Bollettino ADAPT 13 maggio 2019, n. 18

Il 7 maggio scorso è stata pubblicata la Relazione annuale dell'Autorità Garante della protezione dei dati personali con riferimento all'anno 2018, strumento con il quale, con cadenza annuale, viene fornito al pubblico il resoconto circa l'attività istituzionale complessivamente svolta dall'*Authority* nell'arco di tempo preso a riferimento.

Il presente report, tuttavia, si segnala rispetto ai precedenti per due peculiari motivi: l'uno riferito al fatto che esso costituisce l'ultima Relazione annuale presentata dall'attuale collegio, ora presieduto da Antonello Soro e destinato presto ad esaurire il proprio mandato settennale (le prossime nomine sono previste infatti per giugno prossimo), mentre l'altro legato all'oggetto stesso del report, l'anno 2018 per l'appunto, che ben può essere classificato come il punto di non ritorno in materia di protezione dei dati personali, stante l'entrata in vigore (il 25 maggio 2018) del rivoluzionario Reg. UE n. 2016/679, meglio noto come GDPR (acronimo dell'etichetta anglosassone "*General Data Protection Regulation*"), recepito poi nel nostro ordinamento per il tramite del d. lgs. n. 101/2018 (qui commentato), vigente invece dal giorno 19 settembre scorso e naturalmente pervaso dalla portata dirompente che caratterizza la sua "sorgente" europea, e con il quale è stato modificato il d. lgs. n. 196/2003 (impropriamente noto come "Codice della privacy", d'ora in poi Cod. priv.).

Tra i vari e innumerevoli aspetti approfonditi, spicca naturalmente la materia

dei rapporti di lavoro, la cui complessità la rende intrinsecamente esposta a maggiori rischi relativi alla protezione dei dati personali di diverse categorie di interessati, *in primis* i lavoratori (ma anche utenti, fornitori e terze parti più in generale), e per questo sottoposta alla lente di ingrandimento dell'Autorità, che a tale aspetto riserva l'intero Capitolo n. 13 della Relazione, oggetto del presente commento.

Detto capitolo è inaugurato da alcune considerazioni di carattere generale suscettibili, tuttavia, di dispiegare effetti anche e soprattutto nell'ambito dei rapporti di lavoro, delle quali meritano di essere menzionate, innanzitutto, l'estensione dell'intero tessuto normativo in materia di *privacy* anche ai trattamenti effettuati da datori di lavoro pubblici (cfr. art. 88 e 9, par. 2, lett. *b*), del GDPR); in secondo luogo e con riferimento alle informazioni che il Garante continua a definire "dati sensibili", benchè l'espressione sia stata ormai superata dalla nuova nomenclatura offerta dagli artt. 9 e 10 del GDPR[1], il rinvio al provvedimento 13 dicembre 2018, n. 497 (doc. web n. 9068972), posto in consultazione pubblica, con il quale il Garante ha provveduto ad individuare, in ossequio a quanto sancito dall'art. 21, d.lgs. n. 101/2018, le prescrizioni imposte dall'Autorità stessa nei vari provvedimenti succedutisi in materia di lavoro (e in particolare nella autorizzazione generale n. 1/2016) che sopravvivono al mutato quadro normativo in quanto compatibili con la riforma europea, seppur destinate a perdere effetto al momento dell'adozione delle regole deontologiche (si v. artt. 2-*quater*, 21, comma 4, e 111, d.lgs. n. 101/2018), il cui rispetto assurge a specifica condizione di liceità del trattamento (art. 21, comma 5, d.lgs. n. 101/2018); infine, il ribaltamento di prospettiva rispetto all'analisi di trattamenti particolarmente gravidi di rischi specifici per i diritti, le libertà fondamentali o la dignità dell'interessato, analisi che un tempo era demandata all'Autorità medesima per il tramite della richiesta di verifica preliminare (ai sensi dell'oramai abrogato art. 17, d.lgs. n. 196/2003), e oggi affidata invece direttamente al titolare stesso, chiamato dall'art. 35 del GDPR ad effettuare, in ipotesi simili, la c.d. "valutazione d'impatto sulla protezione dei dati"[2], e a coinvolgere, *ex* art. 36 del GDPR, soltanto in un secondo momento e soltanto eventualmente l'Autorità qualora, dalla valutazione d'impatto stessa, risulti «*un rischio elevato in assenza di*

misure adottate dal titolare del trattamento per attenuare il rischio» (art. 36, par. 1, GDPR).

