Bollettino ADAPT 6 settembre 2021, n. 30

La tutela normativa dei lavoratori e degli altri soggetti portatori di interesse che vogliano segnalare atti illeciti di cui sono venuti a conoscenza in ragione di un rapporto di lavoro trova un effettivo riconoscimento attraverso il rispetto di specifiche tecnico-informatiche che garantiscano un adeguato livello di anonimato. Di recente, due interventi del Garante della protezione dei dati personali hanno evidenziato l'importanza del rispetto di standard tecnici delle piattaforme di *whistleblowing* al fine di evitare comportamenti ritorsivi o discriminatori da parte dell'organizzazione.

***Whistleblowing*: la normativa applicabile.**

La prima norma che ha regolato la tematica del *whistleblowing* all'interno dell'ordinamento italiano è stata la legge 6 novembre 2012, n. 190 che ha introdotto l'articolo 54-bis del decreto legislativo 30 marzo 2001, n. 165. In particolare, la versione attuale della norma dispone che "Il pubblico dipendente che, nell'interesse dell'integrità della pubblica amministrazione, segnala […] condotte illecite di cui è venuto a conoscenza in ragione del proprio rapporto di lavoro non può essere sanzionato, demansionato, licenziato, trasferito, o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro determinata dalla segnalazione."

Una disciplina simile è stata poi prevista per il settore privato dalla legge 30 novembre

2017, n. 179 che introduce i commi 2-bis, 2-ter e 2-quater all'interno dell'articolo 6 del decreto legislativo 8 giugno 2001, n. 231. In ottemperanza a tale norma, il modello di organizzazione e gestione dell'ente deve prevedere la presenza di uno o più canali che consentano, ai lavoratori di presentare, anche attraverso strumenti informatici, segnalazioni di condotte illecite di cui siano venuti a conoscenza in ragione delle funzioni svolte. I segnalanti sono tutelati da un divieto da parte dell'impresa di compiere atti di ritorsione o discriminatori quali, ad esempio, l'erogazione di sanzioni disciplinari, demansionamenti, licenziamenti, trasferimenti, per motivi collegati direttamente o indirettamente alla segnalazione.

La fattispecie.

L'attività istruttoria del Garante per la protezione dei dati personali ha evidenziato diversi profili di criticità relativi alla piattaforma di *whistleblowing* utilizzata dall'Aeroporto Guglielmo Marconi di Bologna S.p.A. che hanno portato all'adozione di due ordinanze di ingiunzione, una per l'aeroporto ed una per la società fornitrice della piattaforma informatica, per un totale di € 60.000,00. **Tra le motivazioni delle sanzioni, di particolare rilevanza sono i passaggi in cui si argomenta la mancata adozione di tecniche idonee a garantire la riservatezza dell'identità dei *whistleblower* su tre profili.**

In *primis* è stato rilevato il mancato utilizzo di misure di crittografia nei confronti dei dati trasmessi dal *browser* attraverso cui è utilizzato l'applicativo al server che riceve le informazioni. L'utilizzo del protocollo *http* (*Hypertex Transfer Protocol*) anziché del protocollo *https* (*Hypertex Transfer Protocol Secure*), infatti, non garantirebbe un'adeguata protezione per i *whistleblower* nei casi in cui le informazioni venissero intercettate al momento del trasferimento dall'applicativo al server. Tale posizione è confermata anche all'interno dello "Schema di Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing)" adottato da ultimo con Delibera n. 469 del 9 giugno 2021 dall'Autorità Nazionale Anticorruzione (ANAC), che dispone al paragrafo 2.2 relativo alle modalità di gestione delle segnalazioni che la procedura di gestione delle segnalazioni, laddove la piattaforma sia accessibile tramite *firewall* come nel caso in oggetto deve, a tutela del segnalatore, "garantire la non tracciabilità del segnalante nel momento in cui viene stabilita la connessione anche mediante

l'impiego di strumenti di anonimizzazione dei dati di navigazione (ad es. tramite protocollo di trasporto https e accesso mediato dalla rete TOR)".

