STUDIO NICOLAZZO

Business Tax Legal Consulting

Circolare Privacy del 20 giugno 2022

SOMMARIO

ARTICOLI

Quando è lecito controllare la posta elettronica aziendale di un dipendente senza violare la sua privacy?

Una recente sentenza del Tribunale di Genova, relativa a una dipendente licenziata dopo che il datore di lavoro controllando la sua email aveva scoperto che aveva inviato verso terzi dati riservati, permette di approfondire il tema della liceità delle verifiche sull'email di un lavoratore dipendente anche per scopi difensivi. Si tratta di un tema che rimane sempre di grande attualità e di ampio contrasto tra gli addetti ai lavori rispetto; Non poche, infatti, sono le questioni sorte in merito alla legittimità dell'accesso da parte del datore di lavoro o dirigente alla casella di posta elettronica aziendale del dipendente. Al fine di risolvere tali questioni è opportuno ricordare alcuni importanti concetti:

⇒ l'equiparazione della posta elettronica alla corrispondenza tradizionale la cui libertà e segretezza viene tutelata dall'art. 15 della Costituzione;

⇒ la legittimità del controllo della casella della posta elettronica del proprio dipendente da parte del datore di lavoro alla luce di quanto prescritto dall'attuale disciplina in tema di rapporti di lavoro, compreso lo Statuto dei lavoratori;

⇒ la tutela della privacy alla luce di quanto stabilito dal GDPR.

La problematica non è semplice ed il Garante alla luce dei principi di cui sopra è intervenuto già da tempo con un Provvedimento nel quale ha chiarito che i datori di lavoro pubblici e privati **non possono controllare** la posta elettronica e la navigazione in Internet dei dipendenti, se non in casi eccezionali. Spetta al datore di lavoro **definire le modalità d'uso** di tali strumenti ma tenendo conto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali.

Ma cosa succede nel caso di messaggi inerenti al rapporto di lavoro? Anche in questo caso opera il divieto di controllo?

L'Autorità prescrive innanzitutto ai datori di lavoro di **informare con chiarezza** e in modo dettagliato i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli. Il Garante **vieta** poi la lettura e la registrazione sistematica delle e-mail così come il monitoraggio sistematico delle pagine web visualizzate dal lavoratore, perché ciò realizzerebbe un controllo a distanza dell'attività lavorativa vietato dallo Statuto dei lavoratori (art. 4). Viene inoltre indicata tutta una serie di misure per prevenire la possibilità, prevista solo in casi limitatissimi, dell'analisi del contenuto della navigazione in Internet e dell'apertura di alcuni messaggi di posta elettronica contenenti dati necessari all'azienda.

Il Provvedimento sopra citato **raccomanda** l'adozione da parte delle aziende di un **disciplinare interno**, definito coinvolgendo anche le rappresentanze sindacali, nel quale siano chiaramente indicate le regole per l'uso di Internet e della posta elettronica.

Il datore di lavoro è inoltre chiamato ad adottare ogni misura in grado di prevenire il rischio di utilizzi impropri, così da ridurre controlli successivi sui lavoratori.

In particolare, per quanto riguarda la posta elettronica, è opportuno che l'azienda:

⇒ renda disponibili anche indirizzi condivisi tra più lavoratori (info@ente.it; urp@ente.it), rendendo così chiara la natura non privata della corrispondenza;

⇒ valuti la possibilità di attribuire al lavoratore un altro indirizzo (oltre quello di lavoro), destinato ad un uso personale;

⇒ preveda, in caso di assenza del lavoratore, messaggi di risposta automatica;

⇒ metta in grado il dipendente di delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio, ciò in caso di assenza prolungata o non prevista.

Qualora queste misure preventive non fossero sufficienti a evitare comportamenti anomali, gli eventuali controlli da parte del datore di lavoro devono essere **effettuati con gradualità**.

Può un minore firmare una liberatoria per autorizzare altri ad utilizzare la sua immagine?

Come noto la legge sul diritto d'autore (art. 96 legge 633/41) richiede il consenso quando la persona viene ritratta se il fine del ritratto è l'esposizione in pubblico, lo sfruttamento commerciale e/o la riproduzione. Salvi i casi previsti dall'articolo 97 della legge sul diritto d'autore, per procedere alla diffusione di una fotografia o di un filmato **è sempre necessario il consenso** espresso dei soggetti che vi compaiono e la forma prediletta per il rilascio del consenso è costituita dalla c.d. "liberatoria".

Nel caso dei minori spetta a chi detiene la potestà genitoriale il potere di prestare il consenso affinché l'immagine sia legittimamente utilizzata.

In altri termini il consenso alla pubblicazione delle immagini relative ai minori deve essere **espresso da chi esercita la responsabilità genitoriale** e ai fini del rilascio dell'autorizzazione è generalmente necessario il consenso di un solo genitore.

