CONSERVAZIONE DEI DATI: CRITERI E CRITICITÀ (NELL'INCERTEZZA NORMATIVA)

Articolo di Monica Perego Ingegnere (Gaiani Grinzato Avvocati) 12 Settembre 2019

Non esistono, al momento, criteri ufficiali volti a stabilire in modo uniforme modalità e tempi di conservazione dei dati personali. In assenza di altre soluzioni proviamo a fornirli, con le criticità che portano con sé, alla luce dell'esperienza maturata nel settore e sulla base dell'analisi di molteplici contesti.

Il periodo di conservazione dei dati personali – cosiddetta ***data retention*** – è uno degli elementi basilari della protezione dei dati. È pertanto di fondamentale importanza stabilire bene quali siano i "criteri" per la determinazione del periodo massimo di conservazione dei dati personali, e le conseguenti criticità.

Criteri volti a **stabilire in modo uniforme modalità e tempi di conservazione secondo parametri ufficiali** la cui definizione spetta all'Autorità garante che dovrebbe inoltre sollecitare i vari portatori di interesse (associazioni di categoria, ordini professionali) a fornire **indicazioni** che possano fungere da base comune per la definizioni di prassi condivise e che riducano il libero arbitrio.

Che cosa si intende per data retention

Precisiamo anzitutto che cosa si intenda per "*data retention*", e come nasca l'esigenza di stabilire un **periodo di conservazione** oltre il quale i dati personali debbono essere cancellati.

Per "*data retention*" si deve intendere, appunto, il "*periodo di conservazione dei dati*". Il Regolamento UE n. 679/2016 (**GDPR**), non ha previsto sostanzialmente nulla di nuovo rispetto al Codice Privacy (D.lgs. 196/2003) il quale già contemplava, all'art. 11, che i dati personali dovessero essere: "*conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati*", per quanto non ne richiedesse la comunicazione esplicita all'interessato.

La esigenza di stabilire un periodo di conservazione dei dati, invero, nasce in materia normativa sui sistemi di gestione, che trova una declinazione specifica nell'ambito della **sicurezza delle informazioni** (cfr. ISO/IEC 27001). Si tratta, infatti, di un **tempo conservativo,** come lo è richiesto ad esempio per i **dati di backup**[1].

I principi sottesi

- **Principio della limitazione della conservazione**

Ai sensi e per gli effetti di cui all'art. 5, paragrafo 1 lett. e) il Regolamento stabilisce **il principio della limitazione della conservazione** secondo cui, l'arco temporale nel quale i dati possono essere, dal Titolare del trattamento, conservati deve essere rapportato alle finalità specifiche per le quali sono stati raccolti.

- **Principio di minimizzazione**

Dal combinato disposto di cui agli artt. 5 e 6 del GDPR cioè a dire dalle condizioni di liceità e finalità –che, si rammenta, devono essere determinate, esplicite e lecite- nei limiti di quanto necessario per il raggiungimento dello scopo per i quali i dati sono stati raccolti, nasce il *principio di minimizzazione* del trattamento**.** Si tratta di una delle fondamenta dell'intero impianto normativo stabilendo come i dati debbono essere: **adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.**

Tipologia di archivi e conservazione dei dati: aspetti e modalità

I dati sono generalmente conservati in archivi che si distinguono in **cartacei** ed elettronici.

In questa sede si ritiene utile approfondire **la conservazione di dati in archivi automatizzati concepiti per contenerli/conservarli e non certo per cancellarli.** Al di là del fatto che il vero problema del dato informatizzato risieda proprio nella sua impossibilità ontologica di essere completamente distrutto[2].

In pratica, non è possibile garantire una cancellazione/distruzione completa a differenza di come avviene con il **dato cartaceo** il quale può essere completamente distrutto nel trita-documenti, ad esempio.

