GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

17/IT

WP 249

Parere 2/2017 sul trattamento dei dati sul posto di lavoro

adottato l'8 giugno 2017

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B-1049 Bruxelles, Belgio, Ufficio MO59 05/35.

Sito Internet: http://ec.europa.eu/justice/data-protection/index_en.htm

Indice

1 Sintesi

Il presente parere mira a integrare le pubblicazioni precedenti del Gruppo di lavoro Articolo 29 (di seguito "Gruppo di lavoro") ossia il *parere 8/2001 sul trattamento dei dati personali nell'ambito dei rapporti di lavoro* (WP48)[1] e il *documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro* (WP55)[2] del 2002. Rispetto al momento della pubblicazione di questi documenti sono state adottate talune nuove tecnologie che consentono un trattamento più sistematico dei dati personali dei lavoratori sul posto di lavoro, creando sfide impegnative in materia di protezione dei dati personali e della vita privata.

Il presente parere effettua una nuova valutazione dell'equilibrio tra gli interessi legittimi dei datori di lavoro e le ragionevoli aspettative dei dipendenti in materia di tutela della vita privata, descrivendo i rischi posti dalle nuove tecnologie e valutando la proporzionalità di una serie di scenari nel contesto dei quali dette tecnologie potrebbero essere utilizzate.

Pur fondandosi principalmente sulla direttiva sulla protezione dei dati, il presente parere prende in considerazione gli obblighi supplementari imposti ai datori di lavoro dal regolamento generale sulla protezione dei dati. Inoltre esso ribadisce la posizione e le conclusioni del parere 8/2001 e del documento di lavoro WP55, ossia che in caso di trattamento dei dati personali dei dipendenti:

- i datori di lavoro devono sempre tener conto dei principi fondamentali in materia di protezione dei dati, indipendentemente dalla tecnologia utilizzata;
- i contenuti delle comunicazioni elettroniche effettuate a partire dai locali aziendali sono soggetti agli stessi diritti fondamentali di protezione delle comunicazioni effettuate con mezzi analogici;
- è estremamente improbabile che il consenso costituisca una base giuridica per il trattamento dei dati sul posto di lavoro, a meno che i dipendenti non possano rifiutarsi di concederlo senza subire conseguenze negative;
- talvolta è possibile invocare l'esecuzione di un contratto e legittimi interessi, purché il trattamento sia strettamente necessario per una finalità legittima e sia conforme ai principi di proporzionalità e sussidiarietà;
- i dipendenti devono ricevere informazioni efficaci in merito al monitoraggio svolto; e
- qualsiasi trasferimento internazionale dei dati dei dipendenti deve avvenire soltanto se è garantito un adeguato livello di protezione.

[1] Gruppo di lavoro Articolo 29, *Parere 8/2001 sul trattamento dei dati personali nell'ambito dei rapporti di lavoro*, WP 48 del 13 settembre 2001, URL (in inglese): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.

[2] Gruppo di lavoro Articolo 29, *Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro*, WP 55 del 29 maggio 2002, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_it.pdf.

2. Introduzione

La rapida adozione di nuove tecnologie dell'informazione sul posto di lavoro, in termini di infrastrutture, applicazioni e dispositivi intelligenti, consente nuovi tipi di trattamento sistematico dei dati sul posto di lavoro potenzialmente invasivi. Ad esempio:

- sul posto di lavoro si possono attualmente usare tecnologie che consentono il trattamento dei dati a costi notevolmente ridotti rispetto a quelli di diversi anni fa, con un aumento esponenziale delle capacità di trattamento dei dati;
- alcune nuove forme di trattamento, come quelle relative ai dati personali legati all'utilizzo di servizi online e/o dati relativi all'ubicazione ricavati da un dispositivo intelligente, sono molto meno visibili ai dipendenti rispetto ad altri tipi più tradizionali, quali le telecamere visibili del sistema di televisione a circuito chiuso. Ciò solleva dubbi in merito al grado di consapevolezza dei dipendenti rispetto a queste tecnologie, in quanto i datori di lavoro potrebbero procedere illecitamente a tali trattamenti senza informarne preventivamente i dipendenti; inoltre
- i confini tra l'ambito domestico e quello lavorativo sono diventati sempre più labili. Ad esempio, quando i dipendenti lavorano da remoto (ad esempio da casa) oppure durante gli spostamenti per lavoro, può avvenire un monitoraggio delle attività al di fuori dell'ambiente fisico di lavoro che può includere potenzialmente il monitoraggio di una persona in un contesto privato.

Di conseguenza, sebbene l'utilizzo di tali tecnologie possa essere utile per individuare o prevenire la perdita di proprietà aziendali intellettuali e materiali, migliorare la produttività dei dipendenti e proteggere i dati personali di cui il titolare del trattamento è responsabile, si tratta di tecnologie che pongono al contempo sfide impegnative in termini di protezione dei dati e della vita privata. Pertanto è necessaria una nuova valutazione in merito all'equilibrio tra il legittimo interesse del datore di lavoro a proteggere la propria attività e la ragionevole aspettativa di protezione della vita privata degli interessati, ossia dei dipendenti.

Nonostante il presente parere si concentri sulle nuove tecnologie dell'informazione valutando nove scenari diversi nei quali le stesse possono essere impiegate, esso esaminerà brevemente anche metodi più tradizionali di trattamento dei dati sul posto di lavoro nel contesto dei quali i rischi vengono amplificati dal cambiamento tecnologico.

Con il termine "dipendente", nel presente parere il Gruppo di lavoro non si riferisce esclusivamente alle persone soggette a un contratto di lavoro riconosciuto come tale ai sensi delle leggi vigenti in materia. Negli ultimi decenni sono diventati più comuni nuovi modelli aziendali serviti da tipi diversi di rapporto di lavoro, in particolare il ricorso a lavoratori *freelance*. Il presente parere intende trattare tutte le situazioni di rapporto di lavoro, indipendentemente dal fatto che tale rapporto si basi su un contratto di lavoro.

È importante riconoscere che i dipendenti si trovano raramente nella posizione di concedere, rifiutare o revocare liberamente il consenso al trattamento dei dati, vista la dipendenza derivante dal rapporto datore di lavoro/dipendente. Salvo in situazioni eccezionali, i datori di lavoro dovranno basarsi su un fondamento giuridico diverso dal consenso, ad esempio la necessità di trattare i dati per un loro legittimo interesse. Tuttavia, un legittimo interesse non è in sé sufficiente per prevalere sui diritti e sulle libertà dei dipendenti.

Indipendentemente dalla base giuridica del trattamento, prima di procedere allo stesso si dovrebbe verificarne la proporzionalità in modo da valutare se il trattamento sia necessario

per conseguire una finalità legittima ed esaminare le misure da adottare per garantire che le violazioni dei diritti alla vita privata e alla segretezza delle comunicazioni siano limitate al minimo necessario. Tale attività può costituire parte di una valutazione d'impatto sulla protezione dei dati.

3. Il quadro giuridico

Sebbene l'analisi che segue sia stata condotta principalmente in relazione all'attuale quadro giuridico definito dalla direttiva 95/46/CE (direttiva sulla protezione dei dati)[3], il presente parere esaminerà anche gli obblighi derivanti dal regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati)[4], che è già entrato in vigore e che sarà applicabile a partire dal 25 maggio 2018.

Per quanto riguarda la proposta di regolamento "ePrivacy"[5], il Gruppo di lavoro invita i legislatori europei a creare un'eccezione specifica per l'interferenza con i dispositivi rilasciati ai dipendenti[6]. La proposta di regolamento non contiene un'eccezione adeguata al divieto generale di interferenza e i datori di lavoro non possono in genere esibire un consenso valido per il trattamento dei dati personali dei loro dipendenti.

3.1 Direttiva 95/46/CE - Direttiva sulla protezione dei dati*

Nel parere 8/2001 il Gruppo di lavoro ha indicato che i datori di lavoro, quando trattano dati personali nell'ambito dei rapporti di lavoro, devono tenere conto dei principi fondamentali in materia di protezione dei dati sanciti nella direttiva sulla protezione dei dati. Lo sviluppo di nuove tecnologie e nuovi metodi di trattamento in questo contesto non ha modificato tale situazione, infatti, si può affermare che tali sviluppi hanno reso *più* importante per i datori di lavoro procedere in tal senso. In detto contesto, i datori di lavoro devono:

- garantire che i dati siano trattati per finalità specifiche e legittime, che sono proporzionate e necessarie;
- tenere conto del principio della limitazione delle finalità, assicurandosi al contempo che i dati siano adeguati, pertinenti e non eccessivi per la finalità legittima prevista;
- applicare i principi di proporzionalità e di sussidiarietà indipendentemente dal fondamento giuridico applicabile;

---

[3] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati *(GU L 281 del 23.11.95, pag. 31), URL:* http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:31995L0046.

[4] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) *(GU L 119 del 4.5.2016, pag. 1)*, URL: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679.

[5] Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE, 2017/0003 (COD), URL: http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017PC0010&from=IT.

* N.d.T.: La versione italiana del regolamento (UE) 2016/679 ha modificato alcuni termini della direttiva 95/46/CE (abrogata dal regolamento stesso). Per coerenza terminologica, questo testo riprende sempre la terminologia del regolamento. Pertanto "controller" è il "titolare del trattamento" ("responsabile del trattamento" nella direttiva) e "processor" è il "responsabile del trattamento" ("incaricato del trattamento" nella direttiva).

[6] Cfr. Gruppo di lavoro Articolo 29, *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation* (in inglese) (Parere 01/2017 sulla proposta di regolamento per il regolamento ePrivacy), WP 247 del 4 aprile 2017, pag. 29; URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

- essere trasparenti con i dipendenti in merito all'uso e alle finalità delle tecnologie di monitoraggio;
- consentire l'esercizio dei diritti degli interessati, ivi compresi i diritti di accesso e, se del caso, la rettifica, la cancellazione o il congelamento dei dati personali;
- mantenere i dati esatti e non conservarli più a lungo del necessario; e
- adottare tutte le misure necessarie per proteggere i dati dagli accessi non autorizzati, oltre a garantire che il personale sia sufficientemente consapevole degli obblighi in materia di protezione dei dati.

