DDL Cybersicurezza e tutela dei lavoratori, in rapporto al Gdpr

Home > Sicurezza Digitale

Il DDL Cibersicurezza si sovrappone in parte al GDPR, richiedendo una stretta collaborazione tra i referenti per la cybersicurezza e i responsabili della protezione dei dati. Implica anche la necessità di bilanciare i controlli cyber con il rispetto della privacy e delle norme lavoristiche, evidenziando l'importanza di sistemi di controllo adeguati e la gestione dei metadati nel rispetto delle normative sulla privacy

Pubblicato il 17 mag 2024

Luca Antonetto
Consigliere e Coordinatore Comitato Studi AODV231

Titolo: Il nuovo DDL Cybersicurezza e l'interazione con il vigente quadro regolatorio in materia *data protection*, anche a tutela dei lavoratori.

Autori: Avv. Luca Antonetto (Consigliere e Coordinatore Comitato Studi AODV[231]), Avv. Edoardo Lombardo, LL.M. in Law of IT, CIPP/E (Membro Commissione IA – Consiglio dell'Ordine Avvocati di Torino)

1. **Premessa.**

Questo contributo segue il precedente articolo https://www.agendadigitale.eu/sicurezza/nuovo-ddl-cybersicurezza-gli-enti-e-la-compliance-231/

Il nuovo DDL Cybersicurezza, approvato il 25 gennaio 2024, attualmente in corso di esame dalle Commissioni riunite Affari Costituzionali e Giustizia della Camera dei Deputati, porta con sé novità rilevanti per garantire un più immediato intervento dell'Agenzia per la Cybersicurezza Nazionale ("ACN") per prevenire attacchi e mitigare le conseguenze, garantendo il rapido ripristino delle funzionalità dei sistemi informatici. Tali nuovi obblighi si sovrappongono agli adempimenti già previsti in ambito *data protection* e in capo alla pubblica amministrazione.

Si segnalano, in particolare:

1) **l'obbligo di segnalazione e notifica per determinati soggetti pubblici.**

Le pubbliche amministrazioni centrali, con le rispettive società in-house, le Regioni e le Province autonome di Trento e Bolzano, i comuni con una popolazione superiore ai 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore ai 100.000 abitanti e le aziende sanitarie locali, dovranno segnalare

tempestivamente all'ACN, e in ogni caso entro 24 ore dalla scoperta dell'incidente, fornendo una notifica completa entro 72 ore dalla stessa data.

gli incidenti informatici subiti aventi impatto su reti, sistemi informativi e servizi informatici. Il mancato rispetto di tali obblighi potrà comportare sanzioni per importi che variano da 25.000 a 125.000 euro. Per i dipendenti delle pubbliche amministrazioni, la violazione di queste disposizioni può comportare responsabilità disciplinare e amministrativo-contabile.

2) **La convocazione del Nucleo per la Cybersicurezza.**

Questo nucleo, che potrebbe includere rappresentanti della Procura nazionale antimafia e antiterrorismo, della Banca d'Italia e altri attori, potrà essere convocato per affrontare le questioni più cruciali riguardanti la cybersicurezza nazionale.

3) **L'individuazione di un referente per la cybersicurezza.**

Questo professionista, che dovrà essere nominato in seno alle Pubbliche Amministrazioni, avrà il compito di seguire l'iter parlamentare per l'approvazione definitiva della legge, garantendo così un'implementazione efficace e tempestiva delle nuove disposizioni e dovrà essere basata sulle "qualità professionali possedute", evidenziando l'importanza di competenze e esperienze specifiche nel campo della sicurezza informatica. Tale figura sarà, inoltre, il punto di contatto unico dell'amministrazione con l'Agenzia per la Cybersicurezza Nazionale.

2. **DDL Cybersicurezza e il GDPR.**

La possibile sovrapposizione tra i nuovi obblighi per la pubblica amministrazione in materia di *cybersecurity* e la vigente normativa *data protection* è rilevante.

Rispetto agli obblighi di notifica ricordiamo, infatti, che l'art. 33 GDPR prescrive che il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, notifichi la violazione al Garante per la protezione dei dati personali ("*Autorità Garante*") a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Così come previsto dalla normativa *data protection*, l'inosservanza di tali obblighi può comportare una sanzione pecuniaria rilevante anche con il nuovo DDL Cybersicurezza. Nei casi di reiterata inosservanza dell'obbligo di notifica, infatti, l'ACN potrà applicare, al pari del Garante, una sanzione amministrativa pecuniaria stabilita, in questo caso, da euro 25.000 a euro 125.000.