Al di là delle osservazioni di carattere generale di cui si è appena detto, **le considerazioni del Garante si concentrano poi su alcuni specifici e peculiari contesti o situazioni di lavoro, di recente e crescente diffusione alla luce dell'incessante rivoluzione digitale ancora in atto, e rispetto alle quali i moniti dell'Autorità stessa altro non rappresentano se non la specificazione concreta dei più generali principi che permeano l'intera materia della protezione dei dati personali**, quali, in particolare, i "rivoluzionari" principi c.d. di *accountability* (detto anche di responsabilizzazione, cui il GDPR fa più volte cenno già a partire dall'art. 5, par. 2, e consistente nella somma data dal rispetto delle prescrizioni normative con la prova delle stesse), di *privacy by design* e *by default* contenuti nell'art. 25 del GDPR (e che rispettivamente impongono la minimizzazione dei dati trattati tanto in fase di progettazione del trattamento quanto in modalità di impostazione predefinita a trattamento già intrapreso), nonché quelli più generali e già noti di liceità, correttezza e trasparenza, non eccedenza e necessità, minimizzazione dei dati, esattezza, limitazione delle finalità e della conservazione, corollari del più ampio principio di proporzionalità ed elevati dall'art. 5 del GDPR a condizione di liceità di ogni trattamento.

L'applicazione specifica degli stessi rende pertanto evidente perché, in materia di rapporti di lavoro, il trattamento dei dati relativi alle convinzioni religiose sembri essere ammesso solo «*in caso di fruizione di permessi in occasione di festività religiose o per individuare le corrette modalità di erogazione dei servizi di mensa o (…) per l'esercizio dell'obiezione di coscienza*»; spiega altresì la premura con cui l'*Authority*, rispetto ai trattamenti svolti per ragioni organizzative, come ad esempio in vista della predisposizione dei turni di lavoro, sottolinea di non indicare, nelle rispettive comunicazioni, le causali dell'assenza ogni qualvolta si evincano, dall'indicazione stessa, particolari categorie di dati, *in primis* quelli di natura sindacale e sanitaria, e altresì la severità con cui viene circondata la pubblicazione sulla bacheca aziendale di

dati valutativi e disciplinari, illegittima in quanto eccedente rispetto al trattamento ammesso, in materia di gestione del rapporto di lavoro, da norme di legge, regolamento o contrattazione collettiva e/o individuale, oggetto del provvedimento 13 dicembre 2018, n. 500, doc. web n. 9068983, con cui le modalità di effettuazione del trattamento sono state accusate di lesione della dignità personale, dal momento che esponevano i dipendenti all'osservazione continua dei colleghi e ad una concorrenza esasperata coi medesimi; altrettanto rigore è stato manifestato rispetto ai trattamenti finalizzati al versamento delle quote di iscrizione ad associazioni su delega e per conto del lavoratore, ove si è esclusa l'ammissibilità della comunicazione ad una sigla sindacale circa la diversa organizzazione sindacale cui ha aderito un suo ex iscritto (il caso coinvolgeva anche l'art. 26 della l. n. 300/1970, nota come "Statuto dei Lavoratori" e d'ora in avanti Stat. Lav., nonché il provv. 18 dicembre 2014, n. 609, doc. web n. 3721603, e la *newsletter* 7 dicembre 2018, doc. web n. 9065999).

