La conservazione dei dati al tempo del GDPR

Il principio di limitazione dei tempi di conservazione dei dati personali è stato incluso nel Regolamento UE 679/2016 (il c.d. GDPR) ed è ribadito in diversi punti del Regolamento stesso. Ad esempio, al considerando 39 troviamo scritto:

"…Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati."

Tale principio prevede delle eccezioni, anche quando l'interessato ha esercitato il diritto all'oblio; al considerando 65, infatti, troviamo scritto*:"… Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archivia¬zione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria."*

La limitazione della conservazione dei dati personali è un obbligo in capo al Titolare del trattamento, ma anche al Responsabile (cfr. considerando 81: "*Dopo il*

completamento del trattamento per conto del titolare del trattamento, il responsabile del trattamento dovrebbe, a scelta del titolare del trattamento, restituire o cancellare i dati personali salvo che il diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento prescriva la conservazione dei dati personali.").

Il principio di limitazione alla conservazione è comunque esposti in maniera tassativa all'articolo 5 (**Principi applicabili al trattamento di dati personali**), punto c), quando il GDPR ci informa che i dati personali sono: "*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trat¬tati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attua¬zione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»)*;".

I limiti temporali di conservazione dei dati personali sono citati anche all'articolo 6 (**Liceità del trattamento**), relativamente al fatto che la **base giuridica** del trattamento potrebbe regolamentare anche i tempi di conservazione.

Il **periodo di conservazione** massimo (ovvero il termine per la cancellazione dei dati personali) **deve essere anche documentato**, come ci indica l'articolo 13 – relativamente alle informazioni da fornire all'interessato, ovvero la c.d. "Informativa privacy" – al comma 2 a): "*il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;*".

Infine, all'articolo 30 (**Registri delle attività di trattamento**), il GDPR impone di documentare – al comma 1 f) – "*ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;*".

Se da un lato il principio di limitare la conservazione dei dati personali allo stretto necessario per espletare le finalità del trattamento è abbastanza chiaro e se ne comprende la ratio, non fosse altro che per il fatto che una conservazione eccessiva di archivi di dati personali espone tali dati a maggiori rischi di perdita di riservatezza degli stessi, dall'altro non è sempre facile soddisfare "alla lettera" tale principio.

Passati i primi tempi di attuazione del GDPR, nei quali molti hanno indicato nelle informative (peraltro sollevando diversi dubbi – anche da parte di chi scrive – sulla correttezza dell'affermazione) che i dati personali sono conservati per il tempo necessario a completare il trattamento per il quale ne è stata prevista la raccolta, si è iniziato a porsi parecchi interrogativi. Vediamo quali.

Relativamente ai dati del personale dipendente di un'azienda, chiaramente i dati relativi alle buste paga, al versamento dei contributi e tutte le evidenze di aver adempiuto a tutti gli obblighi di legge da parte del Datore di Lavoro è corretto che vengano mantenuti per 10 anni dopo la rescissione del rapporto di lavoro. Viceversa, come ci si deve comportare relativamente a tutte le registrazioni presenti in azienda relative alle attività svolte dal dipendente e dalle sue competenze? Mi riferisco a schede di formazione del personale o attestanti le specifiche competenze; registrazioni di attività, verifiche e controlli svolti, partecipazioni a riunioni; redazione, verifica ed approvazione di documenti emessi e così via. Per non parlare della **posta elettronica**: se la casella di posta elettronica personale deve essere disattivata appena possibile dopo l'interruzione del rapporto contrattuale del dipendente o collaboratore con l'azienda (è utile impostare un inoltro delle e-mail in ingresso verso altra casella, con risposta automatica al mittente comunicando che la persona non è più in forza all'azienda, ma non tutti lo fanno), che ne sarà degli archivi di posta elettronica?