Senza ripetere nuovamente i suggerimenti dati in precedenza, il Gruppo di lavoro desidera sottolineare tre principi, ossia: i fondamenti giuridici, la trasparenza e le decisioni automatizzate.

3.1.1 *FONDAMENTI GIURIDICI (ARTICOLO 7)*

In caso di trattamento di dati personali nei rapporti di lavoro, deve essere soddisfatto almeno uno dei criteri di cui all'articolo 7. Qualora i tipi di dati personali trattati riguardino le categorie particolari (esaminate all'articolo 8), il trattamento è vietato a meno che non si applichi un'eccezione[7,8]. Anche nel caso in cui il datore di lavoro possa fare affidamento su una di tali eccezioni, è comunque necessario che sia soddisfatto uno dei fondamenti giuridici di cui all'articolo 7 affinché il trattamento possa essere considerato legittimo.

In sintesi, i datori di lavoro devono pertanto prendere atto di quanto segue:

- per la maggior parte delle attività di trattamento svolte sul posto di lavoro**, la base giuridica non può e non dovrebbe essere il consenso dei dipendenti** (articolo 7, lettera a)) in considerazione della natura del rapporto tra datore di lavoro e dipendente;
- il trattamento può essere necessario per **l'esecuzione di un contratto** (articolo 7, lettera b)) nei casi in cui il datore di lavoro debba trattare i dati personali del dipendente per soddisfare gli obblighi legati a detta esecuzione;
- è abbastanza comune che **il diritto del lavoro imponga obblighi legali** (articolo 7, lettera c)) **che richiedono il trattamento di dati personali**; in tali casi il dipendente deve essere informato in maniera chiara e completa in merito a tale trattamento (a meno che non si applichi un'eccezione);
- qualora un datore di lavoro intenda basare il trattamento su un suo **legittimo interesse** (articolo 7, lettera f)) la finalità del trattamento deve essere legittima, il metodo scelto o la tecnologia specifica devono essere necessari, proporzionati e attuati nella maniera meno intrusiva possibile, e il datore di lavoro deve essere in grado di dimostrare che

[7] Come indicato nella parte 8 del parere 8/2001; ad esempio l'articolo 8, paragrafo 2, lettera b), della direttiva prevede un'eccezione ai fini di assolvere gli obblighi e i diritti specifici del titolare del trattamento in materia di diritto del lavoro, nella misura in cui il trattamento stesso sia autorizzato da norme nazionali che prevedono adeguate garanzie.

[8] Va osservato che in alcuni paesi vigono misure speciali che i datori di lavoro devono rispettare per proteggere la vita privata dei lavoratori. Il Portogallo è un esempio dei paesi nei quali esistono misure speciali e misure analoghe possono essere applicate anche in altri Stati membri. Le conclusioni di cui alla sezione 5.6 nonché gli esempi presentati nelle sezioni 5.1 e 5.7.1 del presente parere non sono pertanto validi in Portogallo per questi motivi.

sono state adottate misure appropriate per garantire un equilibrio rispetto ai diritti e alle libertà fondamentali dei dipendenti[9];

- i trattamenti devono inoltre essere conformi ai **requisiti di trasparenza** (articolo 10 e 11) e i dipendenti devono essere informati in maniera chiara e completa del trattamento dei loro dati personali[10], ivi compreso dell'esistenza di qualsiasi monitoraggio; e
- devono essere adottate **misure tecniche e organizzative appropriate** per assicurare la sicurezza del trattamento (articolo 17).

I criteri più pertinenti di cui all'articolo 7 sono dettagliati qui in appresso.

- **Consenso (articolo 7, lettera a))**

Il consenso, secondo la direttiva sulla protezione dei dati, è definito come qualsiasi manifestazione di volontà libera, specifica e informata con la quale l'interessato accetta che i dati personali che lo riguardano siano oggetto di un trattamento. Affinché il consenso sia valido, esso deve essere anche revocabile.

Nel parere 8/2001 il Gruppo di lavoro ha sottolineato che quando un datore di lavoro deve trattare dati personali dei propri dipendenti, è fuorviante partire dal presupposto che il trattamento possa essere legittimato dal consenso dei dipendenti. Nei casi in cui il datore di lavoro affermi di necessitare del consenso del lavoratore ma un eventuale diniego di quest'ultimo potrebbe causare allo stesso un pregiudizio reale o potenziale (situazione molto probabile nei rapporti di lavoro, in particolare se riguarda il tracciamento da parte del datore di lavoro del comportamento del dipendente nel corso del tempo), allora il consenso non è valido in quanto non può essere espressione di una volontà libera. Di conseguenza, per la maggior parte dei casi di trattamento dei dati dei dipendenti, la base giuridica di tale trattamento non può e non dovrebbe essere il consenso dei dipendenti, per cui è necessario invocare una base giuridica diversa.

Inoltre, anche nei casi in cui sia possibile affermare che il consenso costituisca una base giuridica valida per il trattamento (ossia qualora sia possibile concludere senza ombra di dubbio che il consenso sia stato dato liberamente), esso deve essere una manifestazione specifica e informata della volontà del dipendente. Le impostazioni di default sui dispositivi e/o l'installazione di software che facilitino il trattamento elettronico dei dati personali non possono essere considerati costituire un consenso concesso dai dipendenti, poiché il consenso richiede un'espressione attiva della volontà. La mancata azione (ossia la mancata modifica delle impostazioni predefinite) non può in generale essere considerata un consenso specifico atto a consentire il trattamento[11].

---

[9] Gruppo di lavoro Articolo 29, *Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, WP 217, adottato il 9 aprile 2014, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf.

[10] A norma dell'articolo 11, paragrafo 2, della direttiva sulla protezione dei dati, il titolare del trattamento è esonerato dall'obbligo di fornire informazioni all'interessato nei casi in cui la registrazione o la comunicazione è prescritta per legge.

[11] Cfr. anche Gruppo di lavoro Articolo 29, *Parere 15/2011 sulla definizione di consenso*, WP187 del 13 luglio 2011, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_it.pdf, pag. 28.

- **Esecuzione di un contratto (articolo 7, lettera b))**

I rapporti di lavoro sono spesso basati su un contratto di lavoro tra il datore di lavoro e il dipendente. Se il trattamento di taluni dati personali è necessario per l'adempimento degli obblighi derivanti dal contratto di lavoro, come ad esempio il pagamento del dipendente, il datore di lavoro è tenuto a trattare tali dati.

- **Obblighi legali (articolo 7, lettera c))**

È abbastanza comune che il diritto del lavoro imponga obblighi legali al datore di lavoro che richiedono il trattamento di dati personali (ad esempio per finalità di calcolo delle imposte e di gestione amministrativa delle retribuzioni). Chiaramente, in tali casi, una legge di questo tipo costituisce la base giuridica per il trattamento dei dati.

- **Legittimo interesse (articolo 7, lettera f))**

Se un datore di lavoro intende giustificare il trattamento sulla scorta del fondamento giuridico di cui all'articolo 7, lettera f), della direttiva sulla protezione dei dati, la finalità deve essere legittima e il metodo scelto o la tecnologia specifica con cui verrà effettuato il trattamento devono essere necessari per il legittimo interesse del datore di lavoro. Inoltre il trattamento deve essere proporzionato alle esigenze aziendali, ossia alle finalità per le quali viene svolto. Il trattamento dei dati sul posto di lavoro dovrebbe essere svolto nella maniera meno intrusiva possibile e deve essere mirato allo specifico ambito di rischio. Inoltre, qualora esso si fondi sull'articolo 7, lettera f), il lavoratore conserva il diritto di opporsi al trattamento per motivi preminenti e legittimi a norma dell'articolo 14.

Affinché il trattamento possa basarsi sull'articolo 7, lettera f), è essenziale che siano presenti misure specifiche di attenuazione che garantiscano un adeguato equilibrio tra il legittimo interesse del datore di lavoro e i diritti e le libertà fondamentali dei lavoratori[12]. A seconda della forma di monitoraggio, tali misure dovrebbero includere restrizioni al monitoraggio in maniera da garantire che la vita privata del lavoratore non sia violata. Tali restrizioni potrebbero essere:

- geografiche (ad esempio monitoraggio solo in luoghi specifici; si dovrebbe proibire il monitoraggio di aree sensibili quali luoghi religiosi e, ad esempio, zone ad uso sanitario e locali destinati alle pause);
- orientate ai dati (ad esempio non si dovrebbero monitorare comunicazioni e file elettronici personali);
- definite in termini temporali (ad esempio monitoraggio a campione, anziché continuo).

[12] Per un esempio dell'equilibrio che è necessario realizzare, cfr. il caso di *Köpke contro Germania*, [2010] ECHR 1725, (URL: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), nell'ambito del quale un dipendente è stato licenziato a seguito di un'operazione di videosorveglianza occulta intrapresa dal datore di lavoro e da un'agenzia di investigazione privata. Sebbene nel caso di specie la Corte abbia concluso che le autorità nazionali avevano raggiunto un equilibrio equo tra l'interesse legittimo del datore di lavoro (relativo alla tutela dei suoi diritti di proprietà), il diritto del lavoratore al rispetto della vita privata e l'interesse pubblico relativo all'amministrazione della giustizia, essa ha altresì osservato che in futuro ai vari interessi in gioco potrebbe essere riconosciuta una rilevanza diversa come conseguenza dello sviluppo tecnologico.

3.1.2 *TRASPARENZA (ARTICOLI 10 E 11)*

I requisiti di trasparenza di cui agli articoli 10 e 11 si applicano al trattamento dei dati sul posto di lavoro; i dipendenti devono essere informati dell'esistenza di qualsiasi monitoraggio, delle finalità per le quali i dati personali devono essere trattati e deve essere fornita loro ogni altra informazione necessaria per garantire un trattamento lecito.

Con l'avvento delle nuove tecnologie, la necessità di trasparenza diventa più evidente in considerazione del fatto che tali tecnologie consentono la raccolta e l'ulteriore trattamento in maniera occulta di volumi potenzialmente enormi di dati personali.