Se è pur vero che non tutti gli incidenti di sicurezza comportino violazioni di dati personali, è vero il contrario: pertanto sarà necessario che le pubbliche amministrazioni prevedano procedure di gestione delle violazioni di dati personali che coinvolgano anche il nuovo referente per la cybersicurezza, a cui vengono conferiti poteri e responsabilità molto simili a quelli del responsabile per la protezione dei dati ("DPO") ai sensi dell'artt. 37-39 GDPR. Si ritiene, pertanto, utile che sia previsto un continuo flusso informativo tra i due soggetti, per garantire il migliore rispetto di entrambe le norme.

Con tale nuovo assetto di *governance* saranno coinvolte, così, entrambe le funzioni che fungono da punto di contatto, il primo dell'ACN, e il secondo del Garante per la Protezione dei Dati personali.

Infine, non si può non considerare l'impatto del DDL Cybersicurezza rispetto al dettato dell'art. 32 GPDR "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*" consenta all'Autorità Garante di individuare nel complesso normativo europeo e nazionale descritto lo stato dell'arte applicabile alle pubbliche amministrazioni italiane, laddove non siano già norme direttamente applicabile, evidenziando la necessità di procedere con certificazioni in ambito di

cybersecurity come quella adottata recentemente dalla Commissione Europea su proposta dell'ENISA, al di là delle note certificazioni ISO (27001 e altre).

3. **La recente Giurisprudenza Europea rilevante.**

L'importanza delle misure di sicurezza si rivela sempre più centrale anche rispetto ai possibili rischi risarcitori, verso dei soggetti interessati e coinvolti nella violazione, che si sommano ai rischi sanzionatori già trattati.

A proposito è importante considerare la recente decisione della CGUE nella causa C. 340/21, che ha, di fatto, ampliato il possibile perimetro di responsabilità del titolare del trattamento che, qualora non adotti misure di sicurezza adeguate, anche in possibile violazione delle norme in materia di *cybersecurity* analizzate, si troverebbe a dover rispondere anche di eventuali danni immateriali in favore dell'interessato, al di là delle note sanzioni amministrative.

Nel caso in esame, la ricorrente proponeva, in sede civile, un'azione di risarcimento del danno contro «NAP» (autorità collegata al Ministero delle finanze bulgaro) in ragione della violazione dei dati subìta da quest'ultima. A fondamento di tale richiesta, il timore che i dati della ricorrente possano essere oggetto di utilizzo abusivo.

La Corte ha sancito i seguenti punti di diritto:

1) La divulgazione o l'accesso non autorizzato a dati personali da parte di «terzi» non sono sufficienti, di per sé, per ritenere che le misure tecniche e organizzative attuate dal titolare, ai sensi degli articoli 24 e 32 del GDPR, non sono «adeguate»: l'adeguatezza di dette misure deve infatti essere sempre valutata in concreto dai giudici nazionali.

2) Nell'ambito di un'azione di risarcimento fondata sull'articolo 82 del GDPR, sul titolare incombe l'onere di dimostrare l'adeguatezza delle misure di sicurezza attuate ai sensi dell'articolo 32. La mera perizia in sede giudiziaria, in ogni caso, non può costituire un mezzo di prova sistematicamente necessario e sufficiente in tal senso.

3) Il titolare non può essere esonerato dall'obbligo di risarcire il danno subito da una «persona» per il solo fatto che tale danno deriva da una divulgazione o da un accesso non autorizzati a tali dati da parte di «terzi». Egli deve infatti dimostrare che il fatto che ha provocato il danno in questione non gli è in alcun modo imputabile.

4) Il timore nutrito dall'interessato circa un potenziale utilizzo abusivo dei propri dati personali da parte di terzi a seguito di una violazione può, di per sé, costituire un «danno immateriale» risarcibile.

La sentenza chiarisce il concetto di «danno immateriale» risarcibile, contenuto nell'art. 82 del GDPR, ricomprendendovi anche il semplice timore di un utilizzo abusivo dei dati personali oggetto di violazione.

Considerando, quindi, che la risarcibilità del danno non risulta subordinata al fatto che l'utilizzo abusivo dei dati si sia effettivamente concretizzato, il titolare che subisca un *data breach* si espone non solo al rischio di sanzioni comminate dal Garante o dall'ACN, ma anche a quello di azioni risarcitorie di facile attivazione (richiedendo queste ultime solo la prova della fondatezza di detto timore) esperibili dai titolari dei dati davanti al giudice nazionale.