Conservazione dei dati: criteri e criticità

Come noto, il periodo di conservazione dei dati è uno degli elementi innovativi che il Regolamento ha imposto di indicare, con evidenza, ora nella informativa (art. 13) ora nel registro (art. 30). Con la precisazione che con riferimento alle informazioni di cui all'art. 13 paragrafo 2 lett a) occorre indicare "…*il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo*".

È pertanto di fondamentale importanza stabilire bene quali siano i "criteri" per la determinazione del periodo massimo di conservazione dei dati personali. Sebbene, ad oggi, non ci siano (ancora) **criteri ufficiali** emanati dall'Autorità sul tema, **in assenza di altre soluzioni, per una corretta gestione dei dati sotto il profilo della durata, intendiamo fornirli alla luce dell'esperienza maturata nel settore e sulla base dei molteplici contesti analizzati[3].**

Orbene, per la definizione dei tempi/criteri è fondamentale l'apporto delle Associazioni di categoria, degli Ordini professionali ovvero di quei soggetti che più di altri conoscono le esigenze di (quel specifico) settore (di riferimento) in grado di fornire gli elementi tutti indispensabili per un corretto bilanciamento.

Criteri che portano con se, inevitabilmente, alcune criticità.

Ma andiamo con ordine.

Per il computo del periodo di conservazione dei dati occorre tenere conto dei seguenti canoni:

- **degli obblighi di legge** (normative nazionali ed internazionali);
- delle p**ronunce giurisprudenziali**-provvedimenti dell'Autorità ovvero delle indicazioni fornite dalle Associazioni di categoria, linee guida per le PA[4], o altri soggetti in grado di fornire elementi che facilitino la conservazione;
- dei **contributi apportati dalla dottrina;**
- dalla **casistica** che pone al centro la tutela dell'interessato[5], e la salvaguardia dei contenuti degli archivi storici[6].

Il tutto deve essere fatto in ossequio al principio di minimizzazione succitato.

Per supplire, poi, alle **carenze ed alle lacune normative si può ricorrere alla estensione analogica** atta a disciplinare casi equipollenti e non regolamentati, applicando norme previste per fattispecie similari.

Ancora.

Corre d'obbligo precisare che **il periodo di conservazione non deve essere confuso con il tempo di prescrizione** quale estinzione di un diritto che l'avente diritto non esercita entro il termine di legge, a seconda del settore di riferimento. Non a caso il termine prescrizionale scorre per la proposizione di azioni giudiziarie (qualunque esse siano). La difesa in giudizio costituisce, sì un elemento ulteriore per la valutazione in ordine alla categorie di atti, con una più alta probabilità di coinvolgimento in contenziosi[7], ma non deve essere il criterio madre che stabilisca fino a quando i dati potranno/dovranno essere tenuti.

Tale inciso consente di dire che non sia più sostenibile conservare dati/informazioni/etc, in forza del "*non si sa mai*".

Infine, da segnalare che la ISO/IEC PRF 27552 "*Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*", la cui pubblicazione è, ad oggi, prevista per luglio 2019, non fornisce alcun criterio a riguardo, mentre il tema della cancellazione/distruzione dei dati è ovviamente richiamato sia nei requisiti dello standard, che come punto di controllo.

Di seguito, si delineano due tabelle –a titolo esemplificativo – che riportano l'una i criteri enunciati ed alcune delle possibili criticità; l'altra alcuni esempi con i relativi tempi di conservazione.

Le suddette indicazioni oltre che essere a titolo esemplificativo vanno apprezzate nella misura in cui i tempi (ivi indicati) potrebbero subire allungamenti qualora i dati stessi – o le informazioni- fossero oggetto di indagine, o impugnazione.

