

Diritto e Giustizia

IL QUOTIDIANO DI INFORMAZIONE GIURIDICA



**Il trattamento dei dati personali dei lavoratori: un quadro operativo aggiornato
delle regole applicabili, tra i principi del Regolamento Generale UE sulla
protezione dei dati e le prescrizioni pratiche del Parere dei Garanti UE n. 2/2017
("Trattamento dei dati sui luoghi di lavoro")**

del Prof. Avv. Alessandro del Ninno

Indice

§ 1. *Il trattamento dei dati personali dei lavoratori nell'ambito dei rapporti di lavoro nel Regolamento UE 679/2016: un quadro di insieme dal Considerando n. 155 all'art. 88 RGPD e l'infelice scelta del rinvio ad ulteriori norme nazionali.*

§ 2. *Il Parere dei Garanti UE n. 2/2017 "Trattamento dei dati sui luoghi di lavoro": il quadro generale. La validità (quasi nulla) del consenso del lavoratore quale base giuridica del trattamento: le conseguenze pratiche.*

§ 3. *I nove scenari pratici del Parere 2/2017 sul trattamento di dati dei lavoratori sui luoghi di lavoro: le regole operative.*

§ 3.1. *Segue - Scenario n. 1: il trattamento dei dati personali nel contesto delle attività di recruitment.*

§ 3.2. *Segue - Scenario n. 2: il trattamento dei dati personali derivante delle attività di screening del lavoratore nel corso o a seguito della cessazione del rapporto lavorativo ("in-employment screening").*

§ 3.3. *Segue - Scenario n. 3: il trattamento dei dati personali del lavoratore nel contesto delle attività di controllo e monitoraggio attuate dal datore di lavoro circa l'utilizzo di risorse e strumenti ICT sul luogo di lavoro.*

§ 3.4. *Segue - Scenario n. 4: trattamento dei dati personali del lavoratore nel contesto delle attività di controllo e monitoraggio attuate dal datore di lavoro circa l'utilizzo di risorse e strumenti ICT al di fuori della sede lavorativa e dell'orario di lavoro.*

§ 3.5. *Segue - Scenario n. 5: trattamento dei dati personali del lavoratore nel contesto delle attività di verifica delle presenze e dell'orario lavorativo.*

§ 3.6. *Segue - Scenario n. 6: trattamento dei dati personali del lavoratore nel contesto della operatività di sistemi di videosorveglianza nei luoghi di lavoro.*

§ 3.7. *Segue - Scenario n. 7: trattamento dei dati personali del lavoratore raccolti nel contesto di utilizzo di veicoli geolocalizzabili assegnati a dipendenti.*

§ 3.8. *Segue - Scenario n. 8: trattamento dei dati personali del lavoratore nel contesto delle attività di comunicazione dei dati dei lavoratori a terze parti.*

§ 3.9. *Segue - Scenario n. 9: trattamento dei dati personali nel contesto delle attività di trasferimento internazionale di informazioni riferite ai lavoratori.*

§ 1. Il trattamento dei dati personali dei lavoratori nell'ambito dei rapporti di lavoro nel Regolamento UE 679/2016: un quadro di insieme dal Considerando n. 155 all'art. 88 RGPD e l'infelice scelta del rinvio ad ulteriori norme nazionali.

Il trattamento dei dati dei lavoratori nel Regolamento Generale UE sulla protezione dei dati personali n. 679/2016 (di seguito, "RGPD") riceve una particolare attenzione in termini di garanzia per tali specifici interessati: se è vero difatti che il RGPD menziona – tra i Considerando e il testo egli articoli - varie categorie di persone fisiche i cui dati sono oggetto di trattamento (es: i "clienti", i "pazienti", gli "utenti") è solo ai "dipendenti" (con curiosa specificità lavoristica, che potrebbe creare qualche problema interpretativo e applicativo per le diverse qualifiche dei lavoratori non dipendenti) che dedica un articolo specifico. Infatti, l'art. 88 del RGPD, rubricato *"Trattamento dei dati nell'ambito dei rapporti di lavoro"* contiene delle importanti disposizioni che prevedono la possibilità - a livello di legislazioni nazionali dei singoli Stati Membri - di ulteriori misure legislative di protezione addizionale dei lavoratori sui luoghi di lavoro.