Le osservazioni del Garante, poi, non potevano evitare di intersecarsi con la materia dei controlli a distanza, oramai realizzabili anche con un normale *smartphone* e procedimentalizzati dall'art. 4 Stat. lav.: al riguardo, dalla Relazione emerge un'interpretazione piuttosto restrittiva rispetto all'esenzione, ai sensi del comma 2, degli strumenti di lavoro dalla procedura concertativa-autorizzatoria di cui al comma 1, spingendo in direzione di un allargamento dell'area applicativa coperta dal comma 1 stesso[3].

Sempre in materia di controlli a distanza, sono ancora i consueti principi di necessità e proporzionalità a giustificare diversi giudizi di non legittimità, come è avvenuto rispetto ai trattamenti, effettuati tramite un sistema di localizzazione dei veicoli installato per esigenze organizzative e produttive, che risultavano sproporzionati rispetto alle finalità perseguite, le quali ben potevano essere utilmente centrate mediante raccolte di dati «*assai più limitate e conservate per un arco di tempo sensibilmente più ristretto*», che avrebbero evitato non solo la violazione del principio di *privacy by default* ma anche e soprattutto di «*realizzare il controllo massivo, prolungato*

e indiscriminato dell'attività del lavoratore», elemento, quest'ultimo, rinvenuto altresì in un ulteriore caso, in cui è stata riscontrata anche la violazione dell'art. 8 Stat. Lav. dal momento che dall'attività di geolocalizzazione su veicoli assegnati anche a fini personali risultavano essere trattati dati «*non rilevanti ai fini della valutazione dell'attitudine professionale*»[4]. Gli stessi principi, invece, spiegano la legittimità del trattamento effettuato da una società di vigilanza privata tramite un applicativo, completo di geolocalizzazione, installato sui dispositivi *smartphone* o *tablet* poi consegnati alle guardie giurate, ammesso alla luce del complessivo funzionamento del sistema e, in particolare, dell'esiguità dei tempi di conservazione (24 ore) e della previa individuazione dei casi in cui i soli soggetti autorizzati possono ricorrere alla funzionalità di localizzazione geografica, meccanismo poi arricchito dalle prescrizioni impartite dall'Autorità stessa[5].

Tra i vari aspetti già esaminati dal Garante nel corso della propria "vita" istituzionale, **non manca ovviamente l'ambito dei controlli sulla posta elettronica aziendale**, rispetto ai quali è stato confermato l'orientamento, espresso già nelle «Linee guida per posta elettronica e internet» contenute nel provv. 1° marzo 2007, n. 13, doc. web n. 1387522, fondato sulla centralità e completezza dell'informativa da rilasciare ai dipendenti e sulla limitazione del periodo di conservazione dei dati raccolti, principio, quest'ultimo, sicuramente violato dalla custodia dei medesimi addirittura oltre la cessazione del rapporto di lavoro, com'era nel caso prospettato al Collegio, ove l'immagazzinamento delle conversazioni elettroniche fungeva da strumento di ricostruzione *a posteriori* dell'intera attività aziendale e da mezzo probatorio in occasione di eventuali procedimenti disciplinari, tuttavia non conforme non soltanto a norma del GDPR e della normativa interna di recepimento, ma anche alla luce della disciplina sulla conservazione della documentazione[6], con un monito circa il fatto che la «*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*», senza dimenticare come anche tali ipotesi siano suscettibili di produrre un controllo a distanza che, come tale, deve essere sottoposto alla relativa

disciplina.

Considerazioni sostanzialmente identiche, salvo la violazione della normativa in tema di conservazione della documentazione, sono state mosse rispetto ai trattamenti effettuati da una società privata che svolge servizi di call center, anch'essa colpevole di aver violato sia i principi di cui all'art. 5 del GDPR sia il disposto dell'art. 4 Stat. lav, così come rispetto al controllo, posto in essere da un'altra azienda, delle fatture del *provider* del servizio telefonico al fine di monitorare l'andamento complessivo dei consumi in vista di un'ottimizzazione, sia qualitativa che economico-quantitativa, del servizio complessivo, meccanismo ancora una volta tacciato di sproporzionalità rispetto alle finalità perseguite[7].

