Newsletter
NOTIZIARIO
ANNO XX
WWW.GARANTEPRIVACY.IT

NEWSLETTER N. 439 del 29 marzo 2018

Customer care, no al software di Sky che controlla gli operatori

Il sistema non può essere considerato "strumento di lavoro"

Il Garante per la privacy ha dichiarato illecito [doc. web n. 8163433 (/garante /doc.jsp?ID=8163433)] e ha vietato l´ulteriore trattamento di dati effettuato da SkyItalia senza aver fornito agli operatori di customer care una completa informativa sul funzionamento di un sistema che gestisce le chiamate degli abbonati, e senza aver stipulato uno specifico accordo sindacale.

Dagli accertamenti effettuati dall´Autorità, intervenuta a seguito della segnalazione di una organizzazione sindacale e di alcuni dipendenti addetti al call center, è emerso che il sistema non si limita ad associare, come sostenuto dalla società, la chiamata e l´anagrafica del cliente per facilitare la gestione della richiesta dell´abbonato, ma consente "ulteriori elaborazioni" (memorizzazioni di dati personali degli operatori ed estrazione di report).

Attraverso questo sistema infatti la società è in grado di risalire all´identità del dipendente attraverso l´associazione del "codice operatore" con altre informazioni relative alla sua attività lavorativa (il tipo di operazione svolta, la durata della chiamata, data e orario di termine della chiamata) o mediante l´eventuale incrocio tra informazioni conservate in sistemi separati.

Il software - afferma il Garante - permette di ricostruire anche indirettamente l´attività svolta da centinaia di operatori del call center e rappresenta un sistema di controllo, anche se potenziale e indiretto, dell´attività lavorativa. Oltre alla disciplina di protezione dati il sistema viola anche la disciplina lavoristica sull´impiego di strumenti dai quali possa derivare il controllo a distanza dei lavoratori. Il sistema, contrariamente a quanto affermato dalla società, non può essere considerato uno "strumento di lavoro" per la sola gestione del contatto con il cliente e dunque utilizzato dall´operatore per rendere la prestazione, perché rientra piuttosto - a parere del Garante - tra gli "strumenti organizzativi" per soddisfare esigenze organizzative e produttive del datore di lavoro dai quali può derivare il controllo a distanza dei lavoratori. E, data la loro invasività, prima di impiegare questi strumenti la società avrebbe dovuto attivare tutte le procedure previste dallo Statuto dei lavoratori (accordo sindacale o in mancanza di questo autorizzazione delle direzioni territoriali del lavoro), procedure che non sono state espletate. Tutto ciò senza che la società avesse fornito ai dipendenti una informativa completa e dettagliata sulle effettive modalità e finalità delle operazioni di trattamento rese possibili dall´applicativo.

L´Autorità si riserva di valutare con un autonomo procedimento l´applicazione di sanzioni amministrative per gli illeciti riscontrati.

Lavoro: vietato il controllo massivo e la conservazione illimitata delle email

Attraverso l´accesso ai contenuti delle email ricostruito lo scambio di comunicazioni, anche private, tra i lavoratori

No al controllo massivo e alla conservazione senza limite delle email. Il Garante per la privacy ha vietato ad una società il trattamento di dati personali effettuato sulle email aziendali dei dipendenti in violazione della normativa sulla protezione dei dati e di quella sulla disciplina lavoristica. La società dovrà ora limitarsi a conservare i dati a fini di tutela dei diritti nel giudizio pendente. L´Autorità - intervenuta a seguito del reclamo di un dipendente - ha accertato che la società trattava in modo illecito i dati personali contenuti nelle email in entrata e in uscita, anche di natura privata e goliardica, scambiate dal lavoratore con alcuni colleghi e collaboratori. I dati raccolti nel corso di un biennio erano poi stati utilizzati per contestare un provvedimento disciplinare cui era seguito il licenziamento del dipendente poi annullato dal giudice del lavoro [doc. web n. 8159221] (/garante /doc.jsp?ID=8159221).