Difatti, ai sensi della citata disposizione, gli Stati membri possono addirittura prevedere *"norme più specifiche"* (rispetto ai principi generali, agli istituti ed agli obblighi in via generale previsti dal RGPD) per tutelare i diritti e le libertà nel *"trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro"*, in particolare per finalità di:

1. assunzione;
2. esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi;
3. gestione, pianificazione e organizzazione del lavoro;
4. predisposizione delle garanzie di parità e diversità sul posto di lavoro;
5. salute e sicurezza sul lavoro;
6. protezione della proprietà del datore di lavoro o del cliente;
7. esercizio e godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro;
8. cessazione del rapporto di lavoro.

L'articolo 88 individua anche gli specifici strumenti giuridici per l'introduzione sul piano nazionale di ulteriori misure di tutela nel trattamento dei dati dei lavoratori (*"leggi"*, *"contratti collettivi"* e - la specifica è contenuta nel Considerando n. 155 - *"accordi aziendali"*) e l'oggetto di peculiare tutela che tali specifiche norme nazionali dovranno nel caso disciplinare: si dovrà cioè trattare di misure appropriate e specifiche a salvaguardia della dignità umana, dei diritti fondamentali e degli interessi legittimi dei lavoratori 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.

La scelta del Legislatore UE di rinviare agli ordinamenti giuridici nazionali e di consentire l'adozione di misure statali più specifiche per la tutela dei dati dei lavoratori lascia davvero

perplessi, soprattutto in rapporto alla finalità del RGPD di creare un quadro che dovrebbe essere (ma non sarà affatto) omogeneo di regole sul trattamento dei dati personali nell'Unione Europea. Invece, con l'apertura dell'art. 88, in un settore così delicato e rilevante per la vita delle imprese come il mercato del lavoro, che si esplica oramai in scenari tecnologizzati e globalizzati, ai datori di lavoro (si pensi alle grandi imprese con più sedi nella UE) non sarà sufficiente garantirsi la *compliance* al RGPD nel trattamento dei dati di dipendenti ubicati in varie sedi nella UE, ma essi dovranno andare alla ricerca (con i costi organizzativi e consulenziali immaginabili) delle eventuali fonti nazionali (non solo leggi, ma contratti collettivi e accordi aziendali) che regolamentano con *"misure più specifiche"* i trattamenti dei dati dei lavoratori negli Stati ove l'azienda abbia eventualmente sedi. E a tali misure più specifiche (che ogni Stato membro notificherà alla Commissione entro il 25 maggio 2018, inclusa - successivamente - ogni intervenuta modifica) i titolari del trattamento dovranno adeguarsi, implementando le eventuali necessità tecniche ed organizzative richieste da Stato a Stato.

Le perplessità di una tale scelta normativa aumentano se poi si guarda alla ampiezza dei possibili trattamenti di dati dei lavoratori nel periodo che va dalla assunzione alla cessazione del rapporto di lavoro (e quindi alla conseguente possibile frammentazione di numerose norme nazionali più specifiche che potranno essere adottate dai 28 Stati Membri o che sono già vigenti e semplicemente da notificare alla Commissione UE) e se si considera che le *"misure appropriate e specifiche a salvaguardia della dignità umana, dei diritti fondamentali e degli interessi legittimi"* dei lavoratori interessati dovranno nel caso riguardare i trattamenti più importanti nella prospettiva datoriale: il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale e i sistemi di monitoraggio sul posto di lavoro.

Per fare un esempio pratico, una grande azienda tedesca che opera nel comparto del trasporto aereo con sede anche in Italia, dovrà rendere i trattamenti di dati personali dei dipendenti della sede italiana conformi non solo al RGPD ma anche, tra le altre e per lo meno, alle seguenti misure nazionali più specifiche:

- art. 4 della Legge 300/1970 recante lo Statuto dei lavoratori, per quanto riguarda i controlli sui luoghi di lavoro (che nella sua nuova formulazione successiva alla novella introdotta dal d.lgs. 151/2015 rende applicabili per richiamo tutti i provvedimenti generali in materia emanati dal Garante privacy, come ad esempio le Linee Guida sul trattamento dei dati dei lavoratori nel settore privato, i provvedimenti sulla videosorveglianza, email e Internet sui luoghi di lavoro, etc);
- d.lgs. 81/2008 per i trattamenti di dati personali dei lavoratori svolti a fini di igiene e sicurezza sui luoghi di lavoro;
- l'art. 14 (*"Tutela dei dati personali"*) del Contratto collettivo nazionale di lavoro del settore del trasporto aereo, che prevede specifiche prescrizioni in materia di videosorveglianza.

