1. Le responsabilità: sanzioni, risarcimento danni e conseguenze penali

2. Uso dei social e rispetto privacy

3. Uso telecamere e tutela dei dati

Avv. Luca Spaziani

Le responsabilità: sanzioni, risarcimento danni e conseguenze penali

Quali sono i rischi della mancata compliance alla disciplina in materia di protezione dei dati personali?

Rispondere a questa domanda non è semplice, in un contesto caratterizzato da una disciplina nazionale complessa e frammentata, sulla quale il GDPR si è instaurato.

Le conseguenze del mancato adeguamento vanno oltre le sanzioni economiche previste dal Regolamento.

Seppure il GDPR sia direttamente applicabile negli Stati membri, è imprescindibile il suo coordinamento con la disciplina interna.

Le controversie in materia di trattamento dei dati personali sono demandate solo in parte alla competenza dell'Autorità Garante, la quale decide sull'applicabilità delle misure di cui al GDPR, mentre gli aspetti legati al risarcimento dei danni e alle conseguenze penali sono di rispettiva competenza della giurisdizione civile e di quella penale.

Aspetti civilistici:

Per quanto riguarda gli aspetti civilistici, e in particolare il risarcimento del danno, l'art. 82 paragrafo 6 del GDPR stabilisce che **l'unico rimedio esperibile è il ricorso innanzi ai giudici degli Stati membri**:

A questo proposito, dobbiamo ricordare che l'art. 140-bis del Codice per la protezione dei dati (Codice Privacy, D.lgs. 196/2003) stabilisce che **l'interessato**, ove ritenga che i diritti di cui gode sulla base della normativa in materia di protezione dei dati personali siano stati violati, **può scegliere alternativamente** di proporre reclamo al garante oppure di procedere attraverso il classico ricorso giurisdizionale.

Pertanto, alla luce di quanto letto, sembrerebbe che **in Italia la presentazione del reclamo esclude la possibilità di ricorso, e viceversa**.

Ciò non è corretto

Già nel 2017 la Cassazione (Cass. Civ. 13151/2017) ha riconosciuto che **l'interessato** che riceva una decisione favorevole dal Garante **ha la possibilità di agire successivamente in sede civile per il risarcimento dei danni**, e che il provvedimento del Garante ha il valore di una "**prova privilegiata**" per l'accertamento della violazione da parte del giudice.

Ricordiamo che il ricorso al garante è un mezzo gratuito, semplice e veloce per coloro che vogliano mettere in moto la macchina degli accertamenti nei confronti di un titolare o responsabile del trattamento. Infatti, il reclamo può essere presentato compilando un semplice modulo messo a disposizione dallo stesso Garante e inviato a mezzo raccomandata o PEC. Inoltre, il Garante "decide il reclamo entro 9 mesi dalla data di presentazione".

Gli interessati che mirino al risarcimento dei danni, invece, dovranno necessariamente armarsi di un buon avvocato e della pazienza di attendere l'esito di un più costoso, lungo e complesso procedimento civile

Art. 82

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento ***solo se*** *non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.*

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 ***se dimostra*** *che l'evento dannoso non gli è in alcun modo imputabile.*

6. ***Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro***

Considerando 146:

Qualora i titolari del trattamento o i responsabili del trattamento siano coinvolti nello stesso trattamento, ***ogni titolare del trattamento o responsabile del trattamento dovrebbe rispondere per la totalità del danno****.* ***Tuttavia****, qualora essi siano riuniti negli stessi procedimenti giudiziari conformemente al diritto degli Stati membri,* ***il risarcimento può essere ripartito in base alla responsabilità*** *che ricade su ogni titolare del trattamento o responsabile del trattamento per il danno cagionato dal trattamento, a condizione che sia assicurato il pieno ed effettivo risarcimento dell'interessato che ha subito il danno.*

Il titolare del trattamento o il responsabile del trattamento che ha pagato l'intero risarcimento del danno ***può successivamente proporre un'azione di regresso*** *contro altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento*

Aspetti penalistici:

Il Codice Privacy ***(modificato dal D.Lgs 101/2018)*** *prende in considerazione varie fattispecie agli artt. 167 e ss.*

Mettendo per un attimo a lato i reati di cui al 167 e al 167-bis, rispettivamente "Trattamento illecito di dati telefonici" e "Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala", i quali non pongono particolari problemi interpretativi e che in linea di massima potrebbero riguardare, se vogliamo, una ridotta platea di titolari e responsabili (fornitori di servizi), i reati nei quali molti potrebbero inconsapevolmente incorrere sono invece quelli di cui agli artt. 168, 170 e 171 dello stesso Codice Privacy.