3.1.3 *DECISIONI AUTOMATIZZATE (ARTICOLO 15)*

L'articolo 15 della direttiva sulla protezione dei dati riconosce agli interessati anche il diritto di non essere sottoposti ad una decisione fondata esclusivamente su un trattamento automatizzato, laddove tale decisione produca effetti giuridici o abbia effetti significativi nei loro confronti e sia fondata esclusivamente su un trattamento automatizzato di dati intesi a valutare taluni aspetti della loro personalità, quali il rendimento professionale, a meno che detta decisione non sia necessaria per la stipula o l'esecuzione di un contratto, autorizzate dal diritto dell'Unione o di uno Stato membro, oppure si basi sul consenso esplicito dell'interessato.

3.2 Regolamento (UE) 2016/679 - regolamento generale sulla protezione dei dati

Il regolamento generale sulla protezione dei dati include e migliora le prescrizioni della direttiva sulla protezione dei dati; inoltre, introduce nuovi obblighi per tutti i titolari del trattamento dei dati, ivi inclusi i datori di lavoro.

3.2.1 *PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE*

L'articolo 25 del regolamento generale sulla protezione dei dati impone ai titolari del trattamento di attuare una protezione dei dati fin dalla progettazione e una protezione per impostazione predefinita. Ad esempio, se il datore di lavoro rilascia ai dipendenti dispositivi che includono tecnologie di tracciamento, si devono selezionare le soluzioni che proteggono maggiormente la vita privata. Inoltre, si deve prendere in considerazione anche la minimizzazione dei dati.

3.2.2 *VALUTAZIONI D'IMPATTO SULLA PROTEZIONE DEI DATI*

L'articolo 35 del regolamento generale sulla protezione dei dati fa obbligo al titolare del trattamento di effettuare una valutazione d'impatto sulla protezione dei dati quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. È il caso, ad esempio, di una valutazione sistematica e globale di aspetti personali di persone fisiche basata su un trattamento automatizzato che include la profilazione, in base alla quale sono prese decisioni che hanno effetti giuridici o analogamente incidono in modo significato sugli interessati.

Laddove la valutazione d'impatto sulla protezione dei dati indichi che il titolare del trattamento non è in grado di gestire in maniera sufficientemente adeguata i rischi individuati, ossia che i rischi residuali rimangono elevati, il titolare del trattamento deve consultare

l'autorità di controllo prima di procedere al trattamento (articolo 36, paragrafo 1) come chiarito nelle linee guida del Gruppo di lavoro in materia di valutazioni d'impatto sulla protezione dei dati[13].

3.2.2 "*TRATTAMENTO DEI DATI NELL'AMBITO DEI RAPPORTI DI LAVORO*"

L'articolo 88 del regolamento generale sulla protezione dei dati stabilisce che gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro. In particolare, dette norme possono essere previste per finalità di:

- assunzione;
- esecuzione del contratto di lavoro (compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi);
- gestione, pianificazione e organizzazione del lavoro;
- parità e diversità sul posto di lavoro;
- salute e sicurezza sul lavoro;
- protezione della proprietà del datore di lavoro o del cliente;
- esercizio e godimento (individuale) dei diritti e dei vantaggi connessi al lavoro; e
- cessazione del rapporto di lavoro.

A norma dell'articolo 88, paragrafo 2, tali norme devono includere misure appropriate e specifiche a salvaguardia della dignità umana, dei legittimi interessi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda:

- la trasparenza del trattamento;
- il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune; e
- i sistemi di monitoraggio sul posto di lavoro.

Nel presente parere il Gruppo di lavoro ha fornito linee guida per l'uso legittimo di nuove tecnologie in una serie di situazioni specifiche, descrivendo nel dettaglio le misure appropriate e specifiche per salvaguardare la dignità umana, il legittimo interesse e i diritti fondamentali dei dipendenti.

4. Rischi

Le tecnologie moderne consentono di tracciare i dipendenti nel corso del tempo, nei luoghi di lavoro e nelle loro abitazioni, attraverso numerosi dispositivi diversi, quali smartphone, computer da tavolo, tablet, veicoli e dispositivi indossabili. Qualora il trattamento non sia soggetto a restrizioni e non sia trasparente, sussiste il rischio elevato che il legittimo interesse del datore di lavoro al miglioramento dell'efficienza e alla protezione dei beni aziendali si trasformi in un monitoraggio ingiustificabile e intrusivo.

[13] Gruppo di lavoro Articolo 29, *Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679*, WP 248 del 4 aprile 2017, URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, pag. 18.

Le tecnologie che monitorano le comunicazioni possono altresì dissuadere dall'esercizio dei diritti fondamentali dei dipendenti di organizzare e tenere riunioni dei lavoratori e di comunicare in maniera confidenziale (ivi incluso il diritto di chiedere informazioni). Il monitoraggio delle comunicazioni e del comportamento esercita pressioni sui dipendenti che sono spinti a conformarsi in maniera da evitare comportamenti che potrebbero essere percepito come anomali, in maniera analoga al modo in cui l'uso intenso di sistemi di televisione a circuito chiuso ha influenzato il comportamento dei cittadini negli spazi pubblici. Inoltre, in considerazione delle capacità di tali tecnologie, i dipendenti potrebbero non essere consapevoli di quali dati personali vengono trattati e per quali finalità e per di più potrebbero non essere nemmeno consapevoli dell'esistenza della tecnologia di monitoraggio in sé.

Anche il monitoraggio dell'uso delle tecnologie dell'informazione si differenzia da altri strumenti di monitoraggio e osservazione più visibili, quali i sistemi di televisione a circuito chiuso, in quanto può avvenire in maniera occulta. In assenza di una politica per il monitoraggio sul posto di lavoro facilmente comprensibile e prontamente accessibile, i dipendenti potrebbero non essere consapevoli dell'esistenza e delle conseguenze del monitoraggio in atto e, di conseguenza, potrebbero non essere in grado di esercitare i propri diritti. Un ulteriore rischio deriva dalla "raccolta eccessiva" di dati nel contesto di tali sistemi, si pensi ad esempio ai sistemi che raccolgono dati relativi all'ubicazione tramite WiFi.

L'aumento della quantità di dati generati sul luogo di lavoro, in associazione alle nuove tecniche per l'analisi dei dati e la creazione di corrispondenze incrociate tra gli stessi, è un fattore che può contribuire anch'esso alla creazione di rischi di ulteriore trattamento incompatibile. Un esempio di ulteriore trattamento illegittimo è l'uso di sistemi legittimamente installati per proteggere i beni dell'impresa per successive finalità di monitoraggio della disponibilità e del rendimento dei dipendenti nonché della loro gentilezza nei confronti dei clienti. Un altro esempio è l'utilizzo di dati raccolti tramite un sistema di televisione a circuito chiuso per monitorare sistematicamente il comportamento e il rendimento dei dipendenti oppure l'impiego dei dati di un sistema di geolocalizzazione (ad esempio, derivanti dal tracciamento WiFi o Bluetooth) per controllare costantemente i movimenti e il comportamento di un dipendente.

Di conseguenza, un tale tracciamento può violare il diritto alla tutela della vita privata dei dipendenti, indipendentemente dal fatto che il monitoraggio abbia luogo sistematicamente od occasionalmente. Il rischio non è limitato all'analisi del contenuto delle comunicazioni. Pertanto, l'analisi di metadati relativi a una persona potrebbe consentire un monitoraggio dettagliato altrettanto invasivo della vita privata e dei modelli di comportamento di una persona.

L'utilizzo diffuso delle tecnologie di monitoraggio può limitare altresì la disponibilità dei dipendenti (e dei canali tramite i quali essi possono procedere) a informare i datori di lavoro in merito a irregolarità o azioni illegali commesse da superiori e/o altri dipendenti che minacciano di danneggiare l'attività aziendale (in particolare i dati dei clienti) o il posto di lavoro. Spesso, affinché il dipendente interessato agisca attivamente e segnali tali situazioni è necessario che lo stesso possa beneficiare dell'anonimato. Il monitoraggio che viola il diritto alla tutela della vita privata dei dipendenti può ostacolare le necessarie comunicazioni alle

persone competenti. In casi analoghi, i mezzi messi a disposizione degli informatori interni possono diventare inefficaci[14].

5. Scenari

Questa sezione esamina una serie di scenari di trattamento dei dati sul posto di lavoro nel contesto dei quali le nuove tecnologie e/o gli sviluppi di tecnologie esistenti hanno o potrebbero presentare potenziali rischi elevati per la vita privata dei dipendenti. In tutti questi casi i datori di lavoro dovrebbero valutare se:

- l'attività di trattamento è necessaria e, in caso affermativo, quali sono i fondamenti giuridici che trovano applicazione;
- il trattamento proposto dei dati personali è corretto nei confronti dei dipendenti;
- l'attività di trattamento è proporzionata alle preoccupazioni sollevate; e
- l'attività di trattamento è trasparente.

5.1 Trattamenti durante il processo di assunzione

Le persone usano i media sociali diffusamente ed è relativamente comune che i profili utente siano pubblicamente visibili a seconda delle impostazioni scelte dal titolare dell'account. Di conseguenza, i datori di lavoro possono credere che esaminare i profili sociali dei potenziali candidati possa essere giustificato durante il processo di assunzione. Lo stesso può valere per altre informazioni pubblicamente disponibili sul potenziale dipendente.

Tuttavia, i datori di lavoro non dovrebbero supporre di essere autorizzati a trattare tali dati per proprie finalità semplicemente perché il profilo di una persona sui media sociali è pubblicamente accessibile. Per poter procedere a un simile trattamento è necessario disporre di un fondamento giuridico, ad esempio un legittimo interesse. In questo contesto, prima di esaminare il profilo del candidato sui media sociali, il datore di lavoro dovrebbe innanzitutto considerare se il profilo ha finalità commerciali o private, in quanto ciò può rappresentare un'indicazione importante dell'ammissibilità giuridica dell'esame di tali dati. Inoltre, il datore di lavoro è autorizzato a raccogliere e trattare i dati personali del candidato soltanto nella misura in cui tale raccolta è necessaria e pertinente per l'esecuzione del lavoro per il quale è stata presentata domanda.

In linea di principio, i dati raccolti durante il processo di assunzione dovrebbero essere cancellati non appena sia evidente che non verrà fatta alcuna offerta di impiego o che l'offerta non sarà accettata dal candidato[15]. Quest'ultimo deve inoltre essere correttamente informato di qualsiasi simile trattamento prima dell'avvio del processo di assunzione.

