Privacy e controlli dei lavoratori: dai social media al GPS

di Giorgio Pedrazzi[1]

Introduzione

La tutela dei dati personali dei lavoratori è giunta ad assumere una rilevanza centrale nella corretta gestione dei processi aziendali. Le ragioni alla base di questa accresciuta importanza risiedono, da un lato, nell'evoluzione tecnologica che rende estremamente facile l'elaborazione e la trasmissione, nel gergo giuridico "trattamento", di un'enorme quantità di dati e, dall'altro, nell'introduzione di nuovi strumenti in grado di raccogliere dati e informazioni con sempre maggiore precisione.

Gli uffici amministrativi sono interconnessi tra loro e verso l'esterno, così come, oramai, anche i veicoli aziendali, le linee produttive e la maggior parte degli apparati (*device*) utilizzati in azienda.

'Internet of Things', meglio noto con l'acronimo IoT, promette una sempre più spinta interazione tra gli oggetti utilizzati nelle abitazioni e nelle unità produttive o, addirittura, indossati dagli utenti dei servizi.

La nozione di dato personale nell'ambito del rapporto di lavoro va, quindi, estesa: ricomprende anche le immagini riprese dalle telecamere di videosorveglianza fino agli identificatori univoci come le coordinate geografiche della posizione elaborati dal sensore GPS, gli indirizzi IP che mostrano la connessione alla rete, il *mac-address* che traccia l'apparato con il quale si è connessi e, tutti i riferimenti idonei ad individuarlo oltre, conseguentemente, al lavoratore che lo sta utilizzando. In considerazione di questa evoluzione, come esplicitato dal considerando 5 dello stesso regolamento UE 2016/679, l'Unione Europea ha introdotto un pacchetto di strumenti al fine di adeguare la data protection agli standard tecnologici attuali: questa disciplina prende il nome di General Data Protection Regulation, più comunemente richiamata con l'onnipresente acronimo GDPR. La protezione dei dati personali, rivolta agli individui dell'Unione Europea, trova la sua massima espressione nell'ambito del rapporto di

[1] Professore aggregato di Istituzioni di Diritto Privato presso l'Università degli Studi di Brescia.

lavoro, sebbene ciascuno Stato membro possa prevedere, tramite leggi o contratti collettivi, discipline più specifiche per assicurare la protezione dei diritti e delle libertà con riferimento al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro (art. 88, co. 1, Reg. UE n. 2016/679).

Nei successivi paragrafi affronteremo brevemente gli aspetti dell'utilizzo della Rete Internet sul luogo di lavoro, anche attraverso email, navigazione e attività sui social media accanto alla gestione di strumenti di geolocalizzazione.

Privacy e lavoro

Per definire il perimetro della conformità del trattamento di dati personali in ambito lavorativo è necessario individuare le fonti di riferimento. Già ad un esame superficiale, appare evidente come la complessità della materia si rifletta nella molteplicità degli strumenti giuridici che ne definiscono la disciplina. Il D.Lgs. 196/03, comunemente indicato come Codice Privacy, adottato in recepimento della Direttiva 95/46, è stato oggi sostituito dal GDPR che costituisce, quindi, la disciplina attuale, insieme al decreto legislativo di raccordo, che abroga il Codice Privacy.

Per comprenderne appieno i profili applicativi è, poi, necessario considerare la prassi del Garante accanto ad una giurisprudenza che appare sempre più calata in una dimensione europea. Ad un ulteriore livello di approfondimento, lo specifico settore lavorativo richiede di essere riconciliato con la disciplina contenuta nello Statuto dei Lavoratori, L. 300/70. In particolare l'art. 4, dedicato ai controlli dei lavoratori e recentemente riformato dai decreti attuati del Jobs Act. Anche su questo tema la prassi svolge un ruolo rilevante, come testimoniato dalla recente circolare INL (Ispettorato Nazionale del Lavoro) n. 5 del 18 febbraio 2018. La giurisprudenza domestica, sia in sede civile che penale, è stata chiamata spesso a pronunciarsi sui temi più controversi come quello, ad esempio, dei controlli difensivi. Infine, un riferimento imprescindibile, soprattutto in questi primi tempi di applicazione del GDPR, è rappresentato dai pareri resi dal Gruppo di lavoro articolo 29 per la protezione dei dati (Working Party art. 29), istituito in virtù dell'articolo 29 della direttiva 95/46/CE, che riuniva le Autorità Garanti dei diversi Stati membri. In questi anni è stato l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata e ha rappresentato il preludio dell'attuale

Comitato dei Garanti Europei (European Board), che avrà il compito di seguire l'applicazione del GDPR.