Qualche ipotesi di riferimento per settore

Nel settore del **marketing**, quanto mai coinvolto nella pratica di cui si discorre, con specifico riferimento alle comunicazioni commerciali si palesa erroneo il binomio "*cancellazione dati/riduzione delle vendite*". Non è corretto infatti associare ciò poiché tutti i dati devono poter essere cancellati. Tutti i dati hanno una "scadenza" nel senso che essi debbono essere trattati per lo stretto necessario in termini di finalità e tempi. Al riguardo, si richiama il provvedimento[9] del Garante italiano che, in materia, ha stabilito – predeterminandoli- i tempi di conservazione in **24 mesi** dalla registrazione.

Nel settore delle **risorse umane**, circa la selezione del personale, senz'altro molto sentita è la problematica relativa alla conservazione dei dati, nei DB aziendali, delle candidature ricevute sulla base o delle posizioni aperte, o in modo spontaneo. Per una corretta conservazione occorre che l'Azienda informi il candidato che, per l'utilizzo dei suoi dati personali ai sensi del Regolamento (UE) 679/2016 e del novellato D.Lgs. 196/2003, l'aspirante candidato provveda all'aggiornamento della candidatura entro 45 giorni; in difetto (trascorsi i 45 giorni), si dovrà procedere alla cancellazione dei dati. Ne consegue che detti tempi di conservazione sarà il Titolare del trattamento a deciderli in relazione alla ricezione spontanea del CV.

L'Azienda, in ogni caso, dovrebbe provvedere alla cancellazione – con distruzione dei CV- dei dati (aggiornati) nel momento in cui la posizione/fase di selezione si concluda. A tutto concedere, l'Organizzazione potrebbe conservare il curriculum vitae del candidato non selezionato, ma non oltre i 6 mesi da quella selezione. Al riguardo, una precisazione si impone. Tale periodo di tempo (sei mesi) dipende dalla posizione da selezionare. I tempi di conservazione del CV di un *addetto alla movimentazione* potrebbero essere maggiori di quelli di un *social media marketing* la cui (ultima) posizione potrebbe aver la necessità di aggiornamento CV con frequenza notevole[10].

Nell'ambito della **posta elettronica dei dipendenti**, il provvedimento n. 53/2018 del Garante, ha sanzionato la conservazione *sine die* dei messaggi. L'Organizzazione conservava, in modo sistematico, i dati esterni ed il contenuto di tutte le email scambiate dai dipendenti per l'intera

durata del rapporto di lavoro e anche dopo la sua interruzione, giustificando questo comportamento con finalità generiche (interesse legittimo, necessità di difesa in giudizio).

Sul punto, si riporta il link al citato **provvedimento** del Garante in materia, che tratta, al punto paragrafo? (ci sono troppi punti) 3.2 la tematica relativa alla conservazione dei dati[11].

Si evidenzia quindi la necessità di dotarsi di un **sistema di gestione documentale** che consenta la separazione dei messaggi di carattere lavorativo, contabile in virtù dell'art. 2214 c.c. (conservazione per 10 anni, come prescritto dall'art. 2200 c.c.) da quelli meramente personali, in modo da consentire la rimozione della casella di posta del dipendente alla cessazione del rapporto di lavoro.

Procedura di gestione, conservazione ed eventuale distruzione

Poiché in questa sede, sono stati sinora illustrati **generici criteri di conservazione** a prescindere dal tipo di archivio, mette ora in conto evidenziare che alcuni contesti, a rilevante impatto privacy, è d'uopo predisporre una "*politica di conservazione dei dati*" (cd *Data Retention Policy*) e, conseguentemente, una "procedura di conservazione dei dati" recante indicazioni operative sulle modalità di conservazione e quindi sui **tempi massimi** di conservazione dei documenti generati e/o custoditi dalla Organizzazione di riferimento, contenenti dati di natura personale ed identificativa, anche particolari, relativi agli Interessati al trattamento (dipendenti e collaboratori, clienti – anche potenziali-, fornitori, utenti di siti web, eccetera).