---

[14] Cfr. ad esempio: Gruppo di lavoro Articolo 29, *Parere 1/2006 relativo all'applicazione della normativa UE sulla protezione dei dati alle procedure interne per la denuncia delle irregolarità riguardanti la tenuta della contabilità, i controlli contabili interni, la revisione contabile, la lotta contro la corruzione, la criminalità bancaria e finanziaria*, WP 117 dell'1 febbraio 2006, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_it.pdf.

[15] Cfr. anche il documento del Consiglio d'Europa, *Raccomandazione CM/Rec(2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale*, paragrafo 13.2 (1° aprile 2015, URL: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/4224268). Qualora il datore di lavoro desideri conservare tali dati in previsione di ulteriori opportunità lavorative, ne deve informare l'interessato di conseguenza, il quale avrà la possibilità di opporsi a tale ulteriore trattamento; in quest'ultimo caso, i dati devono essere cancellati (ibidem).

Non esiste alcun fondamento giuridico che giustifichi la "richiesta di amicizia" di un datore di lavoro nei confronti di potenziali dipendenti o qualsiasi altra richiesta di accesso ai contenuti dei loro profili.

Esempio

Durante il processo di assunzione di nuovo personale, un datore di lavoro verifica i profili dei candidati su varie reti sociali e include le informazioni provenienti da tali reti (nonché qualsiasi altra informazione disponibile su Internet) nel processo di screening.

Il datore di lavoro può disporre di un fondamento giuridico a norma dell'articolo 7, lettera f), per esaminare le informazioni relative ai candidati accessibili al pubblico sui media sociali soltanto se tale esame è necessario ai fini del lavoro offerto, ad esempio per poter valutare rischi specifici correlati ai candidati che dovranno svolgere una funzione specifica, e se i candidati vengono informati correttamente in proposito (ad esempio nel testo dell'annuncio relativo al posto di lavoro).

5.2 Trattamenti derivanti da uno screening durante il periodo di impiego

In considerazione dell'esistenza di profili sui media sociali e dello sviluppo di nuove tecnologie di analisi, i datori di lavoro hanno (o possono ottenere) la capacità tecnica di effettuare uno screening permanente dei dipendenti, raccogliendo ad esempio informazioni riguardanti i loro amici, opinioni, credenze, interessi, spostamenti, atteggiamenti e comportamenti, acquisendo quindi dati che afferiscono anche alla vita privata e familiare dei dipendenti.

Lo screening durante il periodo di impiego dei profili dei dipendenti sui media sociali non dovrebbe avvenire su una base generalizzata.

Inoltre, il datore di lavoro dovrebbe astenersi dal chiedere a un dipendente o a un candidato l'accesso alle informazioni che questi condivide con altre persone sui media sociali.

Esempio
Un datore di lavoro monitora i profili LinkedIn di ex dipendenti per la durata dell'applicazione delle clausole di non concorrenza. La finalità del monitoraggio è il controllo del rispetto di tali clausole. Il monitoraggio è limitato agli ex dipendenti soggetti a tali clausole.

Fintantoché il datore di lavoro riesce a dimostrare che il monitoraggio è necessario per proteggere i propri legittimi interessi, che non esistono altri mezzi meno invasivi e che gli ex dipendenti sono stati adeguatamente informati sulla portata del monitoraggio sistematico delle loro comunicazioni pubbliche, il datore di lavoro potrà fare affidamento sul fondamento giuridico di cui all'articolo 7, lettera f), della direttiva sulla protezione dei dati.

Inoltre, i dipendenti non dovrebbero essere tenuti a utilizzare un profilo sui media sociali messo a disposizione dal loro datore di lavoro. Anche qualora ciò sia specificamente previsto in considerazione delle mansioni affidate agli stessi (ad esempio, quella di agire da portavoce di un'organizzazione), i dipendenti devono conservare l'opzione di disporre di un profilo non pubblico, ossia "non lavorativo", che possono utilizzare in sostituzione del profilo "ufficiale"

correlato al datore di lavoro, e ciò dovrebbe essere specificato nelle condizioni del contratto di lavoro.

5.3 Trattamenti risultanti dal monitoraggio dell'uso delle tecnologie dell'informazione e della comunicazione sul posto di lavoro

Tradizionalmente, il monitoraggio delle comunicazioni elettroniche sul posto di lavoro (ad esempio, telefono, navigazione in Internet, posta elettronica, messaggistica istantanea, VOIP, ecc.) è stato considerato la minaccia principale per la vita privata dei dipendenti. Nel *documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro* del 2001, il Gruppo di lavoro ha tratto una serie di conclusioni sul monitoraggio dell'utilizzo di posta elettronica e Internet. Sebbene tali conclusioni rimangano valide, occorre tener conto degli sviluppi tecnologici che hanno consentito nuove modalità di monitoraggio potenzialmente più intrusive e pervasive. Tali sviluppi includono, tra l'altro:

- strumenti per la prevenzione della perdita di dati (DLP) che monitorano le comunicazioni in uscita per individuare eventuali violazioni dei dati;
- sistemi di firewall di nuova generazione (NGFW, *Next-Generation Firewall*) e di gestione unificata delle minacce (UTM, *Unified Threat Management*), che possono mettere a disposizione una varietà di tecnologie di monitoraggio, tra cui quelle di *deep packet inspection* (ispezione profonda dei pacchetti), intercettazione TLS, filtraggio dei siti web, filtraggio dei contenuti, rendicontazione sulle applicazioni, informazioni relative all'identità degli utenti e (come descritto in precedenza) prevenzione della perdita di dati. Tali tecnologie possono essere altresì utilizzate individualmente, a seconda del datore di lavoro;
- applicazioni e misure atte a garantire la sicurezza che prevedono la registrazione dell'accesso dei dipendenti ai sistemi del datore di lavoro;
- la tecnologia *eDiscovery*, che si riferisce a qualsiasi processo in cui si effettuano ricerche di dati elettronici per utilizzarli come prova;
- il tracciamento dell'utilizzo di applicazioni e dispositivi tramite software invisibili, sia sul computer da tavolo che nel cloud;
- l'uso sul posto di lavoro di applicazioni per ufficio fornite come servizio cloud, le quali consentono in teoria di effettuare una registrazione molto dettagliata delle attività dei dipendenti;
- il monitoraggio di dispositivi personali (ad esempio computer, telefoni cellulari, tablet) che i dipendenti mettono a disposizione per lo svolgimento del loro lavoro in conformità con una specifica politica di utilizzo denominata *Bring-Your-Own-Device* (BYOD, ossia utilizza i tuoi dispositivi privati), nonché il ricorso alla tecnologia *Mobile Device Management* (gestione dei dispositivi mobili) che consente la distribuzione di applicazioni, dati e impostazioni di configurazione, nonché patch per dispositivi mobili; e
- l'uso di dispositivi indossabili (ad esempio dispositivi per il fitness e la salute).

È possibile che un datore di lavoro implementi una soluzione di monitoraggio "omnicomprensiva", ad esempio un insieme di pacchetti per la sicurezza che gli consentano di monitorare l'utilizzo di tutte le tecnologie dell'informazione e della comunicazione sul posto di lavoro, rispetto al semplice monitoraggio di posta elettronica e/o siti web, come

accadeva un tempo. Le conclusioni adottate nel documento WP55 si applicano a qualsiasi sistema che consente un tale monitoraggio[16].

Esempio

Un datore di lavoro intende utilizzare un apparecchio di intercettazione TLS per decrittare ed esaminare il traffico protetto al fine di individuare eventuali azioni dolose. L'apparecchio è in grado altresì di registrare e analizzare l'intera attività di un dipendente mentre è online sulla rete dell'organizzazione.

L'uso di protocolli di comunicazione crittografati è sempre più attuato per proteggere dalle intercettazioni i flussi di dati online che coinvolgono dati personali. Tuttavia, ciò può porre problemi, in quanto la crittografia rende impossibile monitorare i dati in entrata e in uscita. Le apparecchiature di intercettazione TLS decodificano il flusso di dati, analizzano il contenuto a fini di sicurezza e successivamente criptano nuovamente il flusso.

In questo esempio, il datore di lavoro si basa sul suo legittimo interesse, ossia la necessità di proteggere la rete e i dati personali dei dipendenti e dei clienti ivi conservati dall'accesso non autorizzato o dalla perdita di dati. Tuttavia, il monitoraggio di tutte le attività online dei dipendenti è una risposta sproporzionata e costituisce un'interferenza con il diritto alla segretezza delle comunicazioni. Il datore di lavoro dovrebbe innanzitutto prendere in considerazione altri mezzi, meno invasivi, per proteggere la riservatezza dei dati dei clienti e la sicurezza della rete.

Nella misura in cui un'intercettazione del traffico TLS possa qualificarsi come strettamente necessaria, l'apparecchio dovrebbe essere configurato in maniera tale da impedire la registrazione permanente dell'attività dei dipendenti, ad esempio, bloccando il traffico sospetto in entrata o in uscita e reindirizzando l'utente a un portale informativo nel quale egli può chiedere un riesame di tale decisione automatizzata. Tuttavia, nel caso in cui una certa forma di registrazione generale dei dati si renda strettamente necessaria, l'apparecchio può essere configurato anche per non conservare i dati di registro, a meno che l'apparecchio non segnali il verificarsi di un incidente, riducendo così al minimo le informazioni raccolte.

Come buona prassi, il datore di lavoro potrebbe offrire un accesso alternativo non monitorato ai dipendenti, ad esempio offrendo un accesso Wi-Fi gratuito oppure mettendo a disposizione dispositivi o terminali indipendenti (dotati di opportune misure di salvaguardia per garantire la riservatezza delle comunicazioni) tramite i quali i dipendenti possano esercitare il loro legittimo diritto di utilizzare le strutture di lavoro per un determinato uso privato[17]. Inoltre, i

[16] Cfr. anche *Copland contro Regno Unito*, (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ECHR 253 (URL: http://www.bailii.org/eu/cases/ECHR/2007/253.html), nell'ambito del quale la Corte ha dichiarato che i messaggio di posta elettronica inviati dai locali aziendali e le informazioni desunte dal monitoraggio dell'uso di Internet potrebbero costituire parte della corrispondenza e della vita privata di un dipendente e che la raccolta e la conservazione di tali informazioni senza che il dipendente ne sia a conoscenza costituirebbero un'interferenza con i diritti dei lavoratori, nonostante la Corte non si sia espressa in merito al fatto che tale monitoraggio non sarebbe assolutamente necessario in una società democratica.