Particolare attenzione va posta alle coppie separate, come nella sentenza del Tribunale di Mantova, dove nel caso di un genitore separato con affido condiviso, che ha pubblicato le foto del figlio su Facebook senza il consenso dell'altro, ha affermato la necessità del consenso di entrambi i genitori, o meglio che non sussista l'opposizione di uno di essi, per la pubblicazione delle immagini. In un procedimento di divorzio, il Tribunale di Chieti ha, invece, prescritto a entrambi i genitori di evitare la pubblicazione di foto col figlio 17'enne sui profili social, a meno che non abbiano ricevuto l'esplicito consenso del ragazzo.

Ricordiamo che l'articolo 2-quinquies del Codice afferma che il minore che ha **compiuto i quattordici anni** può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione.

Rischio valanga di telefonate commerciali sui cellulari

È l'effetto beffa che potrebbe derivare da una lettura delle norme sul nuovo Registro delle Opposizioni al telemarketing (RPO), che farà il suo debutto entro il **31 luglio 2022**. La novità più esaltata delle disposizioni della legge 5/2018 potrebbe, dunque, trasformarsi in un boomerang per gli utenti, se non si disinnesca una interpretazione suggestiva, che sfrutta alcune incertezze nella formulazione delle norme.

Da un lato abbiamo la tanto attesa estensione ai numeri di cellulare della possibilità di iscrizione nel Registro Pubblico delle Opposizioni (RPO): questo significa che i numeri iscritti **non possono essere chiamati** per scopi di telemarketing, vendite dirette e ricerche di mercato. Dall'altro lato, però, si potrebbe intendere che se il numero di cellulare non è iscritto nel RPO, allora, in virtù della disciplina del RPO, il numero mobile si potrebbe chiamare, anche se il titolare dell'utenza mobile non ha espresso alcun preventivo consenso. Da ciò deriverebbe la regola per cui se il numero di cellulare è iscritto non si può chiamare. Il problema che sta sollevando le discussioni tra gli operatori del settore riguarda, però, i numeri di cellulare che non saranno iscritti.

In sostanza, ci si chiede se, con l'estensione della disciplina del RPO alle utenze mobili, qualunque numero di telefono fisso o mobile non iscritto nel RPO, possa essere liberamente contattato da operatori umani del call center senza bisogno di un previo espresso consenso da parte dell'utente (se e in quanto appunto non iscritto nel RPO).

A sbarrare la strada a questo esito paradossale è, però, una lettura sistematica della legge 5/2018 e del DPR 26/2022 confrontati con gli articoli 129 e 130 del Codice della privacy; In sostanza se non c'è una precedente iscrizione in un pubblico elenco (come avviene per i cellulari), ci vuole sempre il **consenso preventivo** (primo comma dell'articolo 130 codice privacy).

Garante Privacy: no a diffusione di foto lesive della dignità da parte delle questure. Sanzionato il Ministero dell'Interno

Due sanzioni, per complessivi **110mila euro**, sono state comminate dal Garante privacy al Ministero dell'interno per la diffusione da parte di due Questure, nel corso di conferenze stampa, di immagini e video di persone arrestate o detenute, lesivi della loro dignità, senza che la divulgazione fosse giustificata da necessità di giustizia o di polizia.

Nel primo caso, il video, pubblicato su alcuni siti internet e testate giornalistiche mostrava i volti in primo piano e i nominativi di otto persone arrestate e le immagini dei momenti in cui venivano condotte (in questo caso, con il volto coperto) dagli agenti di polizia nelle auto di servizio. Il video, liberamente visibile per oltre 5 anni sul profilo Facebook di una Questura, era stato rimosso dopo l'intervento dell'Autorità.

Nell'irrogare la **sanzione di 60mila euro** per questo episodio il Garante ha ritenuto che, alla luce della normativa nazionale ed europea, e della giurisprudenza della Corte di Cassazione e della CEDU, le immagini, per le caratteristiche dell'inquadratura e la presenza del logo della Polizia di Stato, fossero nella sostanza assimilabili alle foto segnaletiche, pur non avendo i numeri in sovrimpressione; La diffusione delle foto segnaletiche è consentita solo se ricorrono fini di giustizia e di polizia o motivi di interesse pubblico. Nel corso dell'istruttoria invece non è emersa alcuna necessità di divulgare le immagini in questione, in aggiunta alle altre informazioni fornite alla stampa. La Questura è così incorsa in un trattamento non necessario, eccedente e lesivo della dignità della persona.

Nel secondo caso, un'altra Questura ha divulgato alla stampa, sempre senza che ve ne fosse alcuna necessità, le generalità e l'immagine in primo piano di una persona già in carcere per dare la notizia di un ulteriore provvedimento restrittivo emesso nei suoi confronti. Il Garante ha ritenuto illecita anche questa divulgazione di dati personali e ha applicato al Ministero una sanzione pecuniaria di **50mila euro**.