La procedura costituisce un valido strumento di ausilio per conservare i dati personali trattati nel rispetto dei principi suindicati e per assicurare che il tempo di conservazione sia proporzionale alla realizzazione degli scopi per i quali tali dati siano stati raccolti. Il che consente di conservare unicamente quanto mantenga un rilievo giuridico o abbia assunto valore storico, eliminando invece la documentazione non più utile.

Circa il **contenuto** della *policy*, una volta stabiliti i principi, calati nel contesto, essa dovrà contenere, almeno:

- la **modalità** di comunicazione e/o diffusione della *"politica di conservazione dei dati"* provvedendo alla sua comunicazione all'interno dell'Organizzazione e oggetto di formazione per gli autorizzati e di successivo audit. Il Titolare del trattamento potrà altresì diffondere tale documento o estratti dello stesso pubblicandolo su piattaforme web a di lui dominio onde porla a conoscenza di tutti gli interessati;
- il **sistema di controllo** tramite il quale per ogni ufficio/area funzionale i soggetti designati (interni, ove presenti) dovranno controllare periodicamente, ad esempio avvalendosi di uno scadenzario, la presenza di dati archiviati il cui periodo di conservazione sia giunto allo scadere e quindi si imponga la cancellazione, ovvero la conservazione per quei dati da dover tenere illimitatamente. Il tutto al fine di gestire, in maniera ordinata e sistematica, gli archivi permettendo di conservare solo i dati considerati necessari;
- **la prassi per la cancellazione dei dati**, intendendosi per essa la distruzione materiale o tecnica sufficiente per rendere i dati/le informazioni contenute in un o supporto non più recuperabili con gli ordinari mezzi disponibili in commercio. Il Titolare del trattamento è tenuto ad adottare dei metodi di distruzione concordati ed approvati con i tecnici o meglio *process owner*, utilizzabili per ogni tipo di informazione archiviata su supporti elettronici/multimediali (come chiavette USB ed altri tipi di supporti mobili, *devices*, drive portatili o database registrati o copie di back-up, archivi in *cloud*, eccetera);
- **la modalità di diffusione della policy** provvedendo alla sua pubblicazione sulla rete aziendale intranet, se presente, ovvero tramite affissione in bacheca poiché sia visibile a chiunque vi abbia interesse, ed in particolare alle persone autorizzate. Il Titolare del trattamento potrà altresì pubblicare tale documento o estratti dello stesso anche su piattaforme web a di lui dominio onde porla a conoscenza di tutti gli interessati;

- le prassi da rispettare per limitare la duplicazione dei dati e degli archivi contenenti dati anche su supporti diversi;
- **le modalità di comunicazione** verso i Responsabili che trattano dati per conto del Titolare e che, a secondo dello specifico trattamento, i quali dovrebbero o meglio mettiamo devono aver ricevuto le istruzioni in merito alla cancellazione/distruzione/restituzione dei dati trattati per conto del Titolare, l'applicazione di tali procedure potrebbe anche essere oggetto di audit da parte di quest'ultimo[12].
- **l'indicazione delle sanzioni** ogniqualvolta non vengano rispettate le misure suddette potendo, tale violazione, comportare: sospensione o revoca dell'accesso individuale ai sistemi informatici o agli archivi dell'Azienda, relative procedure disciplinari e talvolta, in determinate circostanze, finanche azioni legali.

Traccia procedurale

Si fornisce ora una traccia per la stesura di una procedura di conservazione dei dati.

La presenza di una procedura per la gestione della conservazione ed eventuale distruzione della documentazione è una **misura organizzativa** nonché di *accountability* importante per garantire il presidio di questo aspetto; essa potrebbe essere parte del Modello Organizzativo Privacy.

Di seguito, ci si limita ad illustrare **i capisaldi della procedura per la gestione dei soli archivi cartacei**, in quanto quella relativa a quelli informatici oltre che ad essere molto complessa, presente delle peculiarità a seconda delle tecnologie utilizzate; il che richiederebbe un approfondimento tecnico ultroneo alle odierne finalità.