[17] Cfr. *Halford contro Regno Unito*, [1997] ECHR 32, (URL: http://www.bailii.org/eu/cases/ECHR/1997/32.html), nel contesto del quale la Corte ha dichiarato che "le chiamate telefoniche provenienti da locali aziendali e da casa possono rientrare nelle nozioni di 'vita privata' e 'corrispondenza' ai sensi dell'articolo 8, paragrafo 1 [della Convenzione]"; e *Barbulescu contro Romania*, [2016] ECHR 61, (URL: http://www.bailii.org/eu/cases/ECHR/2016/61.html), riguardante l'uso di un account professionale di messaggistica istantanea per la corrispondenza personale, nel contesto del quale la Corte ha dichiarato che il monitoraggio dell'account da parte del datore di lavoro è stato limitato e proporzionato;

datori di lavoro dovrebbero valutare alcuni tipi di traffico la cui intercettazione mette a repentaglio il giusto equilibrio tra i loro legittimi interessi e la vita privata dei dipendenti, ad esempio l'uso di posta elettronica privata, visite a siti online di servizi bancari e siti web legati alla salute, onde configurare in maniera appropriata l'apparecchio in modo da non intercettare comunicazioni in circostanze non conformi al criterio di proporzionalità. È necessario specificare ai dipendenti informazioni sul tipo di comunicazioni che l'apparecchio è inteso monitorare.

Si dovrebbe sviluppare e rendere facilmente e costantemente accessibile a tutti dipendenti una politica relativa alle finalità per le quali i dati delle registrazioni sospette possono essere consultati e alle persone che possono farlo, anche al fine di fornire una guida sull'uso accettabile e inaccettabile della rete e delle strutture. Ciò consentirebbe ai dipendenti di adattare il proprio comportamento in maniera da evitare di essere monitorati quando utilizzano legittimamente le strutture di lavoro informatiche per uso privato. Come buona prassi, una tale politica dovrebbe essere riesaminata, almeno una volta l'anno, per valutare se la soluzione di monitoraggio scelta dia i risultati previsti e se esistono altri strumenti o mezzi meno invasivi per conseguire le medesime finalità.

Indipendentemente dalla tecnologia in questione o dalle sue capacità, la base giuridica di cui all'articolo 7, lettera f), è disponibile soltanto se il trattamento soddisfa determinate condizioni. Innanzitutto, i datori di lavoro che utilizzano questi prodotti e queste applicazioni devono valutare la proporzionalità delle misure che stanno attuando e se sia possibile adottare ulteriori azioni per attenuare o ridurre la portata e l'impatto del trattamento dei dati. Come esempio di buona prassi, una simile valutazione potrebbe essere svolta tramite una valutazione d'impatto sulla protezione dei dati prima di introdurre qualsiasi tecnologia di monitoraggio. In secondo luogo, i datori di lavoro devono attuare e comunicare politiche di utilizzo accettabili, corredate da politiche in materia di tutela della vita privata, che descrivano l'utilizzo consentito della rete e delle attrezzature dell'organizzazione e dettaglino con precisione il trattamento in atto.

In alcuni paesi la creazione di una tale politica richiederebbe per legge l'approvazione del consiglio dei delegati o di un organismo analogo di rappresentanza dei dipendenti. Nella pratica, spesso tali politiche sono redatte dal personale preposto alla manutenzione delle attrezzature informatiche. Dato che il loro obiettivo principale sarà quindi soprattutto la sicurezza e non la legittima aspettativa di tutela della vita privata dei dipendenti, il Gruppo di lavoro raccomanda di coinvolgere sempre un campione rappresentativo di dipendenti nella valutazione della necessità del monitoraggio, nonché della logica e dell'accessibilità della politica.

nonostante il parere contrario del giudice Pinto de Alberquerque che ha sostenuto la necessità di realizzare un equilibrio attento.

Esempio

Un datore di lavoro utilizza uno strumento per la prevenzione della perdita di dati con l'obiettivo di monitorare automaticamente i messaggi di posta elettronica in uscita per impedire la trasmissione non autorizzata di dati proprietari (ad esempio dati personali del cliente), indipendentemente dal fatto che la trasmissione sia intenzionale o meno. Quando un messaggio di posta elettronica viene considerato fonte potenziale di violazione dei dati, viene svolta un'indagine ulteriore.

Anche in questo caso, il datore di lavoro fonda il suo trattamento sulla necessità dettata dal suo interesse legittimo di proteggere i dati personali dei clienti e le proprie risorse aziendali dall'accesso non autorizzato o dalla perdita di dati. Tuttavia, un tale strumento di prevenzione della perdita di dati può comportare l'inutile trattamento di dati personali; ad esempio, un avviso "falso positivo" potrebbe determinare un accesso non autorizzato a messaggi di posta elettronica legittimi inviati dai dipendenti (ad esempio, messaggi di posta elettronica personali).

Di conseguenza, la necessità dello strumento di prevenzione della perdita di dati e il suo utilizzo dovrebbero essere pienamente giustificati in modo da realizzare il giusto equilibrio tra i legittimi interessi del datore di lavoro e il diritto fondamentale alla protezione dei dati personali dei lavoratori. Per poter far valere i legittimi interessi del datore di lavoro, dovrebbero essere prese alcune misure che attenuino i rischi. Ad esempio, le regole seguite dal sistema per classificare un messaggio di posta elettronica come potenziale violazione di dati dovrebbero essere assolutamente trasparenti agli utenti e, laddove lo strumento classifichi un messaggio di posta elettronica in uscita come possibile violazione di dati, il mittente dovrebbe ricevere, prima della trasmissione del messaggio, un messaggio di avviso in modo da poter annullare la trasmissione.

In alcuni casi il monitoraggio dei dipendenti è possibile non tanto grazie a tecnologie specifiche, bensì semplicemente perché i dipendenti sono tenuti a utilizzare applicazioni online messe a disposizione dal datore di lavoro che elaborano dati personali. Un esempio è l'uso di applicazioni per ufficio basate sul cloud (ad esempio editori di testo, calendari, applicativi di social networking). Occorre garantire che i dipendenti possano designare taluni spazi privati ai quali il datore di lavoro non può accedere, fatto salvo in circostanze eccezionali. È il caso, ad esempio, dei calendari, spesso utilizzati anche per appuntamenti privati. Qualora il dipendente classifichi un appuntamento come "privato" o annoti tale osservazione nei dettagli dell'appuntamento stesso, ai datori di lavoro (e agli altri dipendenti) non deve essere consentito esaminare il contenuto dell'appuntamento.

Talvolta, in questo contesto, il requisito della sussidiarietà implica che non sia possibile attuare alcun monitoraggio. È il caso, ad esempio, quando l'uso proibito di servizi di comunicazione può essere impedito bloccando l'accesso a taluni siti web. Qualora sia possibile bloccare i siti web, anziché monitorare continuamente tutte le comunicazioni, occorre optare per il blocco in maniera da rispettare il requisito di sussidiarietà.

Più in generale, si dovrebbe dare più peso alla prevenzione rispetto alla rilevazione: gli interessi del datore di lavoro sono protetti meglio prevenendo un uso improprio di Internet con mezzi tecnici, piuttosto che spendendo risorse per individuare tali usi impropri.

5.4 Trattamenti risultanti dal monitoraggio dell'uso delle tecnologie dell'informazione e della comunicazione al di fuori del posto di lavoro

L'utilizzo delle tecnologie dell'informazione e della comunicazione al di fuori del posto di lavoro è diventato più comune a seguito della crescita di politiche di lavoro a domicilio, lavoro a distanza e utilizzo dei propri dispositivi personali ("*bring your own device*"). Le funzionalità offerte da tali tecnologie possono rappresentare un rischio per la vita privata dei dipendenti, in quanto spesso i sistemi di monitoraggio presenti sul posto di lavoro vengono estesi in maniera efficace alla sfera domestica dei dipendenti nel momento in cui questi utilizzano tali apparecchiature.

5.4.1 *MONITORAGGIO DEL LAVORO A DOMICILIO E DEL LAVORO A DISTANZA*

È diventato più comune per i datori di lavoro offrire ai dipendenti la possibilità di lavorare da remoto, ad esempio, da casa e/o in viaggio. Di fatto si tratta di una delle principali cause della ridotta distinzione tra posto di lavoro e ambito domestico. In generale, la possibilità di lavorare da remoto implica che il datore di lavoro rilascia ai dipendenti apparecchiature TIC o software che, una volta installati a casa o sui dispositivi personali, consentono ai dipendenti di avere lo stesso livello di accesso alla rete, ai sistemi e alle risorse del datore di lavoro del quale beneficerebbero se fossero sul posto di lavoro, a seconda del grado di attuazione.

Sebbene possa essere uno sviluppo positivo, il lavoro a distanza presenta anche un rischio aggiuntivo per il datore di lavoro. Ad esempio, i dipendenti che hanno accesso remoto all'infrastruttura del datore di lavoro non sono vincolati dalle misure fisiche di sicurezza che possono essere messe in atto presso i locali del datore di lavoro. In altri termini: senza l'attuazione di adeguate misure tecniche il rischio di accesso non autorizzato aumenta e può provocare la perdita o la distruzione di informazioni, ivi inclusi i dati personali dei dipendenti o dei clienti, che il datore di lavoro può conservare.

Al fine di attenuare tale rischio, i datori di lavoro potrebbero pensare di essere giustificati a utilizzare pacchetti software (sia in modalità locale che nel cloud) in grado, ad esempio, di registrare i tasti premuti e i movimenti compiuti dal mouse, di acquisire schermate visualizzate (in maniera causale o a intervalli prestabiliti), di registrare le applicazioni utilizzate (e la durata del loro impiego) nonché, su dispositivi compatibili, di attivare telecamere web e raccogliere così filmati registrati. Tali tecnologie sono messe ampiamente a disposizione da terzi, tra i quali i prestatori di servizi cloud.