NEWS

Whistleblowing e Privacy: le indicazioni del Garante

PA e imprese **devono prestare la massima attenzione** nell'impostazione e gestione dei sistemi di whistleblowing, garantendo la massima riservatezza dei dipendenti e delle altre persone che presentano segnalazioni di condotte illecite

Il Garante, nella newsletter dell'11 maggio 2022, segnala di aver **sanzionato**, di recente, un'azienda ospedaliera e la società informatica che gestiva il servizio per denunciare presunte attività corruttive o altri comportamenti illeciti all'interno dell'ente (whistleblowing). Dai controlli effettuati presso l'ASL, segnala il Garante, sono emerse diverse violazioni del GDPR. L'accesso all'applicazione web di whistleblowing, basata su un software open source, avveniva attraverso sistemi che, non essendo stati correttamente configurati, registravano e conservano i dati di navigazione degli utenti, tanto da consentire l'identificazione di chi la utilizzava, tra cui i potenziali segnalanti.

Il Garante ricorda che deve essere prestata **massima attenzione** nell'impostazione e gestione dei sistemi di whistleblowing, garantendo la massima riservatezza dei dipendenti e delle altre persone che presentano segnalazioni di condotte illecite.

La struttura sanitaria in questione, peraltro:

- non aveva informato preventivamente i lavoratori in merito al trattamento dei dati personali effettuato per finalità di segnalazione degli illeciti;
- non aveva effettuato una Valutazione di Impatto (**DPIA**);
- non aveva inserito tali operazioni nel **Registro delle attività di trattamento**.

È infine emersa una non corretta gestione delle credenziali di autenticazione per l'accesso all'applicazione web di whistleblowing da parte del Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT), durante la fase di transizione con il suo successore.

Come fare reclamo al Garante Privacy

Ci sono **due modi** con cui un individuo può tutelare e proteggere la propria privacy:

- attraverso un **reclamo al Garante** o
- facendo **ricorso alla magistratura ordinaria**.

Se, per quanto riguarda la prima opzione, può essere svolta singolarmente senza alcun supporto, il ricorso alla magistratura è cosa più complicata che prevede la presenza di un difensore.

Corte di Giustizia UE, via libera alla "Class Action" privacy

La Corte di giustizia dell'Unione europea ha affermato che le associazioni di tutela dei consumatori **possono esercitare azioni** contro lesioni della privacy, anche in assenza di una delega specifica di una persona danneggiata e anche in via preventiva

Via libera alle Class Action privacy. È questo l'effetto della sentenza della Corte di giustizia dell'UE del 28 aprile 2022, resa nella causa C-319/20, che ha affermato che le associazioni di tutela dei consumatori possono esercitare azioni contro lesioni della privacy, anche in assenza di una delega specifica di una persona danneggiata e anche in via preventiva (e cioè indipendentemente da un danno patito da un interessato).

Attacco hacker al sistema informatico degli ospedali Fatebenefratelli-Sacco: cartelle cliniche criptate da un ransomware

Un attacco hacker ai "servizi di base dell'infrastruttura" ha colpito l'intero sistema gestionale del pronto soccorso degli **ospedali Fatebenefratelli e Sacco** (anche le sedi Buzzi, Melloni e le altre 33 territoriali). Fuori uso sono anche il sito dell'Azienda socio sanitaria territoriale. La conferma di un "attacco ai sistemi informatici" è arrivata dalla Regione Lombardia. Negli ospedali, nel frattempo, sono arrivati i servizi di sicurezza informatica delle Aziende socio-sanitarie territoriali, gli specialisti di Aria (l'Azienda regionale per l'innovazione e gli acquisti) e la polizia postale.

Attacco hacker all'Associazione Bancaria Italiana: criptati dati sensibili e chiesto riscatto

Attacco hacker all'Abi, l'Associazione Bancaria Italiana.

Il sito web e la rete interna sono stati violati da un attacco messo a segno dal gruppo ransomware Vice Society. I dati criptati, per i quali è stato richiesto un riscatto come si legge in un annuncio pubblicato dagli stessi pirati informatici, sono stati mostrati online attraverso degli Screenshot e contengono informazioni finanziarie sensibili e documenti riservati tra cui i numeri delle carte di credito, certificati medici e i prospetti di budget dell'associazione, oltre alle timbrature di ingresso e di uscita del personale o, tra gli altri, le specifiche dei dispositivi elettronici messi a disposizione dei dipendenti.

Spid minorenni, limitazioni e privacy per under 14

Anche i minorenni **possono avere lo Spid** per accedere in maniera semplice, veloce e sicura ai servizi online della Pubblica amministrazione.