La procedura in questione per tutto il ciclo di vita di un archivio dovrebbe prevedere:

- **la gestione delle quattro fasi di creazione, consultazione, archiviazione, distruzione**;
- **il luogo di conservazione/archivio fisico** e, laddove necessario, la gestione dell'accesso in forma controllata, col che tale procedura andrebbe integrata con altra relativa alla gestione delle chiavi e dei *badge* per l'accesso ai locali o agli archivi contenenti tali archivi;
- la **responsabilità** sotto la quale viene conservato l'archivio (funzione/area/ufficio);
- le **misure** messe in atto onde evitare il danneggiamento o la perdita dei documenti dovuti al rischio di eventi quali allagamento/umidità, incendio, presenza di roditori, eccetera.

Si dovrebbero poi indicare i tempi/criteri di conservazione che devono essere congruenti con quelli riportati nel registro del trattamento (ex art. 30 Reg. UE) e nella informativa (ex artt. 13 e ss cit Reg). Senza dimenticare che lo stesso documento potrebbe essere conservato in archivi diversi o sotto differenti responsabilità durante il suo ciclo di vita. Ad esempio, l'informativa fornita ad un dipendente all'atto dell'assunzione, potrebbe avere un luogo di conservazione/archiviazione alternativo nel caso in cui il dipendente sia o meno in servizio presso l'Organizzazione.

La procedura potrebbe anche regolamentare il caso dell'archiviazione presso un fornitore esterno che fornisce servizi di gestione documentale.

La procedura deve quindi specificare **responsabilità e tempi** per la distruzione dei dati che implichino le modalità con cui questo deve avvenire. L'eventuale ricorso a soggetti esterni come potrebbero essere i centri che erogano servizi di distruzione dei dati con l'accortezza che siffatta distruzione venga verbalizzata con la conseguente gestione nella conservazione del verbale stesso, attestante la distruzione.

Resta un problema aperto

l vero problema alla base di questa tematica concerne la difficoltà di provvedere alla cd "*cancellazione mirata*" ovvero di quell'aspetto che risponderebbe da un lato all'obbligo di

conservare solo per il tempo strettamente necessario i dati personali. Per fare ciò occorrerebbero soluzioni "integrate", nonostante i limiti di processo. Ad esempio, nella gestione delle e-mail è impossibile non fare affidamento sulla correttezza dei dipendenti alla "***cancellazione mirata***" in particolare per quanto concerne l'archiviazione informatizzata.

Non appare affatto agevole riuscire ad identificare cosa cancellare/distruggere. Infatti, cancellare in modo mirato è, talvolta, assai complicato. Si pensi ad esempio, all'ipotesi di backup contenenti dati/informazioni che di fatto sono "congelati" ed, in quanto tale, restano *ad libitum*.

In conclusione

Ne consegue, pertanto, che l'opportunità di basarsi su criteri che, come detto in principio, non sono ufficiali, ma dettati da anni di esperienza e ragionevole buon senso, da un lato evidenziano il perché non sia possibile generalizzare per casi specifici in quanto innumerevoli sono le variabili, dall'altro dimostrano come siano una ulteriore misura di *accountabilty* attraverso la quale il Titolare "…***chiede all'interessato di dargli fiducia***".[13]

Questa è la (nuova) *data protection* di cui la *data retention* è, senz'altro, uno degli elementi fondanti.[14]

