PRIVACY NEWS
del 12 Febbraio 2014

Rassegna delle ultime novità Privacy

Videosorveglianza sul luogo di lavoro: senza autorizzazione, responsabilità penale anche con telecamere spente

Con sentenza n. 4331 del 30 gennaio 2014, la Corte di Cassazione ha chiarito che l'installazione di una telecamera puntata sui dipendenti, o in luoghi di lavoro dove questi hanno accesso anche occasionalmente, effettuata senza aver ricevuto preventivamente l'autorizzazione dell'ispettorato del lavoro, o senza aver stipulato prima uno specifico accordo con le rappresentanze sindacali, comporta la responsabilità penale del datore di lavoro.

Non conta, secondo gli ermellini, il fatto che le videoriprese sul posto di lavoro siano iniziate soltanto dopo il benestare della direzione provinciale del lavoro, se le telecamere erano precedentemente installate.

E' stato infatti particolarmente precisato che, in virtù dell'art. 4 dello Statuto dei Lavoratori (Legge 300/1970), a priori va tutelato il bene giuridico della riservatezza del lavoratore e, di conseguenza, il reato a carico del datore può configurarsi con la mera installazione non autorizzata dell'impianto di videoripresa, anche se la telecamera rimane spenta in attesa di ottenere il nulla osta o di siglare l'accordo con i sindacati. Per evitare sanzioni, le telecamere devono quindi essere montate solo ed esclusivamente dopo aver ricevuto l'autorizzazione.

Garante Privacy: attenzione ai solleciti preregistrati nelle attività di recupero crediti

Attenzione ai solleciti preregistrati. A causa della riservatezza della comunicazione la banca non può effettuare il recupero crediti mediante telefonate preregistrate, a meno che non sia in grado di garantire che le sue comunicazioni giungano solo al destinatario o a persone da questi autorizzate. L'Autorità per la privacy ha dato ragione a un cittadino, titolare di un contratto di finanziamento con una banca, che aveva segnalato di aver ricevuto dall'istituto di credito telefonate preregistrate con solleciti di pagamento.

Dall'istruttoria del Garante è emerso che il sistema utilizzato dalla banca per il recupero crediti non garantiva affatto l'accertamento dell'identità di colui che rispondeva alla chiamata, esponendo così l'interessato a una possibile violazione della riservatezza nel caso le informazioni venissero conosciute da altri. L'Autorità ha dunque ritenuto illecito il trattamento dei dati personali nelle modalità effettuate e lo ha di conseguenza vietato.

Il Garante ha ricordato, in base a quanto stabilito dal provvedimento generale in materia, che chiunque effettui un trattamento di dati personali nell'ambito di un'attività di recupero crediti deve "astenersi dal comunicare ingiustificatamente a soggetti terzi (familiari, coabitanti, colleghi di lavoro o vicini di casa) rispetto al debitore informazioni relative alla condizione di inadempimento nella quale versa l'interessato".

Il Garante ha inoltre prescritto alla banca, ove la stessa intenda continuare ad avvalersi di forme di comunicazione automatica, di adottare idonei accorgimenti tecnici, basati su forme di autenticazione, come ad esempio l'uso di un codice (ad es. il codice del contratto) rilasciato dalla banca, da digitare sull'apparecchio telefonico per poter ascoltare le comunicazioni preregistrate.

No all'invio di messaggi promozionali senza idonea informativa e libero, specifico consenso

Non si possono inviare messaggi commerciali con finalità promozionali senza aver fornito un'idonea informativa ai sensi dell'art. 13 del D.Lgs. n. 196/2003 (c.d. Codice Privacy) **e senza aver ottenuto un consenso libero e specifico come previsto dagli artt. 23 e 130, comma 2, della predetta norma**. È quanto ribadito dall'Autorità **Garante per la privacy** in un recente **provvedimento** con il quale ha dichiarato illecito il trattamento di dati effettuato da una società in violazione della disciplina rilevante in materia.