Infine, il Considerando n. 155 del RGPD precisa ulteriormente (e tale precisazione non è ripetuta ed è assente nell'art. 88) che gli Stati Membri possono prevedere norme specifiche per il trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, *"in particolare per quanto riguarda le condizioni alle quali i dati personali nei rapporti di lavoro possono essere trattati sulla base del consenso del dipendente"*: il che implica, sul piano pratico, che ciascuno Stato UE potrebbe in certi casi, mediante norme nazionali, ritenere non sufficiente la prestazione del consenso del lavoratore come presupposto di legittimità di taluni tra i più delicati trattamenti nell'ambito del rapporto di lavoro: anzi è proprio questa la prospettiva (che definirei di progressivo "depotenziamento" del consenso quale presupposto di legittimità dei trattamenti) che gli stessi Garanti UE riuniti nel Working Party Art. 29 suggeriscono nel Parere dell'8 Giugno 2017 n. 2 che sarà oggetto di analisi e valutazione pratica nell'ambito del presente articolo.

§ 2. Il Parere dei Garanti UE n. 2/2017 "Trattamento dei dati sui luoghi di lavoro": il quadro generale. La validità (quasi nulla) del consenso del lavoratore quale base giuridica del trattamento: le conseguenze pratiche.

Il Parere 2/2017 sul trattamento dei dati sui luoghi di lavoro, adottato dal Working Party art. 29, l'organismo che riunisce a livello UE le Autorità privacy nazionali (e che sarà rimpiazzato a far data dal 25 Maggio 2018 dal *Comitato europeo per la protezione dei dati* previsto dagli art. 68 e ss. del RGPD), aggiorna ed integra i precedenti pareri che il Gruppo dei Garanti UE aveva rilasciato nel 2001 (Opinion 8/2001 *"Trattamento dei dati personali nel contesto lavorativo"*) e nel 2002 (WP55 - *Documento di lavoro sulla sorveglianza delle comunicazioni elettroniche sui luoghi di lavoro*).

Scopo del nuovo parere, che si segnala per l'interessante contenuto di stampo eminentemente pratico ed operativo, con una serie di indicazioni organizzative davvero utili per i datori di lavoro, è quello di:

- aggiornare alle più recenti tecnologie impiegate sui luoghi di lavoro le indicazioni sulla corretta impostazione dei relativi trattamenti dei dati dei lavoratori;
- indicare il corretto bilanciamento tra il legittimo interesse del datore di lavoro e le ragionevoli aspettative di tutela della riservatezza dei lavoratori (sia pure sul luogo di lavoro);
- allineare le regole sul trattamento dei dati sui luoghi di lavoro ai nuovi principi, processi ed istituti previsti dal RGPD.

Il Parere si concentra dunque su nove diversi scenari pratici - frequenti sui luoghi di lavoro - caratterizzati dal rilevante impatto delle nuove tecnologie nel contesto lavorativo (e sui relativi trattamenti di dati personali) e riguarda i "lavoratori" intesi in senso ampio di esistenza di

qualsivoglia relazione lavorativa, indifferentemente se essa sia basata o meno sulla esistenza di un contratto di impiego.

In linea generale, il Parere evidenzia fra le prime indicazioni preliminari ed operative come i datori di lavoro non dovrebbero fare affidamento sul consenso prestato dai lavoratori quale base giuridica del (lecito) trattamento dei dati nel contesto lavorativo, poiché per i Garanti UE il consenso in tale contesto non può mai considerarsi del tutto libero e il rifiuto di prestarlo privo di conseguenze. Dunque, a meno di situazioni eccezionali, per i Garanti UE i datori di lavoro dovrebbero cercare un'altra base giuridica del trattamento (alternativa al consenso), come ad esempio la necessità di procedere al trattamento per perseguire il proprio legittimo interesse.

L'affermazione sulla ridotta (quasi inesistente) validità giuridica del consenso prestato dai lavoratori per il trattamento dei loro dati nell'ambito del rapporto di lavoro può sembrare sorprendente, ma è in linea con la nuova filosofia del RGPD, in base alla quale il consenso informato non è più il principale pilastro su cui poggiare l'intero sistema della protezione dei dati. Difatti, gli stessi Considerando 42 e 43 del RGPD chiaramente statuiscono che:

- a) il consenso non costituisce un valido presupposto per il trattamento dei dati personali qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente;
- b) il consenso non è considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio.