Nel disporre il divieto l´Autorità ha rilevato numerose e gravi violazioni. La società non ha infatti fornito ai dipendenti alcuna informazione su modalità e finalità di raccolta e conservazione dei dati relativi all´uso della posta elettronica, né con una informativa individualizzata né attraverso la policy aziendale. Un comportamento in contrasto con l´obbligo della società di informare i lavoratori riguardo alle caratteristiche essenziali dei trattamenti effettuati, comprese le operazioni che possono svolgere gli amministratori di sistema (ad es., accesso ai contenuti delle email). La società, inoltre, conservava in modo sistematico i dati esterni e il contenuto di tutte le email scambiate dai dipendenti per l´intera durata del rapporto di lavoro e anche dopo la sua interruzione, violando così i principi di liceità, necessità e proporzionalità stabiliti dal Codice privacy. La società - afferma l´Autorità - anziché mettere in atto un trattamento così invasivo, avrebbe potuto agire in modo più efficiente e più rispettoso della riservatezza dei lavoratori predisponendo dei sistemi di gestione documentale in grado di individuare selettivamente i documenti che avrebbero dovuto essere via via archiviati. Inoltre - continua il Garante - la conservazione estesa e sistematica delle mail, la loro memorizzazione per un periodo indeterminato e comunque amplissimo nonché la possibilità per il datore di lavoro di accedervi per finalità indicate in astratto (ad es. difesa in giudizio, perseguimento di un interesse legittimo) consente il controllo dell´attività dei dipendenti. Controllo vietato dalla disciplina di settore che non autorizza, anche dopo le modifiche del Jobs Act, verifiche massive, prolungate e indiscriminate. Il datore di lavoro infatti pur potendo controllare l´esatto adempimento della prestazione e il corretto uso degli strumenti di lavoro deve sempre salvaguardare la libertà e la dignità dei dipendenti.

Ingiustificata, in particolare, la raccolta a priori di tutte le email in vista di futuri ed eventuali contenziosi, il Garante ha ribadito infatti che la conservazione deve riferirsi a contenziosi in atto o a situazioni precontenziose e non a ipotesi astratte e indeterminate. Il Garante ha ritenuto, infine, non conforme alla legittima aspettativa di riservatezza della corrispondenza l´accesso della società alle email in ingresso sull´account aziendale dopo il licenziamento del lavoratore. Al cessare del rapporto di lavoro la casella di posta elettronica deve essere disattivata e rimossa e al suo posto di devono attivare eventuali account alternativi.

L´Autorità si riserva di valutare con un autonomo procedimento la contestazione di sanzioni amministrative relative agli illeciti riscontrati.

Trasporto locale: sì a registrazione immagini in caso di sinistri

Via libera del Garante all´installazione di un dispositivo sui mezzi di trasporto di Genova

Il Garante per la privacy ha autorizzato [doc. web n. 8159431 (/garante/doc.jsp?ID=8159431)] L´Azienda Mobilità e Trasporti di Genova (AMT S.p.A.) ad installare sul parabrezza anteriore dei propri veicoli aziendali un dispositivo denominato "Roadscan DTW", in grado di registrare, in caso di incidenti, le immagini relative alla sede stradale prospiciente il veicolo o, su comando attivato dall´autista, le immagini della zona interna del mezzo e di localizzarlo senza riprendere il conducente.

Il sistema permetterà la ricostruzione dinamica di eventuali sinistri e la prevenzione e il contrasto di atti di vandalismo, potenziando la sicurezza dei passeggeri e degli autisti.

Il trattamento potrà essere effettuato solo per le finalità previste e nel rispetto di idonee misure di sicurezza volte a preservare l´integrità dei dati e prevenire accessi abusivi da parte di personale non autorizzato. A tutela dei lavoratori, la società ha concordato con le organizzazioni sindacali l´utilizzo del dispositivo secondo le finalità dichiarate, in base all´art. 4 dello Statuto.

Le informazioni relative alla localizzazione tramite GPS non potranno essere utilizzate per rintracciare on line il veicolo, né per definirne a posteriori il percorso effettuato.

I dati raccolti in occasione di sinistro potranno essere conservati sino a 24 mesi, scadenza del temine di prescrizione previsto dal Codice civile.

La società dovrà adottare un modello semplificato di informativa inglobata in un pittogramma (da collocare su ogni veicolo aziendale), che renda noto agli interessati (utenti, dipendenti e terzi) che in caso di sinistro le immagini saranno registrate.

Garanti Ue: più trasparenza per profilazione e decisioni automatizzate

Profilazione più trasparente, no a decisioni completamente automatizzate che possono produrre effetti giuridici per la persona o che incidano su di essa in modo significativo, pieno riconoscimento e tutela dei diritti e delle libertà degli utenti. Questi in sintesi i principi che ispirano le Linee guida su profilazione e decisioni automatizzate (/regolamentoue/profilazione) adottate di recente dalle Autorità di protezione dati europee alla luce del Regolamento europeo in materia di protezione dei dati personali.