La pronuncia dell'*Authority* è intervenuta a seguito della segnalazione con la quale un cittadino aveva lamentato la ricezione, via e-mail, di diversi messaggi promozionali indesiderati da parte di una società che aveva raccolto i suoi dati in occasione dell'attivazione della garanzia relativa all'acquisto di un casco da motociclista. **L'invio dei messaggi era, inoltre, continuato nonostante l'interessato avesse più volte formulato richieste di cancellazione**.

Nel corso dell'indagine era emerso come il consenso alla ricezione di messaggi promozionali era stato ottenuto mediante la sottoscrizione di un modulo in cui era genericamente scritto che "*tutti i nominativi che appongono la firma in calce forniscono l'autorizzazione al trattamento dei dati personali da parte di Evolve S.r.l. Tali dati sono utilizzati sia per l'attivazione della garanzia sia per finalità statistiche e commerciali oltre che per l'invio di materiale pubblicitario e promozionale*".

Oltretutto, all'interno di tale modulo veniva richiesto di fornire numerosi dati personali e informazioni relative alle abitudini di acquisto (potenzialmente atti a definire profili e personalità) **senza essere, però, specificati l'obbligatorietà o meno del conferimento nonché i soggetti o le categorie di soggetti che avrebbero potuto trattarli**.

Alla luce di quanto precede, **il Garante ha dichiarato illecito il trattamento *de quo*** ricordando come le operazioni per finalità commerciali che esulano da quelle necessarie per adempiere ad obblighi contrattuali richiedano la preventiva acquisizione di un libero specifico e documentato consenso. E al riguardo, l'Autorità ha ribadito che non può certo definirsi "*"libero"….il consenso a ulteriori trattamenti di dati personali che l'interessato debba prestare quale condizione per conseguire una prestazione richiesta…Gli interessati devono essere messi in grado di esprimere consapevolmente e liberamente le proprie scelte in ordine al trattamento dei dati che li riguardano, manifestando il proprio consenso per ciascuna distinta finalità perseguita dal titolare (cfr. provv. 24 febbraio 2005, punto 7, doc. web n. 1103045)*".

Videosorveglianza: approfondimento della sentenza di Cassazione 4331/2013

Con la sentenza della Corte di Cassazione sezione penale nr. 4331 del 12.11.2013, depositata in cancelleria il 30 gennaio 2014, torna alla ribalta il dibattito sulla videosorveglianza non solo in materia di lavoro; ma anche in quella più in generale della riservatezza personale diritto garantito dalla stessa Carta Costituzionale.

Il problema della videosorveglianza - che negli ultimi anni è stato sempre al centro dell'attenzione - non si limita alla semplice affermazione di essere spiati continuamente (da occhi indiscreti) stante le numerose telecamere installate, oramai ad ogni angolo di strada, negli androni condominiali, nei supermercati, negli uffici pubblici e privati ecc., quanto il fatto se le telecamere siano state installate secondo le disposizioni previste dalla normativa vigente, dai regolamenti e dai provvedimenti emessi dall'Autorità del Garante ed all'uopo è spontaneo chiedersi: come avviene il trattamento? chi è l'amministratore di sistema e la cui figura rispetta le

disposizioni del provvedimento del Garante e la durata della registrazione?

A tal proposito, la sentenza in commento, chiarisce ovvero stabilisce cosa è lecito e cosa non lo è in materia di installazione di telecamere le quali contribuiscono - per le forze di polizia - ad individuare eventuali reati ed i possibili esecutori degli stessi.

A ciò deve aggiungersi l'ultima trovata circa l'utilizzo di videocamere per prevenire o scoprire infrazioni stradali e quindi installate nei maggiori centri urbani; ottimo escamotage per far cassa da parte dei Comuni.

L'argomento facilmente ci porta a divagare e spostare l'attenzione dalla sentenza della suprema Corte che come già detto contribuisce a chiarire un altro aspetto dell'intera problematica. L'esistenza di telecamere - seppure non funzionanti - non esonera il titolare del trattamento (datore di lavoro o rappresentante legale) da responsabilità circa gli adempimenti preventivi richiesti dall'art. 4 della legge 300/1970. Infatti, l'art. 4 dello Statuto dei lavoratori, rubricato "impianti audiovisivi" così recita: *"E' vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.*

Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.

Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.

Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale."

Ad una più attenta lettura della predetta norma si rileva che essa individua due fattispecie -tra loro diverse- per le finalità di trattamento dei dati.

Per completezza di informazione un breve inciso è qui doveroso. La lett. a) dell'art. 4 del **codice in materia di protezione dei dati personali (d.lgs 30 giugno 2003, n. 196)** stabilisce come *"trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;"*

La prima fattispecie riguarda un controllo intenzionale ovvero sancisce un divieto di utilizzare delle apparecchiature finalizzate al mero controllo dell'attività lavorativa. Il presupposto della vigilanza sul lavoro, ritenuto indispensabile per l'organizzazione produttiva da parte dello stesso datore, è vietato con l'uso di apparecchiature in quanto l'utilizzo improprio delle stesse potrebbe ledere la riservatezza dei lavoratori ed ancor di più la loro autonomia di movimento nello svolgimento del lavoro. Salvo che (seconda fattispecie) il datore di lavoro per motivi di sicurezza anche del personale e per preservare il patrimonio della stessa azienda (organizzazione ed esigenze aziendali) disponga l'installazione di impianto di videosorveglianza previo consenso delle rappresentanze sindacali (ove esistenti) ovvero mediante una autorizzazione amministrativa dinanzi all'Ispettorato Provinciale del Lavoro. Anche in questo caso, considerate le numerose istanze preventive pervenute -negli ultimi tempi- presso gli uffici preposti il citato ente ha inteso bene snellire le procedure autorizzatorie mediante un iter semplificativo.

Infatti, con circolare del 16.04.2012 la Direzione Generale per l'Attività Ispettiva del Ministero del Lavoro e delle Politiche Sociali per i casi in essa descritta (attività economiche a forte rischio) non necessitano di un "accertamento tecnico preventivo

dello stato dei luoghi in quanto sostanzialmente influenti ai fini del rilascio dell'autorizzazione". Ciò significa che con una semplice istanza si potrebbe ottenere il rilascio dell'autorizzazione (senza preventivo sopralluogo) purché corredate da idonea documentazione indicata nella predetta circolare.

In caso di violazione del citato art. 4 legge 300/1970 il datore di lavoro va incontro a tre diverse conseguenze. La prima è di natura penale: ammenda da € 154,94 ad € 1549,37 od arresto da 15 giorni ad un anno (salvo che il fatto non costituisca più grave reato. In questo caso il contravventore -a valutazione del giudice penale- può essere ammesso all'oblazione con conseguente estinzione del reato. La seconda è di natura civile in quanto i dati eventualmente acquisiti impropriamente dal datore del lavoro (registrazione immagini mediante impianto di telecamere) non farebbero testo (ovvero "non hanno valore probatorio") in un eventuale contenzioso con il dipendente ripreso. Infine, la terza è di natura sindacale (art. 28 dello statuto dei lavoratori) allorquando il datore di lavoro non ha rispettato le procedure di preventiva consultazione dei rappresentanti sindacali ove esistenti.

La richiamata sentenza ha trattato una violazione da parte del legale rappresentale di una società (gestore di un supermercato) che aveva installato un certo numero di telecamere alcune delle quali orientate sulle casse senza il preventivo accordo con le rappresentanze sindacali e senza la preventiva autorizzazione dell'ispettorato del lavoro. La pronuncia è da intendersi innovativa in quanto la suprema Corte non ha tenuto conto della difesa del contravventore (il quale dichiarava che l'impianto di videosorveglianza "non era funzionante") perché l'art. 4 dello Statuto dei Lavoratori è comunque violato in quanto ..."l'idoneità degli impianti a ledere il bene giuridico protetto , cioè il diritto alla riservatezza dei lavoratori, sia necessaria affinché il reato sussista emerge ictu oculi dalla lettura del testo normativo - idoneità che peraltro è sufficiente anche se l'impianto non è messo in funzione , poiché, configurandosi come un reato di pericolo, la norma sanziona a priori l'installazione prescindendo dal suo utilizzo o meno".

12/02/2014 *Cordiali saluti*

G.Paolo Morabito