Di conseguenza, considerati i lavoratori alla stregua di "soggetti deboli" nel contesto lavorativo poiché per i Garanti UE esiste un evidente squilibrio tra datore di lavoro-titolare del trattamento e dipendente-interessato, la conseguenza sarebbe quella della invalidità del consenso prestato dal lavoratore come presupposto e base giuridica del trattamento, perché – a priori – tale consenso non sarebbe espresso dal lavoratore in modo autenticamente libero. Dunque, dal punto di vista organizzativo, sarebbero solo casi eccezionali (e da documentare in base al principio dell'*accountability* introdotto dal RGPD) quelli in cui un datore di lavoro può legittimamente avvalersi del consenso informato e libero prestato dal lavoratore.

Chi scrive non è d'accordo con l'assunto aprioristico di una sempre verificata "debolezza" del lavoratore quale soggetto parte del rapporto di lavoro e ciò per una serie di ragioni. La prima: se si pensa a realtà aziendali con una forte presenza sindacale di base (RSA o RSU) quale presidio e garanzia dei lavoratori anche rispetto alle politiche del trattamento dei dati che li riguardano attuate dal datore di lavoro, si riscontrerà che spesso nella realtà pratica l'assunto aprioristico di un lavoratore "soggetto debole" non sempre è corretto e corrisponde ai fatti... La seconda ragione è di ordine più pratico ed organizzativo: negare – di fatto e quasi sempre – la validità del consenso

del lavoratore quale base giuridica del trattamento (o considerarlo valido solo in casi “eccezionali”) determinerà nei contesti lavorativi enormi difficoltà pratiche, soprattutto quando non è possibile richiamare altri presupposti (alternativi al consenso) come ad esempio far valere uno specifico interesse legittimo del datore di lavoro (e d'altra parte gli stessi Garanti privacy UE nel Parere 2/2017 in esame affermano che “*non sempre il legittimo interesse del datore di lavoro è un presupposto di liceità in grado di travalicare i diritti e le libertà dei lavoratori*”).

Facciamo un esempio di possibili difficoltà pratiche derivante dal “depotenziamento” del consenso del lavoratore come base giuridica del trattamento. Una multinazionale petrolifera con sedi anche in Italia deve trasferire i dati dei dipendenti italiani in Russia, ove ha sede legale la casa madre ed ove è ubicata la piattaforma di gestione centralizzata dei dati dei lavoratori di tutte le sedi mondiali della multinazionale. Con riferimento ai presupposti di liceità del trattamento rappresentato dal trasferimento all'estero verso un Paese extra UE, nel caso in esame:

- non è applicabile l'art. 45 RGPD (non esistendo per la Russia una decisione di adeguatezza emanata dalla Commissione UE che abbia deciso che tale paese garantisce un livello di protezione adeguato);
- non è applicabile l'articolo 46 RGPD, in quanto la sede centrale della multinazionale non intende – ad esempio – sottoscrivere con la sede italiana un *data transfer agreement*; oppure non esistono norme vincolanti di impresa, meccanismi di certificazione, adesione a codici di condotta, etc;
- non sono applicabili i presupposti di liceità del trattamento alternativi al consenso di cui all'art. 6 RGPD con riferimento al trattamento e al trasferimento dei dati personali comuni dei lavoratori, in quanto – ad esempio – per il trasferimento extra UE in Russia dei dati del fascicolo del dipendente non potrebbe richiamarsi come base giuridica “*l'obbligo di dare esecuzione ad un contratto*”, che sarebbe nel caso il contratto di lavoro (italiano); né sarebbe applicabile il presupposto del legittimo interesse del datore di lavoro (come anche definito dal Parere 6/2014 dei Garanti UE sul concetto di “legittimo interesse”), che non potrebbe essere ritenuto prevalente sui diritti e sulle libertà fondamentali del lavoratore i cui dati sarebbero trasferiti in un Paese terzo che non garantisce opportune garanzie;
- non sono applicabili i presupposti di liceità del trattamento alternativi al consenso di cui all'art. 9 RGPD con riferimento al trattamento e al trasferimento dei dati personali di particolare natura (ex sensibili) dei lavoratori, in quanto il trasferimento extra UE in Russia dei dati perseguirebbe per il datore di lavoro solo una finalità di più efficiente organizzazione amministrativo-lavoristica e non potrebbe richiamarsi come base giuridica quella di “*assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale*”;
- allo stesso modo, non sono applicabili gli ulteriori presupposti e deroghe previste per il trasferimento extra UE all'art. 49 RGPD.