Tuttavia, il trattamento comportato da tali tecnologie è sproporzionato ed è altamente improbabile che il datore di lavoro disponga di un fondamento giuridico e di un legittimo interesse per registrare, ad esempio, i tasti premuti e i movimenti del mouse compiuti da un dipendente.

La chiave sta nell'affrontare il rischio posto dal lavoro a domicilio o a distanza in maniera proporzionata e non eccessiva, indipendentemente dal modo in cui tale opzione è offerta e dalla tecnologia proposta, in particolare se i confini tra l'uso aziendale e privato sono labili.

5.4.2 *BRING YOUR OWN DEVICE (BYOD)*

A causa dell'aumento della popolarità, delle caratteristiche e delle capacità dei dispositivi elettronici di consumo, i datori di lavoro possono trovarsi nella situazione di gestire le richieste di dipendenti che intendono utilizzare i loro dispositivi personali sul posto di lavoro per svolgere i propri compiti. Tale fenomeno è noto come "*bring your own device*" (abbreviato in BYOD), che indica appunto l'utilizzo di propri dispositivi personali.

L'attuazione efficace di questa politica può comportare una serie di vantaggi per i dipendenti, tra cui una maggiore soddisfazione nei confronti del proprio lavoro, un aumento del morale complessivo, una maggiore efficienza sul lavoro e una maggiore flessibilità. Tuttavia, per definizione, il dispositivo del dipendente sarà in parte usato per fini personali, con più probabilità in determinati momenti della giornata (ad esempio la sera e nei fine settimana). Di conseguenza, esiste la possibilità concreta che l'uso di dispositivi propri da parte dei dipendenti comporti un trattamento da parte dei datori di lavoro di informazioni non aziendali relative a tali dipendenti ed eventualmente a qualsiasi loro familiare che utilizzi i dispositivi in questione.

Nei rapporti di lavoro, i rischi per la vita privata derivanti dall'uso di dispositivi propri sono comunemente associati a tecnologie di monitoraggio che raccolgono identificatori quali gli indirizzi MAC oppure ai casi in cui il datore di lavoro accede al dispositivo del dipendente con la giustificazione di effettuare una scansione per finalità di sicurezza, ad esempio per rilevare la presenza di malware. In questi ultimi casi esistono numerose soluzioni commerciali che consentono la scansione di dispositivi privati; tuttavia il loro utilizzo potrebbe concedere potenzialmente accesso a tutti i dati presenti sul dispositivo, pertanto devono essere gestite con attenzione. Ad esempio, in linea di principio, non si dovrebbe accedere alle sezioni del dispositivo che si presume vengano utilizzate esclusivamente per scopi privati (ad esempio la cartella dedicata alla conservazione di immagini scattate tramite il dispositivo).

Il monitoraggio dell'ubicazione e del traffico di tali dispositivi può essere considerato rientrare nel legittimo interesse di proteggere i dati personali per i quali il datore di lavoro è responsabile in qualità di titolare del trattamento; tuttavia potrebbe essere illecito quando riguarda un dispositivo personale di un dipendente e permette di acquisire anche dati relativi alla vita privata e familiare del dipendente. Per impedire il monitoraggio delle informazioni private, è necessario che siano attuate misure appropriate per distinguere tra l'uso privato e quello aziendale del dispositivo.

I datori di lavoro dovrebbero altresì attuare sistemi che consentano il trasferimento sicuro, tra il dispositivo del dipendente e la propria rete, dei propri dati presenti sul dispositivo. Il dispositivo potrebbe quindi essere configurato in modo tale da indirizzare tutto il traffico attraverso una VPN in ritorno nella rete aziendale, in modo da offrire un certo livello di sicurezza; tuttavia, laddove utilizzi una simile misura, il datore di lavoro dovrebbe tenere conto del fatto che il software installato per finalità di monitoraggio costituisce un rischio per la vita privata del dipendente quando questi usa il dispositivo per fini personali. Si potrebbero anche utilizzare soluzioni di protezione supplementare quali lo "*sandboxing*", che prevede la conservazione dei dati in un'applicazione specifica.

Per contro, il datore di lavoro deve anche valutare la possibilità di vietare l'uso di dispositivi di lavoro specifici per fini privati qualora non sia possibile impedire il monitoraggio dell'uso

privato, ad esempio se il dispositivo in questione consente l'accesso remoto a dati personali per i quali il datore di lavoro è il titolare del trattamento.

5.4.3 *GESTIONE DEI DISPOSITIVI MOBILI (MOBILE DEVICE MANAGEMENT)*

La gestione dei dispositivi mobili consente ai datori di lavoro di localizzare i dispositivi a distanza, di installare configurazioni e/o applicazioni specifiche e di eliminare dati su richiesta. Un datore di lavoro può gestire questa funzionalità autonomamente oppure darne l'incarico a terzi. I servizi di gestione dei dispositivi mobili consentono inoltre ai datori di lavoro di registrare o tracciare il dispositivo in tempo reale anche quando non ne è stato segnalato il furto.

Prima di impiegare una simile tecnologia, laddove essa sia nuova o comunque nuova per il titolare del trattamento, è necessario effettuare una valutazione d'impatto sulla protezione dei dati. Se dalla valutazione emerge che la tecnologia di gestione dei dispositivi mobili è necessaria in specifiche circostanze, si dovrebbe in ogni caso effettuare una valutazione della conformità ai principi di proporzionalità e sussidiarietà del trattamento dei dati risultante. I datori di lavoro devono assicurarsi che i dati raccolti nel contesto di tale capacità di localizzazione remota siano trattati per finalità specifiche e non costituiscano, o non possano costituire, parte di un programma più ampio che consente il monitoraggio continuo dei dipendenti. Anche in caso di finalità specifiche, le caratteristiche di tracciamento dovrebbero essere attenuate. I sistemi di tracciamento possono essere progettati per registrare i dati relativi all'ubicazione senza presentarli al datore di lavoro: in tal caso, i dati relativi all'ubicazione dovrebbero essere resi disponibili soltanto nelle circostanze in cui il dispositivo venga segnalato come rubato o perso.

I dipendenti i cui dispositivi sono inseriti in tali servizi di gestione dei dispositivi mobili devono essere pienamente informati sul tipo di tracciamento attuato e sulle sue conseguenze nei loro confronti.

5.4.4 *DISPOSITIVI INDOSSABILI*

I datori di lavoro sono sempre più tentati di fornire dispositivi indossabili ai propri dipendenti per tracciarne e monitorarne la salute e l'attività all'interno e talvolta anche all'esterno del posto di lavoro. Tuttavia, un tale trattamento implica il trattamento di dati relativi alla salute ed è pertanto vietato a norma dell'articolo 8 della direttiva sulla protezione dei dati.

Dato l'impari rapporto tra datori di lavoro e dipendenti, dovuto alla dipendenza finanziaria dei secondi nei confronti dei primi, nonché data la natura sensibile dei dati relativi alla salute, è altamente improbabile che possa essere concesso un consenso esplicito legalmente valido al tracciamento o al monitoraggio di tali dati, in quanto i dipendenti non sono sostanzialmente "liberi" di concedere tale consenso in primo luogo. Anche qualora il datore di lavoro si rivolga a un terzo per la raccolta dei dati relativi alla salute e il terzo gli fornisca poi soltanto informazioni aggregate sugli sviluppi generali in materia di salute, tale trattamento sarebbe comunque illecito.

Inoltre, come descritto nel *parere 5/2014 sulle tecniche di anonimizzazione*[18], è tecnicamente molto difficile garantire una completa anonimizzazione dei dati. Anche in un contesto con più

[18] Gruppo di lavoro Articolo 29, *Parere 5/2014 sulle tecniche di anonimizzazione*, WP 216 del 10 aprile 2014, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf.

di mille dipendenti, considerata la disponibilità di altri dati sui dipendenti, il datore di lavoro potrebbe comunque essere in grado di individuare i singoli dipendenti disponendo di particolari indicazioni in merito alla loro salute, quali l'ipertensione o l'obesità.

Esempio

Un'organizzazione offre dispositivi di monitoraggio della forma fisica ai propri dipendenti come regalo generalizzato. I dispositivi contano il numero di passi compiuti dai dipendenti, ne registrano il battito cardiaco e i modelli di sonno nel corso del tempo.

I risultanti dati relativi alla salute dovrebbero essere accessibili esclusivamente ai dipendenti e non al datore di lavoro. Qualsiasi dato trasferito tra il dipendente (in qualità di interessato) e il prestatore di servizi/del dispositivo (in qualità di titolare del trattamento) è una questione che riguarda solo tali parti.

Poiché i dati relativi alla salute potrebbero essere trattati anche dalla parte commerciale che ha prodotto i dispositivi o che offre un servizio al datore di lavoro, nello scegliere il dispositivo o il servizio il datore di lavoro dovrebbe valutare la politica in materia di tutela della vita privata attuata dal fabbricante e/o dal prestatore di servizi, al fine di assicurarsi che non dia adito a un trattamento illecito dei dati relativi alla salute dei dipendenti.

5.5 Trattamenti relativi agli orari e alle presenze

Anche i sistemi che consentono ai datori di lavoro di controllare chi può entrare nei loro locali e/o in determinate aree all'interno degli stessi possono consentire il tracciamento delle attività dei dipendenti. Sebbene tali sistemi esistano da diversi anni, le nuove tecnologie di tracciamento degli orari e delle presenze dei dipendenti sono ora più diffuse, incluse quelle che elaborano dati biometrici e altre quali il tracciamento di dispositivi mobili.

Nonostante tali sistemi possano costituire una componente importante della traccia di controllo di un datore di lavoro, essi presentano anche il rischio di fornire un livello invasivo di conoscenza e controllo in merito alle attività del dipendente sul posto di lavoro.

Esempio

Un datore di lavoro dispone di una sala server nella quale sono conservati, in formato digitale, i dati sensibili per l'attività aziendale e i dati personali relativi ai dipendenti e ai clienti. Al fine di rispettare gli obblighi legali che impongono di proteggere tali dati dall'accesso non autorizzato, il datore di lavoro ha installato un sistema di controllo degli accessi che registra l'ingresso e l'uscita dei dipendenti che dispongono dell'opportuna autorizzazione per accedere a tale stanza. In caso di perdita di un componente dell'apparecchiatura oppure di accesso non autorizzato ai dati o loro perdita o furto, le registrazioni conservate dal datore di lavoro gli consentono di stabilire chi ha avuto accesso alla stanza in quel momento.