Qui si apre un altro problema: gli archivi di posta spesso contengono informazioni di business, oltre a dati personali di dipendenti, collaboratori, persone che rappresentano clienti e fornitori (effettivi o potenziali) ed applicare un criterio di *retention* massima a tutta la posta potrebbe causare la perdita di informazioni importanti. Questo problema è spesso dovuto alle cattive abitudini delle aziende di conservare i documenti e le informazioni di business negli archivi di posta elettronica anziché impiegare **sistemi di gestione documentale** e **applicativi gestionali specifici** (CRM, software pe la gestione dei progetti, applicativi di *issue & bug tracking/management* nello sviluppo software, sistemi di *ticketing* per gestire le richieste di assistenza, ecc.). In tal caso il problema è organizzativo, non è la privacy che impone regole strane poco gestibili!

Cancellare selettivamente dalle e-mail le informazioni relative ad un numero circoscritto di persone fisiche è comunque infattibile con gli strumenti attualmente disponibili. Dunque che ne è dei **diritti alla cancellazione** dei propri dati personali esercitabili dall'interessato? In questo caso forse chi ha scritto il Regolamento ha mancato di senso pratico e tuttora nessuno ha pubblicato delle linee guida al riguardo.

Da un punto di vista strettamente teorico è possibile soddisfare la richiesta di un cliente (più probabilmente un privato) che chiede la cancellazione dei propri dati dagli archivi aziendali: fatti salvi gli obblighi di conservazione dei dati relativi a fatture ed ordini per adempiere ad obblighi contabili e fiscali, potrebbe essere semplice cancellare i dati del cliente nell'anagrafica del gestionale e/o del CRM. Ma come si fa a cancellare i dati personali del cliente da tutta la documentazione prodotta internamente e presente in altri archivi del *file system*, all'interno di file di Office, compresa la posta elettronica? Al momento non credo ci siano applicazioni in grado di gestire una cancellazione così selettiva, tenendo anche presente che nei documenti aziendali sono presenti dati personali di uno o più soggetti interessati, ma anche altre informazioni di business. Non sarebbe dunque

opportuno cancellare un documento, magari recente, perché contiene i dati personali di una persona che ha esercitato il diritto all'oblio; infatti si cancellerebbero anche altre informazioni importanti. Viceversa, la cancellazione specifica dei soli dati personali dell'interessato (ad esempio sostituendoli con la stringa "XXXXX") non è praticabile in modo automatico su grandi moli di documenti con i software a disposizione oggi.

Sempre relativamente ai dati personali dei clienti i termini di cancellazione potrebbero essere giustamente allungati dal titolare del trattamento per cautelarsi a fronte di richieste di risarcimento danni, anche da parte di terzi, contenziosi o indagini dell'Autorità Giudiziaria. In buona sostanza per poter dimostrare di aver svolto il proprio compito con diligenza e rispettando le regole. Infatti, al di là dei tempi di prescrizioni previsti dalla legge, in certi settori – ad esempio quello delle costruzioni o quello sanitario – potrebbe essere necessario garantire la bontà del proprio operato per parecchi anni dopo lo svolgimento del servizio.

In certi casi la conservazione dei dati oltre il periodo strettamente necessario potrebbe costituire semplicemente un vantaggio per l'interessato. Ad esempio nel settore della sanità privata, se escludiamo i dati sanitari relativi a ricoveri ed interventi chirurgici – per i quali la legge prevede la conservazione a tempo illimitato -, il fatto di conservare gli esiti di un esame svolto presso la struttura sanitaria potrebbe costituire un indubbio vantaggio per il paziente che si reca nella medesima struttura per svolgere nuovamente il medesimo esame o altri esami o visite di controllo per i quali sarebbe utile disporre delle informazioni relative all'anamnesi del paziente: l'eventuale smarrimento del referto passato da parte dell'interessato potrebbe non essere deleterio per lo stesso paziente. Certamente, in questo caso aumentano i rischi di perdita di riservatezza dei dati personali (appartenenti a particolari categorie di dati), ma quale principio deve prevalere? Il rispetto della privacy o il servizio al cliente? In assenza di una legislazione specifica che imponga limiti di cancellazione determinati o consenta la conservazione per periodi lunghi dei dati personali la scelta resta difficile.