Internet, email e social media al lavoro

Le questioni concernenti l'utilizzo di e-mail e il monitoraggio dell'attività svolta in rete dal dipendente sono costantemente all'attenzione della giurisprudenza. In tempi più recenti la prospettiva è giunta fino alla Corte Europea Diritti dell'uomo, chiamata a pronunciarsi in due occasioni con le sentenze, in parte difformi, rese il 12 dicembre 2016 e il 5 settembre 2017. Nel caso *Bărbulescu*, il più recente, è stata espressamente affermata la necessità per il lavoratore di essere informato sulle modalità e sulle finalità del controllo effettuato sulla posta elettronica.

È pertanto necessario che il datore di lavoro informi in modo adeguato e completo il lavoratore circa le modalità di utilizzo degli strumenti di connessione ad internet e di comunicazione e messaggistica che gli siano forniti dall'azienda. Riguardo ai social network on-line, compresi quelli aziendali che sono equiparati, in questo senso troviamo il parere 5/2009– WP 163 del Gruppo di lavoro art. 29.

Sul fronte della giurisprudenza italiana, la sentenza della Cassazione del 27 maggio 2015 n. 10955 ha ritenuto ammissibile l'attivazione di un profilo Facebook fittizio da parte del responsabile delle risorse umane di un'azienda allo scopo di verificare l'accesso al social network, durante l'orario di lavoro, di un dipendente.

Per quanto concerne i sistemi di messaggistica e voip, con il provvedimento n. 345 del 4 giugno 2015, il Garante per la protezione dei dati personali ha sanzionato un'azienda che aveva controllato le conversazioni su Skype, attraverso l'installazione di un software sul computer della dipendente, per utilizzare queste informazioni come giustificazione del licenziamento.

In alcuni casi, però, l'informativa non basta ma è richiesto il consenso, come con riguardo alla diffusione dei dati personali in Rete. Come precisato dal Garante nel Vademecum del 2015 «in ambito di lavoro privato per pubblicare informazioni personali (foto, curriculum) nella intranet aziendale e, a maggior ragione in internet, occorre il consenso dell'interessato». Ulteriormente, nella policy aziendale sarebbe opportuno definire le modalità con cui l'utente stesso può rendere di dominio pubblico informazioni circostanziate riguardo alla sua posizione in un dato momento, attraverso la pubblicazione e condivisione sui canali social di

fotografie o informazioni o recensioni con la procedura del c.d. geotagging. Tale argomento conduce agli ulteriori spunti di approfondimento sugli strumenti di controllo, consenso e geolocalizzazione.

Geolocalizzazione e controlli dei lavoratori

L'utilizzo di strumenti di rilevazione della posizione geografica è oggi largamente diffuso, fermo restando che informazioni precise riguardanti l'ubicazione dello strumento si possono ricavare anche da hotspot wi-fi o da celle ripetitori di telecomunicazioni mobili. Pertanto, possiamo considerare tre strumenti di geolocalizzazione come GPS, stazioni base GSM e WiFi. Apparecchi come gli smartphone sono, di fatto, suscettibili di fornire informazioni a tutti e tre i livelli considerati. Il carattere personale di questi strumenti, che il lavoratore porta sempre con sé, fa sì che le informazioni georeferenziate possano seguire le abitudini e le attività del possessore anche in contesti e sfere intime e famigliari protette dal diritto alla privacy e, conseguentemente, subordinate all'acquisizione di un preventivo consenso informato. La possibilità di disattivare il servizio, che pure rappresenta una misura opportuna se non necessaria, non può essere assimilata ad un consenso. Nel caso dei dipendenti, i datori di lavoro possono adottare questa tecnologia solo quando se ne dimostri la necessità per una finalità legittima e gli stessi obiettivi non si possano raggiungere con mezzi meno invasivi.

Recentissima è la verifica del Garante privacy che ha ritenuto lecito, pertinente e non eccedente, il trattamento derivante dall'adozione di un sistema di geolocalizzazione satellitare dei veicoli della polizia municipale che opera nei territori di alcuni comuni aderenti a una convenzione per la gestione associata del servizio. La finalità della localizzazione è individuata nella sicurezza e nell'incolumità del personale, per ottimizzare l'impiego di operatori e veicoli della polizia municipale. Il sistema offre anche rilevazioni di tipo statistico e di rendicontazione del servizio: il vaglio dell'Autorità ha interessato le autorizzazioni, la durata della conservazione e l'aderenza del trattamento alle finalità.

I dati, disponibili in tempo reale su un monitor presso la centrale operativa, sono visualizzabili esclusivamente dal responsabile del servizio o da un suo delegato: il Garante ha richiesto che il sistema sia configurato per consentire solo accessi autorizzati tramite assegnazione di credenziali

di autenticazione differenziate e limitando i profili autorizzati alla modifica e all'estrazione dei dati.

