è autorizzato solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento, ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato.

DECRETO LEGISLATIVO 18 maggio 2018, n. 51

Art. 8

Processo decisionale automatizzato relativo alle persone fisiche

1. Sono vietate le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge.

2. Le disposizioni di legge devono prevedere garanzie adeguate per i diritti e le libertà dell'interessato. In ogni caso è garantito il diritto di ottenere l'intervento umano da parte del titolare del trattamento.

DECRETO LEGISLATIVO 18 maggio 2018, n. 51

Art. 8

Processo decisionale automatizzato relativo alle persone fisiche

1. Sono vietate le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge.

2. Le disposizioni di legge devono prevedere garanzie adeguate per i diritti e le libertà dell'interessato. In ogni caso è garantito il diritto di ottenere l'intervento umano da parte del titolare del trattamento.

Videosorveglianza nelle P.A. – CONCLUSIONI

- Ruolo del Garante della privacy;

- Modello di valutazione del rischio integrato.

Transizione Digitale

GRAZIE MILLE!

CONTATTI

https://www.transizionedigitale.it/contatti

info@transizionedigitale.it