L'Agenzia per l'Italia digitale (AgID) ha approvato le linee guida operative per far sì che anche i minori usufruiscano di tali servizi in modo sicuro e nella piena tutela dei dati. Tali linee guida prevedono trattamenti e servizi diversificati in relazione all'età dei minori, se over o under 14. Questi ultimi, ad esempio, possono fruire dello Spid solo in forma limitata e sotto lo stretto controllo del genitore. Quindi, possono usare la propria identità digitale solo per i servizi online forniti dalle scuole.

I minori che hanno superato i 14 anni, invece, **possono accedere a più servizi**, come quelli Inps, nell'area riservata, fino al Fascicolo sanitario elettronico o la verifica dei punti patente per i ciclomotori. In ogni caso, devono essere sempre i genitori a richiedere lo Spid per i figli minorenni. Per farlo, dovranno rivolgersi al proprio gestore dell'identità digitale e accedere, con le credenziali di livello 2, al servizio.

L'autonomia del Responsabile del trattamento è fonte di responsabilità diretta

Il Responsabile del trattamento dati gode di un'autonomia propositiva nell'adozione di misure tecniche e organizzative adeguate al livello di rischio, tanto da derivarne una **specifica e diretta responsabilità** nel caso di misure rilevatesi inadeguate. È questo, in sintesi, il contenuto del recente provvedimento del garante (n. 107 del 24 marzo 2022) con cui è stato sanzionato un Responsabile del trattamento a causa dell'accesso abusivo al sistema informatico che gestiva per conto del Titolare.

Telecamere intelligenti nella pubblica amministrazione: la conformità al GDPR passa dalla valutazione d'impatto

Molte amministrazioni comunali stanno valutando, o in molte occasioni hanno già acquistato e installato le c.d. "telecamere intelligenti" tipicamente con funzione di riconoscimento targhe (OCR). Sono tecnologie automatizzate per il trattamento di dati personali su larga scala parecchio invasive dal punto di vista della privacy e che generalmente **necessitano preventivamente di una Valutazione d'impatto** (DPIA), procedura che aiuterà a studiare l'opportuna configurazione in modo da ridurre al minimo gli eventuali rischi per i diritti e le libertà degli interessati.

Registrare una conversazione: in quali casi è lecito e quando no?

Brevemente si possono trarre queste sintetiche conclusioni:

1) se una persona raccoglie e si limita a conservare a **scopo personale** delle registrazioni di conversazioni con terzi, con ciò non viola la normativa;
2) neppure la circolazione entro un ambito domestico configura una violazione;
3) se però, più o meno inavvertitamente, quella persona dovesse, per fare degli esempi, prestare/procurare una o più di tali registrazioni a terzi che magari ne facessero uso in giudizio oppure rendere pubbliche le registrazioni, allora l'esenzione domestica sarebbe oltrepassata e non potrebbe invocarsi.

PILLOLE DI "PRIVACY"

- Videosorveglianza, solo l'8% delle telecamere sono segnalate da un regolare cartello, ma a chi le installa la privacy interessa poco o niente
- Facebook non sa dove finiscono i dati dei suoi utenti: *Secondo un report interno, la società non ha il controllo sulla enorme massa di informazioni che acquisisce e tratta.*
- Google rimuoverà indirizzi e numeri di telefono privati da ricerche: *Il motore di ricerca ha annunciato di aver esteso la possibilità di richiedere che i dati sensibili vengano oscurati dai link di ricerca*
- Ricercatori e case farmaceutiche potranno accedere ai dati sanitari degli europei: *Lo prevede la nuova proposta della Commissione, che però ammette l'uso delle informazioni soltanto per finalità specifiche e senza rivelare l'identità degli individui*
- Facebook dice addio alla geolocalizzazione: *Facebook sta mandando in pensione alcune funzioni basate sulla geolocalizzazione dell'utente: impatto eccessivo sulla privacy a fronte di vantaggi dei quali si può fare a meno.*
- Il docente non può registrare le lezioni senza il consenso degli studenti: *Queste le conclusioni della Cassazione (Ordinanza n.14270/2022) che ha respinto il ricorso di un Docente*
- Il Garante sanziona Uber per complessivi 4 milioni e 240mila euro: *Poca trasparenza nel trattamento dei dati di oltre 1 milione e mezzo di utenti italiani*
- Telemarketing: sanzionata un'azienda per mancato riscontro a un cliente: *sanzione da 20.000,00 euro*
- Recupero crediti non corretto: Garante privacy sanziona una finanziaria: *Il sollecito inviato alla moglie del cliente, sanzione di 10.000,00 euro*
- Email aziendale: il collaboratore esterno ha gli stessi diritti del dipendente: *Il Garante sanziona un'azienda per 50.000 euro*