Dato che è necessario e non viola il diritto alla vita privata dei dipendenti, il trattamento può essere svolto in virtù di un legittimo interesse a norma dell'articolo 7, lettera f), purché i dipendenti ne siano adeguatamente informati. Tuttavia, il monitoraggio continuo della frequenza e degli orari precisi di entrata e uscita dei dipendenti non può essere giustificato se tali dati vengono utilizzati anche per altre finalità, quali ad esempio la valutazione del rendimento dei dipendenti.

5.6 Trattamenti utilizzando sistemi di monitoraggio video

Il monitoraggio video e la videosorveglianza continuano a presentare problemi analoghi in materia di tutela della vita privata dei dipendenti rispetto a quelli riscontrati in passato: tali sistemi consentono di acquisire continuamente informazioni sul comportamento del lavoratore[19]. Le modifiche più rilevanti relative all'applicazione di questa tecnologia nei rapporti di lavoro sono la possibilità di accedere facilmente a distanza ai dati raccolti (ad esempio tramite uno smartphone), la riduzione delle dimensioni delle telecamere (associata a un aumento delle loro capacità, ad esempio in termini di alta definizione) e il trattamento che può essere effettuato dalle nuove soluzioni di analisi video.

Grazie alle funzionalità offerte dalle soluzioni di analisi video, il datore di lavoro ha la possibilità di controllare le espressioni facciali del lavoratore utilizzando mezzi automatizzati al fine di individuare deviazioni da modelli di movimento predefiniti (ad esempio nel contesto di una fabbrica) e molto altro ancora. Ciò sarebbe sproporzionato nei confronti dei diritti e delle libertà dei dipendenti e, di conseguenza, in linea di principio, illecito. È probabile inoltre che tale trattamento comporti la profilazione ed, eventualmente, l'adozione di decisioni automatizzate. Pertanto, i datori di lavoro dovrebbero astenersi dall'uso di tecnologie di riconoscimento facciale. Vi possono essere alcune eccezioni a questa regola, tuttavia tali scenari non possono essere utilizzati per invocare una legittimazione generale dell'utilizzo di tale tecnologia[20].

5.7 Trattamenti che coinvolgono veicoli utilizzati dai dipendenti

Le tecnologie che consentono ai datori di lavoro di monitorare i propri veicoli sono attualmente ampiamente adottate in particolare nel contesto di organizzazioni che svolgono attività di trasporto o che dispongono di flotte notevoli di veicoli.

Qualsiasi datore di lavoro che utilizzi dispositivi telematici a bordo di veicoli raccoglierà dati in merito al veicolo e al singolo dipendente che utilizza tale veicolo. Tali dati possono includere non solo la posizione del veicolo (e quindi del dipendente) raccolta dai sistemi di tracciamento di base GPS, ma anche molte altre informazioni, a seconda della tecnologia, compreso il comportamento di guida. Talune tecnologie possono altresì consentire un monitoraggio continuo tanto del veicolo quanto del conducente (si pensi ad esempio ai registratori di dati relativi ad eventi).

Un datore di lavoro potrebbe essere tenuto a installare tale tecnologia di monitoraggio a bordo dei veicoli per dimostrare la conformità ad altri obblighi legali, ad esempio per garantire la sicurezza dei dipendenti che guidano tali veicoli. Il datore di lavoro può anche avere un legittimo interesse a poter individuare i veicoli in qualsiasi momento. Sebbene i datori di lavoro possano disporre di un legittimo interesse a raggiungere tali scopi, occorre innanzitutto valutare se il trattamento per dette finalità sia necessario e se l'effettiva attuazione sia conforme ai principi di proporzionalità e sussidiarietà. Qualora sia consentito l'uso privato di un veicolo professionale, la misura più importante che un datore di lavoro può adottare per garantire il rispetto di tali principi consiste nell'offrire un'opzione di esclusione: in linea di principio, il dipendente dovrebbe avere la possibilità di disattivare

[19] Cfr. il caso citato in precedenza, *Köpke contro Germania*; va altresì osservato che in alcune giurisdizioni è stata riconosciuta come ammissibile l'installazione di sistemi quali quelli di televisione a circuito chiuso al fine di provare un comportamento illecito; cfr. il caso *Bershka* presso la Corte costituzionale di Spagna.

[20] Inoltre, ai sensi del regolamento generale sulla protezione dei dati, il trattamento di dati biometrici per finalità di identificazione deve basarsi su un'eccezione tra quelle previste all'articolo 9, paragrafo 2.

temporaneamente il tracciamento della posizione qualora circostanze particolari lo giustifichino, ad esempio nel caso in cui si rechi a una visita medica. In questo modo, il dipendente può, di propria iniziativa, proteggere determinati dati relativi all'ubicazione considerati privati. Il datore di lavoro deve garantire che i dati raccolti non vengano utilizzati per un ulteriore trattamento illegittimo, per finalità di tracciamento o valutazione dei dipendenti.

Il datore di lavoro deve altresì informare con chiarezza i dipendenti che a bordo del veicolo aziendale da loro guidato è stato installato un dispositivo di tracciamento e che i loro movimenti vengono registrati durante l'uso di detto veicolo (e che, a seconda della tecnologia in questione, potrà essere registrato anche il loro comportamento di guida). Preferibilmente tali informazioni dovrebbero essere esposte in maniera visibile a bordo di ogni vettura, nel campo visivo del conducente.

È possibile che i dipendenti utilizzino veicoli aziendali al di fuori degli orari di lavoro, ad esempio per uso personale, a seconda delle politiche specifiche che disciplinano l'uso di tali veicoli. Data la sensibilità dei dati relativi all'ubicazione, è improbabile che vi sia una base giuridica per il monitoraggio delle posizioni dei veicoli dei lavoratori al di fuori dall'orario di lavoro concordato. Tuttavia, laddove sussista una tale necessità, si dovrebbe prendere in considerazione un'attuazione che sia proporzionata ai rischi. Ad esempio, ciò potrebbe significare che, per prevenire il furto dell'auto, la posizione della stessa non venga registrata al di fuori dell'orario di lavoro a meno che il veicolo non abbandoni una zona ben definita (regione o persino paese). Inoltre, la posizione dovrebbe essere visualizzata soltanto in caso di emergenza: ossia il datore di lavoro dovrebbe poter attivare la "visibilità" della posizione, accedendo ai dati già memorizzati dal sistema, soltanto nel momento in cui il veicolo lascia una regione predefinita.

Come indicato nel *parere 13/2011 sui servizi di geolocalizzazione su dispositivi mobili intelligenti*[21]:

> "I dispositivi di tracciamento dei veicoli non sono dispositivi di tracciamento del personale, bensì 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".

[21] Gruppo di lavoro Articolo 29, *Parere 13/2011 sui servizi di geolocalizzazione su dispositivi mobili intelligenti*, WP 185 del 16 maggio 2011, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_it.pdf.

Inoltre, come indicato nel *parere 5/2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto*[22]:

"Il trattamento dei dati relativi all'ubicazione può essere giustificato quando è effettuato nell'ambito dei controlli sul trasporto di persone o cose ovvero al fine di migliorare la distribuzione delle risorse per i servizi in località remote (ad esempio, in rapporto alla pianificazione in tempo reale delle operazioni) o quando si persegue un obiettivo di sicurezza che è collegato al lavoratore stesso o ai beni o veicoli a lui affidati. Viceversa, il Gruppo ritiene che il trattamento dei dati sia eccessivo se i lavoratori sono liberi di organizzare i loro spostamenti come desiderano, o se il controllo della loro attività lavorativa costituisce la sola finalità di tale trattamento e tale controllo potrebbe essere realizzato con altri mezzi".

5.7.1 REGISTRATORI DI DATI RELATIVI A EVENTI

I registratori di dati relativi a eventi forniscono al datore di lavoro la capacità tecnica di trattare una quantità notevole di dati personali in merito ai dipendenti che guidano veicoli aziendali. Tali dispositivi vengono installati con frequenza sempre maggiore a bordo dei veicoli con l'obiettivo di effettuare registrazioni video, possibilmente inclusive di audio, in caso di incidente. Questi sistemi sono in grado di effettuare le registrazioni in determinati momenti, ad esempio, in risposta a frenate improvvise, improvvisi cambiamenti di direzione o incidenti, nel qual caso vengono conservati anche i momenti immediatamente precedenti l'incidente; tuttavia tali sistemi possono anche essere impostati per effettuare un monitoraggio continuo. Successivamente queste informazioni possono essere utilizzate per osservare e riesaminare il comportamento di guida di una persona allo scopo di migliorarlo. Inoltre, molti di questi sistemi includono una funzionalità GPS che consente il tracciamento della posizione del veicolo in tempo reale e la conservazione per finalità di ulteriore trattamento di altri dettagli relativi alla guida (ad esempio la velocità del veicolo).

Tali dispositivi sono diventati particolarmente diffusi tra le organizzazioni che svolgono attività di trasporto o che dispongono di flotte notevoli di veicoli. Tuttavia, l'impiego di registratori di dati relativi a eventi può essere considerato lecito soltanto se esiste una necessità effettiva di trattare i risultanti dati personali del dipendente per finalità legittime e tale trattamento è conforme ai principi di proporzionalità e sussidiarietà.

Esempio

Un'impresa di trasporti dota tutti i propri veicoli di una videocamera all'interno dell'abitacolo che registra suoni e video. La finalità del trattamento di questi dati è il miglioramento delle capacità di guida dei dipendenti. Le telecamere sono configurate in maniera tale da conservare le registrazioni qualora si verifichino frenate improvvise o bruschi cambiamenti di direzione. L'impresa presume di disporre di un fondamento giuridico per il trattamento nel proprio legittimo interesse legittimo a norma dell'articolo 7, lettera f), della direttiva, al fine di proteggere la sicurezza dei propri dipendenti e quella degli altri conducenti.