---

1. Nel senso di "…arco di tempo in cui un backup è disponibile per il ripristino ovvero per quanto tempo i dati salvati andranno conservati prima di essere cancellati" cit. ↑
2. Lo stesso discorso potrebbe vale con riferimento all'esercizio dei diritti dell'interessato si discute sulla praticabilità del diritto all'oblio (on line) ex art. 17 che, a tutto concedere, consente la deindicizzazione del dato *rectius* informazione senza contare che questa potrebbe sì non più comparire in un portale, ma non è da escludersi che la stessa possa comparire in un altro; e via discorrendo. ↑
3. Peraltro, sono state fornite puntuali risposte a seguito di istanze preliminari. A mero titolo esemplificativo citasi la valutazione dell'Autorità di controllo in ordine alla verifica preliminare in relazione alla conservazione di dati personali riferiti alla clientela per finalità di profilazione e di marketing diretto – 22 maggio 2018. ↑
4. Nella fattispecie, il Gruppo di lavoro per la formulazione di proposte e modelli per la riorganizzazione dell'archivio dei Comuni ha elaborato il "*piano di conservazione selezione e scarto*", del 2005. ↑
5. L'individuazione delle casistiche richiede necessariamente una profonda conoscenza del processo che genera il dato (oggetto del trattamento) e che prevede la sua successiva gestione fino alla cancellazione/distruzione. ↑
6. Si veda D.lgs. 10 agosto 2018, n. 101 – Art. 2-*sexies* (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante), comma 2 "*2. Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:… cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale* (Sistan);…". Inoltre, sempre nel citato decreto di armonizzazione che ha riformato il Cod. Privacy alla lettera "…c) l'articolo 99 è sostituito dal seguente: «*Art. 99 (Durata del trattamento). – 1. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati*". Ulteriori indicazioni in merito

sono fornite nel D.lgs 22 gennaio 2004, n. 42 “Codice dei beni culturali e del paesaggio, ai sensi dell’articolo 10 della legge 6 luglio 2002, n. 137” richiamato dal cit 101 cirt. ↑

7. Cfr. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8159221 a mente del quale “*… si osserva che il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose, non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti, posto che tale estensiva interpretazione - avanzata dalla società - risulterebbe elusiva delle disposizioni sui criteri di legittimazione del trattamento (v. artt. 23 e 24 del Codice; si vedano anche i provv.ti 19 marzo 2015, doc. web n. 4039439, 20 febbraio 2014, doc. web n. e 4 giugno 2009, doc. web n. 1629029).* ↑
8. Per completezza, si riporta di seguito il link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069057 che rimanda alla questione sollevata in materia, di recente, dal Garante della Privacy, come da comunicato stampa del 20 dicembre 2018 e pedissequo provvedimento [doc. web n. 9069072]. ↑
9. Cfr. [Doc. web n. 1103045] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1103045 ↑
10. Al riguardo, l’art. 9. del D.lgs 101/18 ha modificato la parte II, del Titolo VIII, del decreto legislativo 30 giugno 2003, n. 196 nel modo che segue: “*1. Alla parte II, titolo VIII, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:a) la rubrica è sostituita dalla seguente: «Trattamenti nell’ambito del rapporto di lavoro»;b) l’articolo 111 è sostituito dal seguente:«Art. 111 (Regole deontologiche per trattamenti nell’ambito del rapporto di lavoro). — 1. Il Garante promuove,ai sensi dell’articolo 2 -quater , l’adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell’ambito del rapporto di lavoro per le finalità di cui all’articolo 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all’interessato.»;c) dopo l’articolo 111 è inserito il seguente:*

    «*Art. 111 -bis (Informazioni in caso di ricezione di curriculum)*
    . — 1. Le informazioni di cui all’articolo 13 del Regolamento, nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento del primo contatto utile, successivo all’invio del curriculum medesimo. Nei limiti delle finalità di cui all’articolo 6, paragrafo 1, lettera b) , del Regolamento, il consenso al trattamento dei dati personali presenti nei curricula non è dovuto. ↑