4. **L'esigenza di controlli cyber in ambito giuslavoristico e i controlimiti dettati dalle norme *data protection*.**

L'esigenza di controlli, funzionale all'applicazione di appositi sistemi disciplinari, è immanente alla *ratio* preventiva avanzata[1], e coessenziale all'impianto giuridico, della disciplina della responsabilità

[1] In effetti, lo "*scopo delle cautele* [dei modelli organizzativi] *è di agire sull'ipotizzato meccanismo di produzione dell'evento impedendo il verificarsi di accadimenti, prodromici rispetto all'evento lesivo, che rappresentano 'sotto-eventi' dei decorsi causali tipici …*" (così, per tutti, LUNGHINI, *L'idoneità e l'efficace attuazione dei modelli organizzativi ex D.Lgs. 231/2001*, in *I modelli organizzativi ex D.Lgs. 231/2001 - Etica d'impresa e punibilità degli enti*, Milano, 2005, p. 265.)

"*amministrativa*" delle società e degli enti, come rivelano l'art. 6 del d.lgs. 231/2001, in generale, e, in particolare, il successivo art. 7, co. 3., per cui "*Il modello prevede, …., misure idonee … a scoprire ed eliminare tempestivamente situazioni di rischio*", nonché l'art. 30, co. 4, del d.lgs. 81/2008, per cui "*Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo …*". Tale essenziale esigenza propria di tutto il «sistema 231», riguarda vieppiù la prevenzione dei delitti informatici e degli altri reati di matrice informatica, rafforzata dal nuovo DDL Cybersicurezza.

La stessa esigenza è implicata dal dettato del GDPR, in generale, nonché, in particolare, dall'art. 32, con l'imposizione di misure di sicurezza funzionali alla prevenzione dei *data-breach* ex art. 33 GDPR, spesso, se non sempre, congeniti agli attacchi informatici in violazione delle norme in materia di *cybersecurity*, con le conseguenze sanzionatorie e risarcitorie tratteggiate.

Perciò le ultime "*Linee Guida per la costruzione dei modelli …*" di Confindustria, prevedono uno specifico "*sistema di controlli interno all'azienda …*", con, tra l'altro, "*l'adozione di sistemi di logging e monitoring ….*"[2], nel "*rispetto di leggi e regolamenti applicabile alla materia … (Codice in materia di protezione dei dati personali - decreto n. 196 del 2003 - provvedimenti del Garante Privacy, … artt. 4 e 8 della legge n. 300 del 1970, ecc.)*".

Peraltro il contemperamento tra le esigenze di controllo suddette ed il rispetto delle normative da ultimo citate è tutt'altro che agevole da perseguire, come puntualmente rilevato da autorevole dottrina: "*La società che voglia predisporre un Modello Organizzativo per <u>la prevenzione dei reati in commento ha innanzi a sé due distinte esigenze confliggenti fra loro</u>: da un lato, infatti, sta la necessità di predisporre una rete informatica aziendale dotata di un sistema di auditing che preveda la registrazione di file di log delle attività svolte dagli utenti e, dall'altro, il divieto di oltrepassare il livello di controllo oltre il quale si viene a violare la sfera di riservatezza giuridicamente garantita ad ogni singolo individuo … sotto gli aspetti di violazione della privacy e dell'art. 4 dello Statuto dei lavoratori, dovendosi in proposito contemperare due esigenze*[3]*. Tuttavia, nonostante le precauzioni che devono essere adottate* [per] *la tutela della privacy individuale, è certo che <u>la strada del monitoraggio delle attività compiute attraverso il sistema informatico è l'unica possibilità</u> di … risalire all'accertamento delle responsabilità individuali ….*"[4].

In questo contesto - ed in vista del bilanciamento tra esigenze di controllo e rispetto dei diritti dei lavoratori e della *privacy* nei luoghi di lavoro - merita considerare la più recente evoluzione giurisprudenziale in materia di "*<u>controlli difensivi</u>*", cioè dei "*<u>controlli diretti ad accertare condotte illecite del lavoratore</u>*", in quanto tali essenzialmente diversi dal "*controllo riguard*[ante] *(direttamente* o *indirettamente) l'attività lavorativa*" e, perciò, da "*ritenersi certamente fuori dell'ambito di applicazione del …. divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 legge n. 300 del 1970 L. 20/05/1970, n. 300*", come riconosciuto per la prima volta da Cass., Sez. Lav., 03/04/2022, n. 4746.