Tuttavia, il legittimo interesse dell'impresa a monitorare i conducenti non prevale sui diritti di questi ultimi alla protezione dei loro dati personali. Il monitoraggio continuo dei dipendenti per mezzo di tali telecamere costituisce un'interferenza grave nel loro diritto alla tutela della

[22] Gruppo di lavoro Articolo 29, *Parere 5/2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto*, WP 115 del 25 novembre 2005, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_it.pdf.

vita privata. Esistono altri metodi (ad esempio, l'installazione di apparecchiature che impediscono l'utilizzo di telefoni cellulari) e altri sistemi di sicurezza, tra i quali un sistema avanzato di frenatura di emergenza o un sistema di avviso di deviazione dalla corsia, che possono essere impiegati per prevenire incidenti stradali e che possono essere più appropriati. Inoltre, esiste un'elevata probabilità che la presenza di tale registrazione determini il trattamento di dati personali di terzi (come i pedoni) e, per tale trattamento, il legittimo interesse dell'impresa non costituisce una giustificazione sufficiente.

5.8 Trattamenti che implicano la divulgazione di dati dei dipendenti a terzi

È diventata sempre più comune la prassi delle imprese di trasmettere i dati dei propri dipendenti ai propri clienti con l'obiettivo di garantire la prestazione di un servizio affidabile. In alcuni casi possono essere forniti anche dati eccessivi, a seconda della portata dei servizi forniti (ad esempio, qualora si includa una foto di un dipendente). Tuttavia, in considerazione dello squilibrio di potere, i dipendenti non sono in una posizione tale da poter concedere un libero consenso al trattamento dei loro dati personali da parte del loro datore di lavoro, e se il trattamento dei dati non è proporzionale, il datore di lavoro non può fare valere alcun fondamento giuridico.

Esempio

Un'impresa di spedizioni invia ai propri clienti un messaggio di posta elettronica con un collegamento al nome e alla posizione dell'incaricato alla consegna della loro spedizione (dipendente di detta impresa). L'impresa voleva altresì includere una foto in formato fototessera dell'incaricato alla consegna, ritenendo di poter fare valere un fondamento giuridico per tale trattamento svolto nel suo legittimo interesse (articolo 7, lettera f), della direttiva) di consentire al cliente di verificare che la persona che effettua la consegna sia effettivamente la persona all'uopo preposta.

Tuttavia, non è necessario fornire ai clienti il nome e la foto dell'incaricato alla consegna. Non sussistendo alcun motivo di legittimazione per tale trattamento, l'impresa di spedizioni non è autorizzata a fornire tali dati personali ai clienti.

5.9 Trattamenti che comportano trasferimenti internazionali di dati relativi alle risorse umane e altri dati dei dipendenti

I datori di lavoro utilizzano sempre più frequentemente applicazioni e servizi basati sul cloud, come quelli progettati per la gestione di dati relativi alle risorse umane, nonché le applicazioni per ufficio usufruibili online. L'utilizzo della maggior parte di queste applicazioni comporta il trasferimento internazionale di dati a partire dai dipendenti e relativi ai dipendenti. Come già indicato nel parere 8/2001, l'articolo 25 della direttiva stabilisce che i trasferimenti di dati personali a un paese terzo al di fuori dell'UE possono aver luogo soltanto se detto paese garantisce un livello di protezione adeguato. Indipendentemente dalla base giuridica applicata, il trasferimento deve soddisfare le disposizioni sancite dalla direttiva.

Di conseguenza, occorre garantire che siano rispettate le disposizioni relative al trasferimento internazionale di dati. Il Gruppo di lavoro ribadisce la sua posizione precedente secondo la quale è preferibile attuare un'adeguata protezione piuttosto che ricorrere alle deroghe di cui all'articolo 26 della direttiva sulla protezione dei dati. Inoltre, laddove si intenda far valere il consenso, quest'ultimo deve essere specifico, inequivocabile e liberamente concesso. Tuttavia, si dovrebbe altresì garantire che la condivisione dei dati al di fuori dell'UE/del SEE

e l'accesso successivo a detti dati da parte di altre entità appartenenti al medesimo gruppo di imprese rimangano limitati al minimo necessario per le finalità previste.

6. Conclusioni e raccomandazioni

6.1 Diritti fondamentali

I contenuti delle comunicazioni di cui sopra, nonché i dati relativi al traffico connessi a tali comunicazioni, beneficiano delle stesse protezioni in materia di diritti fondamentali riconosciute per le comunicazioni "analogiche".

Le comunicazioni elettroniche effettuate a partire dai locali aziendali possono rientrare nelle nozioni di "vita privata" e "corrispondenza" ai sensi dell'articolo 8, paragrafo 1, della Convenzione europea dei diritti dell'uomo. Ai sensi della direttiva sulla protezione dei dati attualmente in vigore, i datori di lavoro possono raccogliere dati soltanto per finalità legittime e il trattamento correlato deve svolgersi in condizioni adeguate (ad esempio deve essere proporzionato e necessario, attuato a fronte di un interesse effettivo e presente, in maniera lecita, articolata e trasparente) e fondarsi su una base giuridica per il trattamento dei dati personali raccolti o generati tramite comunicazioni elettroniche.

Il fatto che il datore di lavoro sia proprietario delle apparecchiature elettroniche utilizzate non esclude il diritto dei dipendenti alla segretezza delle loro comunicazioni, dei dati relativi all'ubicazione e della corrispondenza. Il tracciamento dell'ubicazione dei dipendenti attraverso dispositivi di loro proprietà o messi a disposizione dall'impresa dovrebbe essere limitato ai casi strettamente necessari per finalità legittime. Sicuramente, in caso di uso di dispositivi di proprietà dei dipendenti è importante che questi ultimi abbiano la possibilità di proteggere le loro comunicazioni private da qualsiasi monitoraggio legato all'attività lavorativa.

6.2 Consenso; legittimo interesse

I dipendenti non sono quasi mai nella posizione di poter concedere, rifiutare o revocare liberamente il consenso al trattamento dei dati, considerata la dipendenza derivante dal rapporto datore di lavoro/dipendente. In considerazione di tale squilibrio di potere, i dipendenti possono concedere liberamente il consenso soltanto in circostanze eccezionali nelle quali l'accettazione o il rifiuto di un'offerta non ha conseguenze per loro.

Talvolta come fondamento giuridico può essere invocato il legittimo interesse dei datori di lavoro, ma solo se il trattamento è strettamente necessario per conseguire finalità legittime ed è conforme ai principi di proporzionalità e di sussidiarietà. Prima di usare un qualsiasi strumento di monitoraggio è opportuno effettuare una prova della proporzionalità per valutare se tutti i dati sono necessari, se il trattamento viola i diritti generali alla vita privata di cui godono i dipendenti anche sul posto di lavoro, e le misure da adottare per garantire che le violazioni dei diritti alla vita privata e alla segretezza delle comunicazioni siano limitate al minimo necessario.

6.3 Trasparenza

Si dovrebbero informare efficacemente i dipendenti su qualsiasi monitoraggio che venga attuato, sulle sue finalità e sulle circostanze nelle quali viene svolto, nonché sulle possibilità di cui dispongono i dipendenti per impedire che i propri dati vengano acquisiti mediante tecnologie di monitoraggio. Le politiche e le norme riguardanti il monitoraggio legittimo devono essere chiare e facilmente accessibili. Il Gruppo di lavoro raccomanda di coinvolgere un campione rappresentativo di dipendenti nel processo di creazione e valutazione di tali norme e politiche, in quanto la maggior parte dei monitoraggi può potenzialmente violare la vita privata dei dipendenti.

6.4 Proporzionalità e minimizzazione dei dati

Il trattamento dei dati sul posto lavoro deve essere una risposta proporzionata ai rischi che il datore di lavoro deve gestire. Ad esempio, l'uso improprio di Internet può essere rilevato senza la necessità di analizzare i contenuti dei siti web visitati. Laddove sia possibile prevenire tale uso improprio (ad esempio, utilizzando filtri web), il datore di lavoro non ha alcun diritto generale di effettuare il monitoraggio.

Inoltre, un divieto assoluto di effettuare comunicazioni per motivi personali è poco pratico e la sua applicazione può richiedere un livello di monitoraggio che può essere sproporzionato. Si dovrebbe privilegiare la prevenzione rispetto alla rilevazione: gli interessi del datore di lavoro risultano protetti meglio prevenendo un uso improprio di Internet con mezzi tecnici, piuttosto che spendendo risorse per individuare gli usi impropri.

Le informazioni registrate tramite il monitoraggio costante, nonché le informazioni mostrate al datore di lavoro, dovrebbero essere limitate al minimo possibile. I dipendenti dovrebbero avere la possibilità di interrompere temporaneamente il tracciamento dell'ubicazione, qualora ciò sia giustificato dalle circostanze. Le soluzioni deputate ad esempio al tracciamento dei veicoli possono essere progettate in maniera tale da registrare i dati relativi all'ubicazione senza presentarli al datore di lavoro.

I datori di lavoro devono tenere in considerazione il principio della minimizzazione dei dati quando decidono di usare nuove tecnologie. Le informazioni dovrebbero essere conservate per il tempo minimo necessario, specificando il periodo di conservazione. Allorché le informazioni non sono più necessarie, dovrebbero essere cancellate.

6.5 Servizi cloud, applicazioni online e trasferimenti internazionali

Laddove i dipendenti siano tenuti a utilizzare applicazioni online che trattano dati personali (ad esempio applicazioni per ufficio online), i datori di lavoro dovrebbero prendere in considerazione la possibilità di consentire ai dipendenti di designare taluni spazi privati ai quali il datore di lavoro non può accedere in nessuna circostanza, ad esempio una casella di posta elettronica privata o una cartella di documenti.

L'utilizzo della maggior parte delle applicazioni tramite il cloud comporterà il trasferimento internazionale dei dati dei dipendenti. Di conseguenza, occorre garantire che il trasferimento di dati personali in un paese terzo al di fuori dell'UE avvenga esclusivamente se è garantito un adeguato livello di protezione e se la condivisione dei dati al di fuori dell'UE/del SEE e il successivo accesso agli stessi da parte di altre entità appartenenti al medesimo gruppo di imprese rimangano limitati al minimo necessario per le finalità previste.

* * *

Fatto a Bruxelles, l'8 giugno 2017

Per il Gruppo
La presidente
Isabelle FALQUE-PIERROTIN