PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4881 di Lunedì 01 marzo 2021

Privacy e lavoro: videosorveglianza e geolocalizzazione

Indicazioni su vari aspetti correlati al tema della privacy nel mondo del lavoro. Le responsabilità, il controllo a distanza e le misure di sicurezza in tema di videosorveglianza e geolocalizzazione.

Pavia, 1 Mar ? Il nostro giornale, specialmente attraverso gli articoli di Adalberto Biasiotti, si è soffermato spesso sul tema della **privacy** con riferimento alle varie fonti normative: dal Regolamento europeo 2016/679 (GDPR - *General Data Protection Regulation*) al Codice in materia di protezione dei dati personali, il D.lgs. 196/2003, come modificato dal D.Lgs. 101/2018.

Un intervento al workshop "**Il fattore umano nella sicurezza stradale**", che si è tenuto lo scorso 4 luglio e che è stato organizzato dal Comitato Trasporti di Assogastecnici, ci permette di tornare a parlare di protezione dei dati personali con riferimento particolare alle attività di trasporto e ad aspetti come la **videosorveglianza** e la **geolocalizzazione** che con il GDPR "subiscono delle modifiche sostanziali".

L'articolo si sofferma sui seguenti argomenti su:

- I ruoli in materia di privacy e il controllo a distanza
- La videosorveglianza e le misure di sicurezza
- La progettazione degli strumenti di geolocalizzazione

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0547] ?#>

I ruoli in materia di privacy e il controllo a distanza

Nell'intervento "**Aspetti legati alla privacy**", a cura di Giuseppe Nucera (Assogastecnici) si ricorda innanzitutto che "nei rapporti di fornitura di servizi intercorrenti tra le aziende dei gas e i loro vettori è bene che sia chiaro quali siano i rispettivi ruoli all'interno delle dinamiche privacy e in particolare cosa determina l'essere un titolare del trattamento, un responsabile e un contitolare".

Riprendiamo alcune indicazioni sui **vari ruoli**:

- **Titolare del trattamento**: è 'la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali' (art. 4. par. 1, n. 7 GDPR). Il titolare del trattamento dei dati "è il soggetto le cui finalità vengono perseguite attraverso il trattamento medesimo (vedi anche Garante per la protezione dei dati personali: provvedimento n. 383 del 14 giugno 2018 avverso una società di smaltimento rifiuti)";
- **Responsabile del trattamento**; "è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR)";
- **Contitolari del trattamento**: "allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. In tale caso la normativa (art. 26 GDPR) impone ai contitolari di definire specificamente, con un atto giuridicamente valido, il rispettivo ambito di responsabilità e i compiti".

Si riportano anche alcune indicazioni sul "**controllo a distanza**" nello Statuto dei lavoratori.

A questo proposito si segnala che "l'attuale formulazione dell'art. 4 dello Statuto dei Lavoratori (l. 300/1970) così come modificata dal D.Lgs. n. 151/2015, protende verso una prospettiva di legittimità dei sistemi di controllo a distanza, a condizione che gli strumenti utilizzati siano impiegati esclusivamente 'per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale' e per l'installazione "sarà necessario un previo accordo collettivo stipulato con la rappresentanza sindacale unitaria o con le rappresentanze sindacali aziendali, oppure previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro".

In particolare "è consentito il controllo a distanza del lavoratore, ma solo in presenza di determinate condizioni" (Tribunale di Roma, sez. III Lavoro, con ordinanza n. 57668/18; depositata il 13 giugno 2018).

La videosorveglianza e le misure di sicurezza

Veniamo al tema della **videosorveglianza**.

La relazione segnala che la materia della videosorveglianza è "caratterizzata dalla particolarità della **doppia informativa** come previsto da un provvedimento del Garante, datato 8.04.2010: un'informativa minima (il cartello 'Area videosorvegliata'), che trae la sua legittimità/esistenza dall'abrogato art. 13 comma 3 del vecchio Codice Privacy ed un'informativa completa che deve essere resa conformemente a quanto disposto dal GDPR (art 13). E attualmente l'uso dell'informativa minima "è ancora molto diffuso e probabilmente lo sarà anche in futuro con gli interventi 'armonizzatori' del legislatore e/o del Garante privacy".

Inoltre le misure di sicurezza da adottare in materia di videosorveglianza e geolocalizzazione "devono rispettare l'art. 32 GDPR e, per la videosorveglianza quanto indicato nel provvedimento del Garante dell'8 aprile 2010, mentre per la geolocalizzazione quanto contenuto nel provvedimento del 4 ottobre 2011".