In breve, l'art. 168 prevede la pena della ***reclusione*** ***(da 6 mesi a 3 anni)*** *per tutti coloro che, nel corso di un procedimento o di accertamenti posti in essere innanzi al Garante, dichiarino il falso, producano documenti falsi o intenzionalmente cagionino l'interruzione o la turbativa del procedimento in questione*

L'art. 170 del Codice per la protezione dei dati personali rappresenta un'altra sottostimata fonte di pericolo. Esso prevede la pena della ***reclusione*** ***(da 3 mesi a 2 anni)*** *per coloro che non rispettino un provvedimento con cui il Garante dispone la limitazione del trattamento, così come* ***per coloro che trattino dati genetici, biometrici, relativi alla salute, religiosi o sindacali fuori dai casi di cui al 9.2 GDPR (che disciplina i casi in cui il trattamento è autorizzato dall'interessato o necessario)*** *e in conformità alle misure di garanzia disposte dal Garante stesso e stabilisce la stessa pena per coloro i quali, essendovi tenuti, non rispettino "i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163". Tali provvedimenti non sono altro che le 5 Autorizzazioni Generali del Garante sottoposte a verifica e ritenute compatibili con l'odierno impianto normativo, le quali assumono un ruolo diverso rispetto agli altri provvedimenti del Garante, ponendosi come condizioni di liceità del trattamento.*

*In conclusione, ad oggi, anche il mancato rispetto delle previsioni di cui alle Autorizzazioni generali n. 1/2016 (**trattamento dei dati sensibili nei rapporti di lavoro**), n. 3/2016 (trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni), n. 6/2016 (trattamento dei dati sensibili da parte degli investigatori privati), n. 8/2016 (trattamento dei dati genetici) e n. 9/2016 (trattamento dei dati personali effettuato per scopi di ricerca scientifica) può essere fonte di responsabilità penale.*

***Anche gli autorizzati potrebbero incorrere in questo tipo di responsabilità penale**: è fondamentale che gli autorizzati siano adeguatamente formati.*

*Una **menzione particolare** merita **l'art. 171 del Codice privacy (modificato dal D.Lgs 101/2018)**, il quale punisce (con ammenda in lire, fino a 3 milioni: L. 300/70) **eventuali violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori**. Prestino quindi particolare attenzione tutti quei titolari o responsabili che si servono di impianti audiovisivi oppure operino nel mondo del lavoro.*

Uso dei social e rispetto privacy

*Ci sono **4 cose importanti da ricordare**:*

1 – La maggior parte dei social media vengono dagli Stati Uniti e quindi:

a) usano una lingua diversa dalla nostra (in quanto anglosassoni);

b) hanno una concezione della privacy completamente diversa dalla nostra e così, quando andiamo a leggere i termini e le condizioni del servizio o l'informativa privacy di questi strumenti, è facile perdersi.

2 – Bisogna capire quando si applica il GDPR e se vengono fatti dei trattamenti di dati personali di cittadini europei, al di fuori dell'Unione Europea. Per esempio, alcuni social, come MailUp, che si usa per inviare le newsletter, sono in UE. Mailchimp, invece, no.

Stessa funzione, strumento simile, Paese diverso.

3 – Quali sono i soggetti che nella pratica utilizzano i social all'interno dell'azienda.

Quindi non sono tanto i soggetti previsti dal GDPR – titolare, responsabile esterno, interessato – ma, per esempio, sono i dipendenti che inviano le newsletter o quelli che gestiscono la sezione «lavora con noi» del sito.

E quindi è importante capire chi fa cosa all'interno dell'organizzazione aziendale.

4 - La co-titolarità. Nel caso dei social media può succedere che si presenti questa situazione: un gruppo di imprese raccoglie i dati delle stesse persone e invia le newsletter, fa selezione del personale, fa delle promozioni dedicate… e visto che queste aziende comunicano tra loro e si passano questi dati, è bene che regolamentino i loro rapporti definendo se sono co-titolari o responsabili esterni.