È invece piuttosto recente l'attenzione riposta dall'Autorità, a partire dal parere 31 luglio 2014, doc. web n. 3423775 (con cui si esprimeva in relazione alle microcamere utilizzate da alcuni reparti mobili della polizia di Stato), **rispetto ai meccanismi** classificati dalla Relazione come **"sistemi di videosorveglianza mobile"**, per tali intendendosi quelli realizzati per il tramite di dispositivi indossabili (c.d. *wearables,* di cui le c.d. *body cams* costituiscono un esempio): il giudizio sul funzionamento del sistema, adottato in via sperimentale da una società erogatrice del servizio di trasporto pubblico ferroviario altresì disponibile all'attivazione della procedura di cui al comma 1, art. 4 Stat. lav. (specificamente per esigenze di sicurezza dei dipendenti e degli utenti), pare essere complessivamente positivo, nonostante alcune indicazioni tecniche[8] che ancora una volta rappresentano il frutto dell'approccio sostanzialista indotto dal GDPR, meno attento ai formalismi rispetto al previgente "Codice della Privacy" e più sensibile all'effettiva e sostanziale tutela degli interessati.

L'Autorità garante della protezione dei dati personali ha dato ulteriore prova della propria capacità di stare al passo con l'irrefrenabile ritmo dettato dall'innovazione tecnologico-digitale, nonostante l'analisi condotta dal medesimo collegio nel corso della propria attività non possa dirsi completamente esaustiva[9], né

tale potrà mai essere definita, stante l'infinita vastità e densità che connota l'ambito dei rapporti di lavoro. Tuttavia, non possono che essere salutati con favore i passi in avanti compiuti, in generale, con l'avvento della riforma europea e con la conseguente logica sostanzialista di cui il principio di *accountability* costituisce il contenitore per antonomasia, così come la crescente attenzione riposta dalla "nostra" Authority rispetto a un tema destinato a catalizzare l'attenzione di accademie e aule giudiziarie, quali appunto i dispositivi c.d. *wearables* di ultima generazione, il cui crescente successo e diffusione si spiega alla luce dell'altrettanto crescenti economicità e utilità degli stessi nel rispondere efficacemente alle esigenze organizzative e produttive dell'azienda, ma anche di sicurezza del lavoro (qui un commento sul rapporto tra *Industry* 4.0 e *Safety* 4.0).

[1] Che al riguardo distinguono, rispettivamente, le «*categorie particolari di dati personali*» dai «*dati personali relativi a condanne penali e reat*i».
[2] Come richiesto dall'art. 35, par. 4, e nell'ambito del «*meccanismo di coerenza*» di cui agli artt. 63 e ss., il Garante, con provvedimento 11 ottobre 2018, n. 467 (doc. web n. 9058979), ha provveduto ad individuare una serie di trattamenti transfrontalieri da sottoporre alla valutazione di impatto; stante il carattere non esaustivo di detto elenco, il medesimo obbligo deve ritenersi efficace anche in presenza dei criteri di cui alle Linee guida in materia di valutazione d'impatto, pubblicate in data 4 aprile 2017 dal Gruppo Art. 29, nella versione fatta propria il 25 maggio 2018 dal Comitato europeo per la protezione, che con la riforma è succeduto, senza soluzione di continuità, al Gruppo stesso.
[3] Sul punto si segnala anche il recente interpello del Ministero del Lavoro e delle Politiche Sociali, n. 3/2019, con il quale si è ribadito che ai fini del rilascio dell'autorizzazione di cui al comma 1, alternativa dell'accordo sindacale, non trova spazio il funzionamento del meccanismo tipicamente amministrativo del silenzio-assenso.
[4] Rispetto ai sistemi di geolocalizzazione il Garante si è preoccupato altresì di dettare alcune indicazioni operative, riportate nei provvedimenti 28 giugno 2018, n. 396, doc.

web n. 9023246 e 19 luglio 2018, n. 427, doc. web n. 9039945, ponendo l'accento sulla possibilità da offrire ai lavoratori, che della medesima devono essere naturalmente informati, di disattivare «*il dispositivo attraverso la cd. funzione privacy e di modificare alcune impostazioni standard del servizio*».