Resterebbe dunque solo il consenso informato dei dipendenti della sede italiana della multinazionale come valida base del trasferimento dei loro dati in Russia. Ma sarebbe questo un caso “eccezionale” di valida prestazione del consenso? Sarebbe prestato in modo autenticamente libero dai dipendenti? Sarebbe possibile per i dipendenti rifiutare il consenso al trasferimento?

E' ovvio che nell'esempio pratico sopra formulato, che tra l'altro non vedrebbe alternative al consenso del lavoratore per il trasferimento dei dati in Russia, onde evitare di invalidare il consenso sulla base delle motivazioni indicate dai Garanti UE, occorrerebbe:

- a) che l'azienda italiana esportatrice dei dati sottoponga ai lavoratori una informativa trasparente, completa di tutti gli elementi informativi obbligatori e che indichi finalità e modalità del trasferimento, illustri il legittimo interesse datoriale al trasferimento e soprattutto – ai sensi dello specifico obbligo di cui all'art. 49 RGPD – informi i dipendenti *“dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate”*;
- b) che il consenso sia qualificato nella informativa come opzionale (e, ove fornito, come revocabile); dunque occorrerebbe prevedere un effettivo diritto del lavoratore di non autorizzare il trasferimento in un Paese che non garantisce idonee garanzie (o di autorizzarlo selettivamente, solo per talune finalità o solo per talune categorie di dati, ad esempio solo i dati contrattuali e non quelli di particolare natura/sensibili), senza che per tale diniego l'interessato subisca conseguenze di sorta;
- c) che l'interessato sia messo in condizione di prestare in maniera granulare il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche connesse al trasferimento.

Procedendo come appena sopra indicato, si ritiene che potrebbe essere superata nel caso specifico dell'esemplificazione illustrata l'impostazione di un consenso che – aprioristicamente – per i Garanti UE sarebbe - in caso contrario (cioè senza l'adozione delle cautele suggerite) - invalidamente prestato dai lavoratori della multinazionale petrolifera.

§ 3. *I nove scenari pratici del Parere 2/2017 sul trattamento di dati dei lavoratori sui luoghi di lavoro.*

Il Parere 2/2017 prende in esame i seguenti nove scenari di trattamenti di dati sui luoghi di lavoro, nella specifica prospettiva di come le nuove tecnologie e/o gli sviluppi di tecnologie esistenti possono determinare rischi per la privacy dei lavoratori:

- 1. trattamento dei dati personali nel contesto delle attività di *recruitment*;
- 2. trattamento dei dati personali derivante delle attività di *screening* del lavoratore nel corso o a seguito della cessazione del rapporto lavorativo (*“in-employment screening”*);
- 3. trattamento dei dati personali del lavoratore nel contesto delle attività di controllo e monitoraggio attuate dal datore di lavoro circa l'utilizzo di risorse e strumenti ICT sul luogo di lavoro;

4. trattamento dei dati personali del lavoratore nel contesto delle attività di controllo e monitoraggio attuate dal datore di lavoro circa l'utilizzo di risorse e strumenti ICT al di fuori della sede lavorativa e dell'orario di lavoro;
5. trattamento dei dati personali del lavoratore nel contesto delle attività di verifica delle presenze e dell'orario lavorativo;
6. trattamento dei dati personali del lavoratore nel contesto della operatività di sistemi di videosorveglianza nei luoghi di lavoro;
7. trattamento dei dati personali del lavoratore raccolti nel contesto di utilizzo di veicoli geolocalizzabili assegnati a dipendenti;
8. trattamento dei dati personali nel contesto delle attività di comunicazione dei dati dei lavoratori a terze parti;
9. trattamento dei dati personali nel contesto delle attività di trasferimento internazionale di informazioni riferite ai lavoratori.