Riassumendo,

i titolari del trattamento, prima di utilizzare uno strumento social, devono fare attenzione

a:

1) ***Valutare*** *e* ***scegliere*** *lo strumento social, per capire se è adeguato o meno alle finalità aziendali e garantisce il rispetto del GDPR;*
2) ***Analizzare*** *come vengono trattati i dati personali degli interessati all'interno di questo social;*
3) ***Capire*** *dove vanno (in quale paese) e con chi vengono condivisi questi dati;*

Uso telecamere e tutela dati

L'attività di videosorveglianza *(Art. 4, L. 300/70) è consentita se sono rispettati i seguenti principi:*

deve essere lecita*: funzionale allo svolgimento delle funzioni istituzionali in caso di enti pubblici, rispettosa degli obblighi di legge in caso di enti privati, oppure se vi è un consenso espresso da parte delle persone riprese;*

deve essere necessaria*: limitata ai soli casi nei quali l'obiettivo non può essere raggiunto con diverse modalità;*

deve essere proporzionata*: l'uso di telecamere deve costituire la misura ultima di controllo, idonea soltanto quando altre misure si sono rilevate insufficienti o inattuabili;*

deve avere una finalità*: i sistemi di videosorveglianza possono essere predisposti solo per specifiche finalità di propria competenza (come il controllo della propria attività) e non per finalità esclusivamente di sicurezza pubblica.*

L'installazione di impianti di sorveglianza in ***ambienti privati*** *è del tutto libera e non necessita di alcuna autorizzazione, a condizione che* ***le telecamere (compresi i videocitofoni) non inquadrino spazi collettivi o luoghi di passaggio pubblico****. Inoltre, qualora il sistema utilizzato conservi* ***le riprese effettuate****, queste* ***non potranno essere in alcun modo diffuse****.*

Nel caso in cui il sistema di videosorveglianza sia installato in un ***ambiente pubblico o all'interno di un'azienda****, sopraggiungono* ***diversi obblighi****, tra cui* ***l'obbligo dell'informativa*** *ovvero la necessità di informare gli interessati della presenza di una zona sorvegliata con cartelli espliciti, comprensibili e sempre visibili.*

Informativa

Il supporto con l'informativa deve avere 3 caratteristiche:

1) *Deve essere collocato **prima del raggio di azione della telecamera**;*
2) *Deve avere un **formato ed una posizione** tale da essere **visibile in ogni condizione ambientale, anche quando il sistema sia attivo in orario notturno**;*
3) *Deve includere un **simbolo di esplicita e immediata comprensione**.*

Verifica preliminare

*Il Garante ha stabilito inoltre che deve essere effettuata una **verifica preliminare**, attivata d'ufficio o a seguito di un interpello del titolare, **quando vi sono rischi specifici per i diritti e le libertà fondamentali in relazione alla natura dei dati, alle modalità di trattamento e agli effetti che questo può determinare**.*

La verifica preventiva deve essere obbligatoriamente effettuata anche su tutti i sistemi di videosorveglianza dotati di software che dispongono di riconoscimento facciale e di associazione dei dati biometrici e sui sistemi intelligenti che sono in grado di rilevare automaticamente comportamenti o eventi anomali.

*La mancata o incompleta notificazione al Garante è punita con una **sanzione amministrativa dai 10.000 ai 60.000 €** come previsto dall'art. 163 del Codice Privacy.*

Raccolta, conservazione e cancellazione dati

***Tutti i dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza**, per ridurre il rischio di perdita, distruzione (anche accidentale) e soprattutto l'accesso di persone non autorizzate agli stessi.*

*Devono essere inoltre predisposte **misure organizzative per la cancellazione** dei dati alla scadenza o dei dati non più necessari.*

***Le riprese possono essere conservate per un massimo di 24 ore e in alcuni casi specifici è ammesso il prolungamento dei tempi fino a 7 giorni**. Per i Comuni e nelle ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, la conservazione dei dati è consentita fino a 7 giorni successivi alla rilevazione, fatte salve specifiche esigenze.*

Il titolare o il responsabile del trattamento dovrà segnalare per iscritto tutte le persone che sono autorizzate ad accedere ai locali in cui sono situate le postazioni di controllo, ad utilizzare gli impianti e, nel caso fosse necessario, a visionare le immagini.

Sanzioni

Per quanto riguarda le sanzioni il Codice Privacy (art. 162-ter, co. 2) prevede sanzioni da € 30.000,00 ad € 180.000,00

GRAZIE PER L'ATTENZIONE !

Avv. Luca Spaziani