Tale istituto pretorio è sopravvissuto alla novella dell'art. 4 dello Statuto dei Lavoratori ad opera del *Jobs Act* (art. 23, d.lgs. 151/2015; v. anche art. 5 d.lgs. 185/2016), nonostante le critiche della dottrina e le perplessità della prima giurisprudenza di merito, per cui "*<u>Il nuovo comma 1</u>* [<u>dell'art. 4 Stat. Lav.</u>] *ha esteso espressamente, …, la possibilità di controllo a distanza dei lavoratori anche a tutela «del patrimonio aziendale»; il vecchio testo non* [lo] *prevedeva … Sulla base di ciò la giurisprudenza aveva ritenuto che non fossero compresi nell'ambito dell'articolo 4 i c.d. controlli difensivi*[5]*; ne segue che con l'innovazione del 2015 la disposizione … viene indubbiamente ad ampliare la sua sfera di*

---

[2] "*Il sistema di controllo per la prevenzione dei reati di criminalità informatica dovrà altresì basarsi, ove applicabili, sui seguenti principi di controllo: … tracciabilità degli accessi e delle attività svolte sui sistemi informatici che supportano i processi esposti a rischio …*"

[3] Cfr. anche *Documento di Approfondimento* recentemente pubblicato da AODV231, con la collaborazione di Deloitte Legal, su "*La prevenzione dei reati informatici: rischi 231, data protection e misure di compliance*", p. 34

[4] SANTORIELLO, *I reati informatici dopo le modifiche apportate dalla legge 48/2008 e la responsabilità degli enti*, in *Resp. Amm. Soc. e enti*, 2011.

[5] - cfr. Cass., Sez. Lav., 28 maggio 2018, n. 13.266; id., 10 novembre 2017, n. 26.682; id., 2 maggio 2017, n. 10.636; id., 8 novembre 2016, n. 22.662.

operatività, pur rimanendo controverso se residuino spazi per la persistente esclusione … dei c.d. controlli difensivi …."[6].

In effetti "*la questione della «sopravvivenza» dei «controlli difensivi» nel regime normativo fissato dalla nuova formulazione dell'art. 4 St. lav.*" è stata positivamente risolta da Cass., Sez. Lav., 22/09/2021, n. 25.732, distinguendo "*tra i controlli a difesa del patrimonio aziendale che riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della loro prestazione di lavoro che li pone a contatto con tale patrimonio, controlli che dovranno necessariamente essere realizzati nel rispetto delle previsioni dell'art. 4 novellato in tutti i suoi aspetti, e «controlli difensivi» in senso stretto, diretti ad accertare specificamente condotte illecite ascrivibili …. a singoli dipendenti, anche se questo si verifica durante la prestazione di lavoro*", e concludendo, in esito ad articolata argomentazione, "*che questi ultimi controlli, anche se effettuati con strumenti tecnologici, non avendo ad oggetto la normale attività del lavoratore, si situano, anche oggi, all'esterno del perimetro applicativo dell'art. 4.*".

Il tutto, peraltro, a ben precise condizioni: **i)** che ci si trovi "*in presenza di un fondato sospetto circa la commissione di un illecito*"; **ii)** che "*il controllo «difensivo in senso stretto»* [sia] *mirato, nonché attuato ex post, ossia a seguito del* [predetto] *illecito*"; **iii)** che "*sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlati alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore*"; **iv)** che "*il controllo riguardi* [esclusivamente] *dati acquisiti successivamente all'insorgenza del sospetto*"[7]. Quest'ultimo limite esclude, *a contrario*, "*l'esame e l'analisi di informazioni precedentemente assunte in violazione delle prescrizioni di cui all'art. 4 St. Lav. …*", perché altrimenti "*il datore di lavoro … potrebbe, in difetto di autorizzazione e/o di adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, nonché senza il rispetto della normativa sulla privacy, acquisire per lungo tempo ed ininterrottamente ogni tipologia di dato provvedendo alla relativa conservazione e, poi, invocare la natura mirata (ex post) del controllo …*".