11. Per comodità di lettura si riporta il provvedimento per esteso. *“3.2. Liceità, necessità e proporzionalità del trattamento. Conservazione dei dati.La conservazione sistematica dei dati esterni e del contenuto di tutte le comunicazioni elettroniche scambiate dai dipendenti attraverso gli account aziendali, allo scopo di poter ricostruire gli scambi di comunicazioni tra gli uffici interni nonché tutti i rapporti intrattenuti con gli interlocutori esterni (clienti, fornitori, enti assicurativi, tour operator), anche in vista di possibili contenziosi, effettuata da soggetti diversi dal titolare della specifica casella di posta elettronica per l´intera durata del rapporto di lavoro e successivamente all´interruzione dello stesso, non risulta altresì conforme ai principi di liceità, necessità e proporzionalità del trattamento (v. artt. 3, 11, comma 1, lett. a) e d) del Codice). La legittima necessità di assicurare l´ordinario svolgimento e la continuità dell´attività aziendale nonché di provvedere alla dovuta conservazione di documentazione in base a specifiche disposizioni dell´ordinamento è assicurata, in primo luogo, dalla predisposizione di sistemi di gestione documentale con i quali - attraverso l´adozione di appropriate misure organizzative e tecnologiche - individuare i documenti che nel corso dello svolgimento dell´attività lavorativa devono essere via via archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile (si veda quanto stabilito dal D.P.C.M. 3 dicembre 2013, recante le Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell´amministrazione*

*digitale di cui al decreto legislativo n. 82 del 2005; parimenti i documenti che rivestano la qualità di "scritture contabili" devono essere memorizzati e conservati con modalità determinate: artt. 2214 c.c.; artt. 43 e 44, d. lgs. 7 marzo 2005, n. 82, "Codice dell´amministrazione digitale"). I sistemi di posta elettronica, per loro stessa natura, non consentono di assicurare tali caratteristiche.Pertanto lo scopo di predisporre strumenti per l´ordinaria ed efficiente gestione dei flussi documentali aziendali può ben essere perseguito - conformemente alle disposizioni vigenti oltre che più efficacemente - con strumenti meno invasivi per il diritto alla riservatezza dei dipendenti e dei terzi, rispetto alla sopra descritta attività di sistematica ed estesa conservazione delle comunicazioni elettroniche, che risulta pertanto non necessaria né proporzionata rispetto allo scopo.[OMISSIS] Resta fermo altresì che in relazione alle attività di raccolta e conservazione necessarie a consentire le operazioni di trattamento da parte dell´interessato, il titolare è tenuto ad osservare quanto stabilito dall´Autorità con il citato Provvedimento 27 novembre 2008 sugli amministratori di sistema. Si rammenta che l´Autorità si è pronunciata sulle condizioni di liceità di alcuni trattamenti di dati tratti dall´utilizzo di strumenti di lavoro, tra cui la posta elettronica, per finalità di sicurezza dei sistemi e di gestione dei servizi (v. Provv. n. 303 del 13.7.2016, doc. web n. 5408460, spec. par. 4.2., 4.3. e 5, anche con riferimento ai tempi di conservazione, con il quale sono stati indicati tra i "sistemi e le misure che […] consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore" i "sistemi di logging per il corretto esercizio del servizio di posta elettronica, con conservazione dei soli dati esteriori, contenuti nella cosiddetta "*envelope" del messaggio, per una breve durata non superiore comunque ai sette giorni*"). ↑*

12. Si rimanda a testi specifici che trattano del sistema di gestione privacy per comprendere l'utilità di tale strumento V sul punto il manuale "*Privacy & Audit. Tipologia, pianificazione e processo. Comunicazione e valutazione. Audit e situazioni particolari*" (di Emegian F. e Perego M., IPSOA-Wolters Kluwer, Milano 2015, nonché nella versione aggiornata 2017 e 2018 con i riferimenti al REG EU 2016/679 e 5^ edizione in corso di pubblicazione) ↑
13. Cit. eloquente del Prof. Pizzetti all'VIII Edizione del Privacy Day Forum -Pisa, 19.06.2019. ↑
14. NDR Si ringraziano alcuni dei Professionisti del Gruppo "*idraulici della privacy*" che hanno effettuato un'analisi critica sul pezzo.