Il Garante ha considerato la natura dell'attività di polizia locale e le misure di sicurezza ma in ogni caso, prima della sua installazione, ciascun Comune aderente alla convenzione è tenuto ad acquisire l'apposita autorizzazione della Direzione territoriale del lavoro, in conformità alla disciplina in materia di controllo a distanza dei lavoratori.

La conservazione dei dati relativi al tempo di permanenza e ai chilometri percorsi in una determinata area è stata determinata in un periodo massimo di trenta giorni ai fini della rendicontazione. Le informazioni riferite ai dipendenti impiegati nel servizio, mai direttamente identificati e comunque non più identificabili a fine turno, sono utilizzate per localizzare la posizione dei veicoli e, se necessario, identificare l'operatore al solo scopo di coordinare in modo più efficiente il servizio o gestire eventuali situazioni di criticità o emergenza. I dati non potranno essere utilizzati per finalità di gestione del rapporto di lavoro, come verifica della presenza in servizio, commisurazione dell'orario di lavoro o per finalità disciplinari. Conforme, ma con esito opposto per l'impresa, va richiamato il provvedimento del 12 gennaio 2017 in cui era stata sanzionata una società di vigilanza notturna per l'utilizzo dei dati GPS elaborati da uno specifico software anche per documentare eventi che hanno dato luogo a sanzioni disciplinari in assenza di adeguata informativa resa ai dipendenti.

Il consenso dell'interessato

Nell'ambito dell'applicazione del GDPR, il consenso non è richiesto in presenza di una base giuridica che giustifichi il trattamento. L'acquisizione di un valido consenso rappresenta una questione problematica in un contesto lavorativo come nel caso, esplicitato dal Gruppo di lavoro art. 29, in cui il consenso del lavoratore risulti necessario, ma un suo eventuale diniego potrebbe causare un reale o potenziale pregiudizio. In tale ipotesi, il consenso stesso non potrebbe qualificarsi come libero, cosicché i lavoratori devono poter negare la propria autorizzazione senza pregiudizio. Una situazione complessa può presentarsi quando il rilascio del consenso diventa una condizione dell'assunzione. Il lavoratore può astrattamente negare il proprio consenso, ma con la conseguenza di perdere l'opportunità di lavoro. In tali circostanze il benestare non si manifesta liberamente e, quindi, non è valido. A questo punto, per utilizzare appieno gli strumenti

di controllo e geolocalizzazione, il GDPR offre la possibilità di trovare una diversa base giuridica che giustifichi la necessità del trattamento di tali tipi di dati.

Invece di richiedere il consenso, i datori di lavoro devono accertarsi che sia possibile dimostrare la necessità di vigilare sull'esatta ubicazione dei dipendenti per una finalità determinata e valutare tale necessità a fronte dei diritti e delle libertà fondamentali dei dipendenti e delle loro legittime aspettative (Considerando 47). Nei casi in cui la necessità possa essere adeguatamente motivata, il fondamento giuridico del trattamento si potrebbe basare sull'interesse legittimo del responsabile (già presente all'articolo 24, lettera g) del Codice Privacy e riaffermato all'art. 6 del GDPR). Anche in questo caso, comunque, il datore di lavoro sarà tenuto ad adottare gli strumenti meno invadenti, evitare il monitoraggio costante. A tal fine potrebbe essere opportuno, ad esempio, scegliere un sistema che trasmetta un allarme quando un dipendente attraversa un confine virtuale prestabilito. Il dipendente dev'essere in grado di disattivare qualsiasi dispositivo di monitoraggio al di fuori dell'orario di lavoro e deve aver ricevuto opportune istruzione sulle modalità con cui esercitare questa opzione. In particolare, i dispositivi di geolocalizzazione dei veicoli non sono dispositivi di tracciamento del personale, ma la loro funzione consiste nel rintracciare o monitorare l'ubicazione dei veicoli sui quali sono installati. I datori di lavoro non dovrebbero considerarli come strumenti per seguire o monitorare il comportamento o gli spostamenti di autisti o di altro personale, ad esempio inviando segnali d'allarme in relazione alla velocità del veicolo.

Conclusioni

Ad esito dell'indagine compiuta sui due ambiti prescelti, è di palmare evidenza l'importanza di un'adeguata informazione da rendere preventivamente ai dipendenti. A parere di chi scrive, per raggiungere lo scopo è caldamente raccomandata l'adozione di policy aziendali, redatte con un linguaggio chiaro ed efficace e opportunamente calibrate sulla realtà aziendale a cui si riferiscono. Per ottenere i migliori risultati, sul piano dell'effettività e della sicurezza informatica, è necessario fornire un'adeguata formazione ai lavoratori, preordinata a far comprendere i diritti e gli obblighi derivanti dalle normative, ma anche l'ambito di operatività e le conseguenze derivanti dalle violazioni delle policy aziendali.