Questo orientamento di legittimità - con i predetti stringenti limiti - è stato confermato da Cass., Sez. Lav., 12/11/2021, n. 34.092[8], con specifico riferimento al controllo dei "*file di log*" e da Cass., Sez. Lav., 26/06/2023, n. 18.168, vera e propria *summa* della materia, con una importante precisazione, restrittiva, circa "*la nozione di «fondato sospetto»*", da intendersi come "*indizi, materiali riconoscibili, non* [come] *espressione di un puro convincimento soggettivo … perché solo la sussistenza di essi costituisce riscontro oggettivo dell'autenticità dell'intento difensivo del controllo*". Sul piano processuale tali elementi devono essere oggetto di specifica "*allegazione e prova che devono riguardare anche circostanze temporalmente collocate*"[9].

La somma di questi principi è stata puntualmente recepita in due recentissime sentenze del Tribunale del Lavoro di Roma – nn. 1869 e 1870 del 14 febbraio 2024 - per dichiarare la nullità di due licenziamenti disciplinari (di dirigenti) irrogati per fatti dei quali il datore di lavoro aveva dedotto di essere "*venuto a conoscenza … in seguito ad una segnalazione anonima*", ma in realtà poi risultati "*precedenti a tale segnalazione ed ai conseguenti accertamenti, sicché (in base ai principi di legittimità sopra riportati) già sotto tale profilo … inutilizzabili ai fini disciplinari*", in quanto avvenuti con "*un illecito accesso alla corrispondenza*" elettronica dei lavoratori, "*in contrasto con il reg. UE 679/2016 e con la legge sulla «privacy» …*".

5. **L'esigenza nel trattare i metadati dei dipendenti per esigenze di cybersicurezza.**

Ci si chiede, pertanto, come correttamente bilanciare le esigenze derivanti dalle norme in materia *cybersecurity*, che imporrebbero di aumentare l'attività di monitoraggio e di controllo, sia per di

---

[6] così, per tutte, App. Roma, Sez. Lav., 15/05/2018, n. 1997

[7] non essendo per converso ammissibile

[8] a fronte un paio di altre pressoché coeve pronunce, apparentemente più «liberali» (Cass., Sez. Lav., 12/11/2021, n. 33.809; id., 09/11/2021, n. 32.760

[9] "*atteso che le stesse segnano il momento a partire dal quale i dati acquisiti possono essere utilizzati nel procedimento disciplinare e, successivamente, in giudizio, non essendo possibile l'esame e l'analisi di informazioni precedentemente assunte in violazione delle prescrizioni di cui all'art. 4 St. lav. …*"

preservare l'infrastruttura informatica, sia per l'esigenza di prevenzione dei reati presupposto, con i limiti di cui allo Statuto dei Lavoratori e le previsioni del GDPR.

Come è noto, il Garante ha recentemente emanato il provvedimento di indirizzo denominato "*Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati*" sulla base dei poteri riconosciutigli ex art. 57, par. 1. lett. b) del GDPR e art. 154-bis, comma 1, lett. a) del Codice Privacy.[10]

Ricordiamo che l'Autorità ha rispettivamente il compito di: 1) promuovere la consapevolezza e la comprensione del pubblico, dei titolari e dei responsabili riguardo a norme, obblighi, rischi, garanzie e diritti stabiliti dal Regolamento; 2) adottare linee guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del GDPR, anche per singoli settori e in applicazione dei principi di cui all'art. 25 GDPR. Sotto questo secondo profilo, il mancato rispetto del documento di indirizzo potrebbe, dunque, far scattare, oltre le autonome violazioni relative allo Statuto dei Lavoratori, anche la violazione del 25 del GDPR, proprio per il tramite dell'art. 154-bis del Codice. (testualmente: "*In considerazione del richiamato quadro giuridico, l'impiego dei predetti programmi e servizi di gestione della posta elettronica, in assenza dell'espletamento delle procedure di garanzia di cui all'art. 4, comma 1, della l. n. 300/1970, prima di dare avvio alla preventiva e sistematica raccolta dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti, e alla conservazione degli stessi per un ampio arco temporale (superiore a sette giorni estensibili di ulteriori 48 ore, alle condizioni indicate al par. 3), si pone in contrasto con la normativa in materia di protezione dei dati personali e con la richiamata disciplina di settore, in violazione degli artt. 5, par. 1, lett. a), 6 e 88, par. 1, del Regolamento, nonché 114 del Codice (in relazione all'art. 4, comma 1, della l. n. 300/1970).*"). Alla luce di quanto sopra, sorgono dunque "*conseguenti responsabilità sul piano sia amministrativo che penale*".