Nel settore del *direct-marketing*, poi, la presenza di dati personali in un CRM o in una *mailing-list* per l'invio di *newsletter* potrebbe costituire un trattamento illecito di dati personali senza il consenso dell'interessato o in assenza di altre basi giuridiche per il trattamento. Fermo restando l'obbligo di consentire la cancellazione dalla *mailing-list* ad ogni invio di comunicazioni, quanto tempo possiamo mantenere i dati nel nostro database per l'invio di newsletter commerciali? Per sempre se l'interessato non esprime la volontà di non ricevere più comunicazioni? Quando cessa di essere valida la finalità del trattamento in oggetto?

Per le attività promozionali legate alle *fidelity card* esistevano – prima del GDPR – dei provvedimenti del Garante italiano che fissavano i limiti di conservazione dei dati e delle relative campagne promozionali in due anni, salvo deroghe concesse in settori particolari.

Come citato all'inizio del presente articolo, tali regole si applicano anche a chi opera come Responsabile del Trattamento secondo l'articolo 28 del GDPR, ma quanti consulenti del lavoro cancelleranno i dati dei dipendenti di un proprio cliente (Titolare del Trattamento) dagli archivi del proprio applicativo per la gestione delle paghe una volta che si è interrotto il rapporto di collaborazione?

Come si può intuire da quanto esposto finora il problema non è solo **definire i limiti di conservazione temporale** dei dati personali, ma anche **attuare i criteri stabiliti**.

Dal punto di vista informatico non so quali software sono in grado di cancellare selettivamente i dati in base ad un determinato criterio di conservazione? Probabilmente alcuni applicativi non permettono neanche la cancellazione di una scheda anagrafica per problemi di "integrità referenziale" (se cancello un'anagrafica di una persona si dovrebbero cancellare anche tutte le informazioni dipendenti legate alla medesima anagrafica, ma ciò non sempre è opportuno per evitare di cancellare altre informazioni necessarie). Sicuramente chi svilupperà i programmi software che gestiscono dati personali dovrà considerare anche questo aspetto legato alla privacy, nelle specifiche che renderanno il prodotto "privacy by design".

In generale la necessità di dover soddisfare un determinato criterio di cancellazione dei dati comporta l'adozione di criteri di archiviazione delle informazioni, sia in digitale, sia su supporto cartaceo, adeguati di conseguenza. Facciamo un semplice esempio per chiarire meglio il concetto.

Se un'impresa conserva le fatture emesse ai clienti nel fascicolo della commessa, dove la commessa si può protrarre per diversi anni, oppure le conserva nella cartella del cliente, si troverà in difficoltà quando si tratterà di cestinare le fatture più vecchie di 10 anni. Dovrà andare a cercare le fatture in tutte le cartelle delle commesse o del cliente per ricercare i documenti obsoleti!

Viceversa, l’impresa che archivierà le fatture in ordine cronologico, per anno di competenza, potrà più agevolmente distruggere (non gettare nei rifiuti in modo indiscriminato) i documenti relativi ad ogni anno di competenza.

Chiaramente il GDPR è entrato in vigore quando le organizzazioni di ogni tipo avevano già impostato criteri di “*data retention*” ed ora si trovano a dover gestire il principio di limitazione del periodo di conservazione dei dati personali anche sul passato. Naturalmente il Regolamento non dice nulla sull’applicabilità di questo principio anche sui dati già presenti negli archivi delle organizzazioni titolari del trattamento al momento dell’entrata in vigore del Regolamento.

Indubbiamente ci sarebbe estremo bisogno di chiarimenti sui criteri di conservazione da adottare per i dati personali al tempo del GDPR, in primis da parte del nostro Garante per la Protezione dei Dati Personali (si ricorda che si attende ancora la nomina del nuovo Garante Privacy da parte del Governo, in quanto il mandato precedente è già scaduto), poi anche da parte delle istituzioni europee.