In particolare "parafrasando l'art 32, i dati raccolti devono essere protetti con adeguate **misure di sicurezza**, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini. Alcuni esempi citati dall'art. 32:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (es. backup / disaster recovery);
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

In particolare il **provvedimento del Garante del 2010** al punto 3.3. "dispone che devono essere adottate specifiche misure tecniche ed organizzative che consentano al titolare del trattamento di verificare l'attività svolta da parte di chi accede alle immagini o controlla i sistemi di ripresa. Sia i soggetti che rilevano (visualizzano le immagini in tempo reale), sia i soggetti che registrano devono possedere credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza".

Il provvedimento del Garante prevede inoltre:

- "limitazione massima dell'accesso alle immagini da parte dei soggetti preposti ad opere di manutenzione del sistema di videosorveglianza;
- protezione degli apparati di ripresa digitali connessi a reti informatiche da rischi di accesso abusivo;
- crittografia della trasmissione tramite rete pubblica di comunicazioni delle immagini riprese, anche per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless".

Per quanto riguarda "il periodo di conservazione delle immagini (a prescindere dalla durata scelta) devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto (utilizzare la sovrascrittura)".

Tendenzialmente si evidenzia poi "il divieto di **audio-videosorveglianza**" (vedi provvedimento n. 11 del gennaio 2012). Le aziende "che acquistano telecamere devono controllare se la specifica prevede l'audio e intervenire di conseguenza".

Riguardo poi alla **videosorveglianza *on-board cameras*** sono riportate nell'intervento le seguenti indicazioni:

- "Assicurarsi che tutti siano informati della registrazione.
- Apporre adesivi all'interno della cabina per avvertire autisti e passeggeri.
- Apporre gli adesivi all'esterno del veicolo per informare il pubblico.
- I messaggi devono essere specifici, ad es. questo veicolo è dotato di un sistema di videoregistrazione allo scopo di prevenire reati criminali e proteggere la pubblica sicurezza.
- Assicurarsi che il personale sia al corrente delle politiche in materia e le comprenda; a tal proposito potrebbe risultare utile organizzare sessioni di formazione per spiegare il funzionamento di tali strumenti.
- Concedere l'accesso ai filmati montati o alle immagini fotografiche a tutte le parti ufficialmente coinvolte nella conduzione di una indagine.
- Fornire le immagini registrate qualora un interessato le richieda per iscritto; le immagini di altri individui identificabili devono apparire sfocate".

La progettazione degli strumenti di geolocalizzazione

L'intervento si sofferma anche sulla **geolocalizzazione**, l'identificazione della posizione geografica, indicando che i lavoratori "devono essere sempre informati che il veicolo è soggetto a localizzazione e pertanto devono essere rese disponibili:

- Una vetrofania all'interno del veicolo, recante la dicitura «Veicolo sottoposto a localizzazione», contenente le informazioni fondamentali
- Un'informativa estesa, contenente tutte le informazioni relative al sistema di geolocalizzazione adottato".

In particolare in ossequio al principio della ***privacy by design***, il Garante per la protezione dei dati personali, "con una recente decisione (provvedimento 232 del 18 aprile 2018) ha individuato i criteri di progettazione degli strumenti di geolocalizzazione:

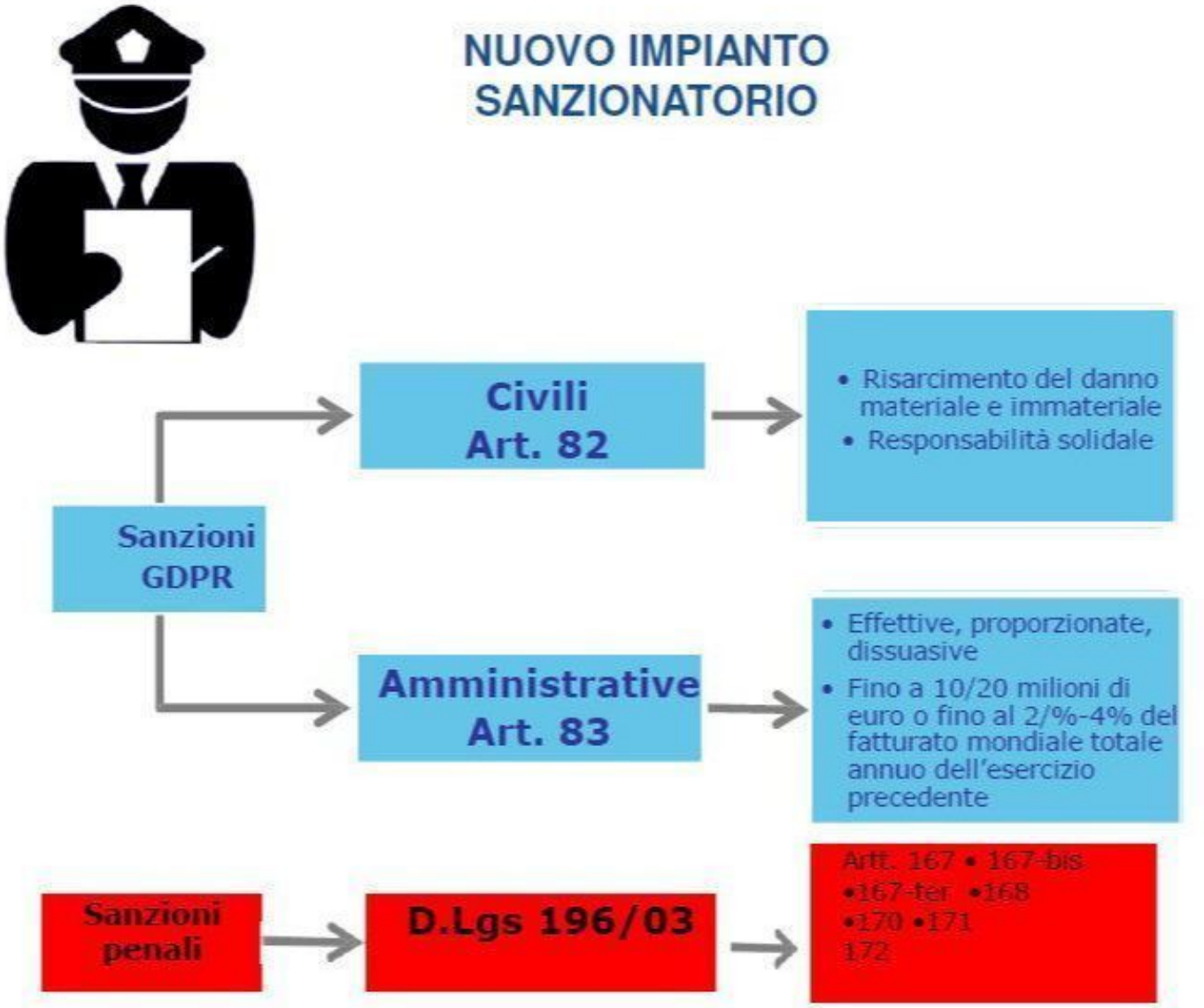
- la configurazione del sistema permetta il posizionamento sul dispositivo di un'icona che indichi che la funzionalità di localizzazione è attiva;
- la configurazione del sistema consenta la disattivazione della funzionalità di localizzazione durante le pause consentite dell'attività lavorativa;
- la configurazione del sistema permetta di oscurare la visibilità della posizione geografica decorso un periodo determinato di inattività dell'operatore sul monitor presente nella centrale operativa relativamente a tale funzionalità".

Inoltre alle suddette misure tecniche il Garante ha affiancato anche le seguenti **misure organizzative**:

- l'individuazione di profili differenziati di autorizzazione relativi alle diverse tipologie di dati e di operazioni eseguibili;
- l'individuazione di tempi di conservazione dei dati in concreto trattati tenendo conto delle finalità perseguite;
- la predisposizione di rapporti per i clienti privi di qualunque riferimento che consenta l'identificazione di dipendenti;
- la designazione, quale responsabile del trattamento, del fornitore del software di localizzazione;
- la predisposizione di periodiche verifiche di test sulla funzionalità e l'affidabilità dei parametri adottati, in vista della valutazione di eventuali falsi positivi o negativi effettuati dal sistema e la conseguente predisposizione di correttivi a tutela della qualità dei dati trattati".

Le impostazioni predefinite del dispositivo di geolocalizzazione ? continua il relatore ? "dovrebbero essere configurate con modalità proporzionate rispetto al principio di riservatezza degli interessati (come sottolineato anche dal Garante) attraverso l'adozione di misure che consentano la rilevazione della posizione ad intervalli non estremamente ravvicinati, la disattivazione della rilevazione geografica durante le pause previste dall'attività lavorativa, oltre che una conservazione della disponibilità del dato per un periodo non eccedente rispetto al perseguimento delle finalità prestabilite (vedi provvedimento Garante n. 396 del 28 giugno 2018").

Riportiamo, infine, dalle slide uno schema relativo al nuovo **impianto sanzionatorio** in materia di privacy:



Concludiamo rimandando alla lettura integrale dell'intervento che riporta ulteriori informazioni sulle possibili sanzioni penali e amministrative e su vari altri aspetti (data breach, profilazione, ...).

RTM

Scarica il documento da cui è tratto l'articolo:

" Aspetti legati alla privacy", a cura di Giuseppe Nucera (Assogastecnici), intervento al workshop "Il fattore umano nella sicurezza stradale" (formato PDF, 1.20 MB).

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it