In particolare, sono di grande rilevanza i seguenti tre passaggi del documento:

1) "*per scelta espressa del legislatore, solo gli strumenti preordinati, anche in ragione delle caratteristiche tecniche di configurazione, alla "registrazione degli accessi e delle presenze" e allo "svolgimento della prestazione" (Art. 4 co.2 St. Lav.) non soggiacciono ai limiti e alle garanzie di cui al primo comma (i.e., accordo sindacale o autorizzazione pubblica) dello Statuto dei Lavoratori in quanto funzionali a consentire l'assolvimento degli obblighi che discendono direttamente dal contratto di lavoro, vale a dire, la presenza in servizio e l'esecuzione della prestazione lavorativa*";
2) "*l'attività di raccolta e conservazione dei soli c.d. metadati necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica, per un tempo che, all'esito di valutazioni tecniche e nel rispetto del principio di accountability – affinché sia ritenuto applicabile il comma 2 dell'art. 4 della L. n. 300/1970* (si veda punto n.1 sopra) *– non può essere superiore di norma a poche ore o ad alcuni giorni, in ogni caso non oltre sette giorni, estensibili, in presenza di comprovate e documentate esigenze che ne giustifichino il prolungamento, di ulteriori 48 ore*".

In attesa dell'esito della pubblica consultazione e rispetto a questo utile passaggio, è doveroso segnalare che non è ancora ben chiaro se l'Autorità intenda riferirsi alla conservazione/trattamento dei soli metadati intesi come una specifica raccolta in forma di database/archivio/organizzazione separata e differente rispetto all'applicativo e-mail. Sembrerebbe di sì, dal momento che si riferisce ai "soli metadati" e che sono previste dalla stessa Autorità *data retention* ben più elevate per la conservazione delle e-mail del dipendente all'interno dei *provider* di posta.

Si ritiene pertanto plausibile ritenere che, in questo caso, l'Autorità intenda limitare la conservazione dei metadati, non quelli inscindibili e presenti all'interno della email e per le quali sono previsti termini di conservazione ben più ampi dei 7 giorni, ma solo se organizzati in forma di archivio

[10] Attualmente l'efficacia del provvedimento è sospesa fino all'esito della pubblica consultazione ritenuta necessaria dalla stessa Autorità.

separato (inteso ai sensi dell'art. 4.6 GDPR, e, cioè, un "*qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico*") e potenzialmente intelligibile a mezzo *software*[11]. Si segnala, inoltre, che da diversi confronti avuti con alcuni dei più grandi fornitori di servizi di posta, sembrerebbe che tali archivi separati siano effettivamente esistenti, intelligibili a mezzo software e prevedano termini di conservazione di circa 6 mesi[12].

3) "*diversamente, la generalizzata raccolta e la conservazione di tali metadati, per un lasso di tempo più esteso – ancorché sul presupposto della sua necessità per finalità di sicurezza informatica e tutela dell'integrità del patrimonio, anche informativo, del datore di lavoro – , potendo comportare un indiretto controllo a distanza dell'attività dei lavoratori, richiede l'esperimento delle note garanzie previste dall'art. 4, comma 1, della predetta L. n. 300/1970*".

Ai più l'intervento dell'Autorità è parso restrittivo, limitante e lontano dalle esigenze del *business*. In realtà, nelle more dei necessari chiarimenti di cui si è già detto e della pendente consultazione pubblica, il Garante espressamente consente, in regime di *accountability*, di estendere il termine di *data retention* individuato per l'attività di raccolta, conservazione e conseguente trattamento dei metadati estratti da un sistema di posta elettronica, ma sarà necessario ottenere un accordo sindacale/autorizzazione dell'ispettorato del lavoro competente. Infatti, il rischio sotteso alla suddetta attività di trattamento è quello di un "monitoraggio sistematico" dei lavoratori, inteso come "*trattamento utilizzato per osservare, monitorare o controllare gli interessati*" e che i dati raccolti per finalità di tutela del patrimonio aziendale, possano essere invece utilizzati per diverse finalità e a nocumento del lavoratore, così come avvenuto nel caso del Provvedimento Regione Lazio[13].

In ogni caso, in sede di bilanciamento dei rischi per gli interessati lavoratori, ben potranno essere evidenziati tutti gli obblighi cui il titolare del trattamento è soggetto (o sarà soggetto) in ambito *cybersicurezza* e/o *compliance* 231.

[11] https://ntpluslavoro.ilsole24ore.com/art/metadati-cloud-computing-privacy-e-controlli-convivenza-conflittuale-AF8zUAmC
[12] https://www.googlecloudcommunity.com/gc/Workspace-Q-A/Gmail-s-metadata/m-p/707907
[13] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9833530