La seconda criticità rilevata riguardava la memorizzazione dei dati di log relativi alle operazioni di navigazione effettuate per una durata di 90 giorni. La piattaforma acquisiva l'indirizzo IP del dispositivo utilizzato ed il nome utente del soggetto che aveva effettuato l'accesso rendendo in questo modo possibile identificare coloro che avevano utilizzato l'applicativo. Sebbene le specifiche del sistema di segnalazione non permettessero di conoscere esattamente le funzionalità utilizzate (se il mero accesso alle FAQ o alla normativa di riferimento ovvero l'attivazione di una procedura di segnalazione), **il Garante ha reputato illecita l'attività di raccolta dei log in quanto non necessaria per la specifica finalità del trattamento**.

Terza irregolarità rilevata dal Garante per la protezione dei dati personali è l'esecuzione tardiva di una valutazione di impatto sulla protezione dei dati di cui all'articolo 35 del Regolamento UE 679/2016. Secondo il Garante, il trattamento dei dati delle segnalazioni necessita di una valutazione d'impatto poiché rientra nei casi in cui è presente un "rischio elevato per i diritti e le libertà delle persone fisiche". Tenuto conto della vulnerabilità degli interessati e considerato che il contesto di riferimento è quello lavorativo, caratterizzato per sua natura da un rilevante squilibrio nel rapporto tra datore di lavoro e lavoratore, il Titolare avrebbe dunque dovuto predisporre la valutazione d'impatto prima dell'avvio delle attività di trattamento dei dati personali.

Misure tecniche ed organizzative per la tutela del diritto alla protezione dei dati personali dei segnalatori.

La difficoltà di provare la reale portata discriminatoria o ritorsiva di una scelta aziendale, unita all'effetto deterrente che ciò può avere nei confronti dei lavoratori che vorrebbero segnalare delle irregolarità, rende necessario garantire ai segnalatori una tutela preventiva. Per tale motivo, l'articolo 2-ter dell'articolo 6, d.lgs. 231/2001 prevede che **gli strumenti di segnalazione debbano garantire la riservatezza dell'identità del segnalante.**

L'intera normativa in materia di protezione dei dati personali si fonda sulla ricerca di un equilibrio tra la definizione delle tipologie di trattamento ammissibili e la tutela dei diritti degli interessati attraverso l'attuazione da parte dei titolari del trattamento di misure tecniche ed organizzative adeguate. Posto che il Regolamento generale in materia di protezione dei dati personali pone raramente dei divieti *tout court* a specifiche attività di trattamento, l'attenzione del Legislatore si focalizza prevalentemente sulle modalità attraverso cui le informazioni sono raccolte, conservate e analizzate.

Ciò è particolarmente evidente, in particolare, dall'articolo 25 del Regolamento, secondo cui "tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento."

Le due decisioni del Garante per la protezione dei dati personali in materia di *whistleblowing* prese in esame mostrano infatti come i princìpi della *privacy by design* e della *privacy by default* di cui all'articolo 25 siano funzionali alla *compliance* rispetto alle altre disposizioni in materia di protezione dei dati personali. **La predisposizione fin dall'inizio di standard tecnici ed organizzativi adeguati nell'ambito di un'attività di trattamento – vale a dire la progettazione di tutte le fasi del trattamento, dei soggetti coinvolti e degli strumenti utilizzati – rappresenta nell'ambito della normativa europea in materia di protezione dei dati personali una importante leva per valorizzare al meglio le informazioni raccolte e garantire al tempo stesso un'adeguata tutela dei diritti degli interessati.**

Gaetano Machì

Scuola di dottorato in Apprendimento e Innovazione nei contesti sociali e di lavoro

ADAPT, Università degli Studi di Siena

gaetanomachi