[5] Con provv. 18 aprile 2018, n. 232, doc. web n. 9358266, si è infatti richiesto, tra le altre cose, la previsione di un meccanismo che consenta la disattivazione della funzionalità di geolocalizzazione in costanza delle pause consentite dall'attività lavorativa; l'oscuramento della posizione una volta decorso un periodo determinato di inattività del dipendente sul monitor e il posizionamento di un'icona, sul dispositivo stesso, utile per indicare quando il sistema sia effettivamente in funzione.

[6] Di cui, in particolare, al Codice dell'Amministrazione Digitale, ossia il d. lgs. n. 82/2005 e corrispondenti decreti attuativi (tra cui il d.P.C.M. 3 dicembre 2013, recante le regole tecniche in materia di conservazione), e all'art. 2214 c.c.

[7] Le censure, riportate assieme alle misure prescritte dall'Autorità stessa a tutela degli interessati nel provv. 18 aprile 2018, n. 229, doc. web n. 8987133, riguardavano vari aspetti, *in primis* il controllo e la registrazione indiscriminati e indifferenziati di tutte le tariffe e delle corrispondenti chiamate, anche quelle di natura personale.

[8] Tra le misure dettate con provv. 22 maggio 2018, n. 362, doc. web n. 8995107, si segnalano la definizione delle condizioni al ricorrere delle quali l'operatore è tenuto ad attivare la videoregistrazione; le specifiche cautele quando ad essere coinvolti sono soggetti particolarmente vulnerabili (come minori o vittime di reati); la previsione di una verifica sulle registrazioni al fine di vagliare la loro effettiva rilevanza rispetto ai fini perseguiti; la disattivazione della funzionalità audio, dalla stessa società ritenuta superflua; l'oscuramento delle immagini riferite a terzi estranei ai fatti in occasione della trasmissione delle registrazioni alle compagnie di assicurazione; la predisposizione di tecniche utili ad evitare la modifica o cancellazione di quanto raccolto; la conservazione in forma cifrata delle videoregistrazioni stesse e, infine, un dispositivo idoneo a rendere edotti gli utenti della presenza e del funzionamento del sistema di videoripresa.

[9] Si allude al fenomeno c.d. "*smart working*" o "lavoro agile", disciplinato dalla l. n.

81/2017 e stranamente rimasto estraneo all'esame del Garante nonostante il discreto successo che sta progressivamente guadagnando, e che ben avrebbe "gradito" alcune indicazioni, soprattutto per ciò che riguarda le modalità del potenziale controllo sullo *smart worker*.

Andrea Tundo
Scuola di dottorato in Formazione della persona e mercato del lavoro
Università degli Studi di Bergamo
@tundo_andrea

Leggi anche

1. Controlli a distanza: l'importanza di un'adeguata informazione nel nuovo articolo 4 dello Statuto dei lavoratori Michele Cibin...
2. Il "nuovo" art. 171 del Codice Privacy: oltre la razionalizzazione normativa? Enrico Angelo Pititto...
3. Il braccialetto di Amazon, facciamo chiarezza Emanuele Dagnino...
4. Videosorveglianza e lavoro domestico: l'Ispettorato sulla inapplicabilità dell'art. 4 Stat. lav. Antonella Mauro...
5. La figura del Data Privacy Officer in azienda Gaetano Machì...
6. Privacy e tecnologie: il Garante contro il controllo delle conversazioni Skype Emanuele Dagnino...