I sistemi di profilazione e i processi decisionali automatizzati trovano impiego in una gamma sempre più ampia di settori pubblici e privati - dalle banche alla sanità, dal fisco alle assicurazioni, dalla pubblicità al marketing – e possono risultare utili per gli individui come pure per la società e l´economia nel suo complesso in termini di incremento di efficienza e risparmio delle risorse. Ma possono comportare rischi significativi per i diritti e le libertà delle persone: oltre ad essere spesso poco trasparenti, questi trattamenti di dati possono confinare una persona all´interno di una determinata categoria limitandone le scelte o suggerendone altre sulla base di quelle già espresse, perpetuare stereotipi, dar luogo a previsioni inesatte, impedire l´accesso a servizi o prodotti e, in taluni casi, causare forme ingiustificate di discriminazione.

Nelle Linee guida le Autorità europee chiariscono le previsioni normative introdotte dal Regolamento in materia di profilazione e decisioni automatizzate, fornendo indicazioni a chi tratta i dati per mettersi in regola con la nuova normativa.

Le società dovranno innanzitutto improntare il trattamento dei dati ai principi di privacy by design e privacy by default e minimizzare il loro uso.

Dovranno poi porre particolare attenzione agli obblighi di trasparenza che il Regolamento Ue attribuisce loro nell´ambito delle decisioni automatizzate. Ciò significa che dovranno informare chiaramente gli utenti sull´attività di profilazione e garantire loro il diritto di conoscere quali dati e quali categorie di dati personali sono stati utilizzati. Per quanto riguarda le decisioni automatizzate i titolari dovranno informare gli utenti sull´esistenza e sulle conseguenze di processi decisionali totalmente automatizzati che possono produrre effetti giuridici per la persona o che incidano su di essa in modo significativo, come, ad esempio, l´eventuale esclusione dal credito sancita da un algoritmo. Alla persona interessata non occorrerà conoscere le formule alla base dell´algoritmo, quanto piuttosto, individuare, in maniera comprensibile i criteri e le modalità di aggregazione dei dati che hanno portato alla sua collocazione in una categoria predeterminata. Ma soprattutto, all´interessato dovrà essere sempre garantito il diritto di ottenere l´intervento umano nella valutazione e di poter contestare la decisione.

Una particolare attenzione è stata richiesta dalle Autorità europee per i trattamenti di dati che riguardano i minori a fronte della loro maggiore vulnerabilità rispetto a trattamenti particolarmente invasivi.

Alle Linee guida, infine, sono allegate alcune raccomandazioni basate sulle "migliori prassi" raccolte negli Stati Membri.

L´ATTIVITÁ DEL GARANTE - PER CHI VUOLE SAPERNE DI PIÚ

Gli interventi e i provvedimenti più importanti recentemente adottati dall´Autorità

- Concluso in Sogei l´incontro del Garante privacy con l´amministrazione finanziaria (/garante /doc.jsp?ID=8162669)

Comunicato del 27 marzo 2018

- Nuovo Regolamento Ue sulla privacy. Online l´aggiornamento 2018 della Guida applicativa (/garante /doc.jsp?ID=8135449)

27 marzo 2018

- Caso Cambridge Analytica. Lettera del Presidente del Garante privacy, Antonello Soro, alla Presidente del Gruppo di lavoro Articolo 29 (/garante/doc.jsp?ID=8069676)

21 marzo 2018

- Regolamento UE. Il Garante per la protezione dei dati personali incontra le Università. A Roma il 6 aprile (/garante/doc.jsp?ID=7977380)

Comunicato del 13 marzo 2018

- Regolamento Ue. Il Garante incontra i Responsabili della Protezione dei Dati (RPD) (/garante /doc.jsp?ID=7917099)

Comunicato del 7 marzo 2018

NEWSLETTER

del Garante per la protezione dei dati personali (Reg. al Trib. di Roma n. 654 del 28 novembre 2002).

Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n. 121 - 00186 Roma.

Tel: 06.69677.2752 - Fax: 06.69677.3755

Newsletter è consultabile sul sito Internet *www.garanteprivacy.it (http://www.garanteprivacy.it/)*