Inoltre, sempre come considerazione introduttiva, i Garanti UE suggeriscono alla luce del RGPD la effettuazione da parte dei datori di lavoro, e indipendentemente dalla base giuridica del trattamento dei dati, di svolgere sempre un test preventivo ai trattamenti per valutare la proporzionalità dei medesimi, le finalità perseguite come strettamente necessarie e tutte le misure atte a ridurre al minimo i rischi di violazione dei diritti di riservatezza dei lavoratori: suggeriscono cioè di fare una Valutazione di Impatto Privacy, come richiesto dal RGPD, non solo nei casi in cui la PIA è effettivamente obbligatoria (e cioè, a mente dell'art. 35 RGPD, quando un tipo di trattamento prevede in particolare l'uso di nuove tecnologie e considerati la natura, l'oggetto, il contesto e le finalità del trattamento esso può presentare un rischio *elevato* per i diritti e le libertà delle persone fisiche) ma anche quando non lo è, come opportuna buona prassi organizzativa.

§ 3.1. Segue - Scenario n. 1: il trattamento dei dati personali nel contesto delle attività di recruitment: le indicazioni operative.

Lo scenario preso in esame dai Garanti UE è quello della raccolta dei dati dei candidati a posizioni lavorative attraverso lo *screening* dei loro profili sui vari *social media* (nella misura in cui l'accesso a tali profili sia settato come "pubblico" da parte dei titolari degli *account*) o la raccolta sul web di altre informazioni che li riguardano.

Il Parere esclude che il mero fatto della disponibilità di profili "pubblici" sul web autorizzi il datore di lavoro a raccogliere *on line* e a trattare le relative informazioni (d'altra parte, è da sempre principio generale nell'ambito della *data protection* che un dato non è "pubblico" solo perché di fatto è disponibile, ad esempio, su Internet; il dato è "pubblico" - e dunque il trattamento è lecito - solo se qualificato come tale dalle specifiche norme che regolano la pubblicità giuridica).

Non vi è in ogni caso alcuna base giuridica che consenta al potenziale datore di lavoro di chiedere amicizia *on line* al potenziale candidato onde poter conseguire accesso ai contenuti del suo profilo:

ciò è sempre vietato. La base giuridica deve essere quella del legittimo interesse: prima dell'accesso e dello *screening* del *social media* del candidato, il datore di lavoro deve valutare la natura privata o pubblica del profilo. In base al requisito del legittimo interesse il datore di lavoro:

1. può raccogliere dati solo da profili di social media pubblici;
2. può raccogliere da tali profili pubblici e trattare esclusivamente i dati personali proporzionati e necessari in rapporto alla specifica posizione/mansione lavorativa ricercata (ad esempio i dati del profilo pubblico possono essere utili al datore di lavoro per fare l'*assessment* del rischio riguardante candidati a particolari e delicate funzioni lavorative);
3. deve comunque informare preliminarmente i candidati (ad esempio: nell'annuncio di lavoro o nell'informativa *ad hoc*, alla cui redazione dovrà dunque prestarsi particolare attenzione nell'ottica della successivo screening - lecito - del profilo) di tutti gli eventuali trattamenti che precedono, rendendo loro una informativa chiara, trasparente e di dettaglio prima dell'avvio della procedura selettiva medesima.

Inoltre, i dati raccolti e trattati durante la fase pre-assuntiva vanno cancellati non appena diviene chiaro che non si stipulerà alcun contratto con gli individui che hanno partecipato alle procedure selettive. Tale ultima previsione appare comunque contrastare con possibili interessi sia dell'azienda che ricerca personale che degli stessi candidati: si pensi a profili professionali e *curricula vitae* che - non selezionati alla conclusione della procedura selettiva - potrebbero essere di interesse dell'azienda nel futuro, aprendosi particolari posizioni lavorative. Dunque il mantenimento nei database aziendali dei *curricula vitae* di candidati non prescelti - in luogo della immediata cancellazione - dovrebbe basarsi su chiare informazioni in tal senso (d'altra parte il nuovo articolo 13 RGPD prevede tra gli elementi obbligatori da fornire all'interessato anche l'informazione sui termini di conservazione e di cancellazione ultima dei dati) e semmai sulla specifica autorizzazione alla ulteriore conservazione dei dati da parte dei candidati.

§ 3.2. Segue - Scenario n. 2: il trattamento dei dati personali derivante delle attività di screening del lavoratore nel corso o a seguito della cessazione del rapporto lavorativo ("in-employment screening").

Gli stessi *social media* sono poi presi in considerazione dal Parere anche come ambiti di *screening* che il datore di lavoro può effettuare sugli stessi lavoratori in forza alla sua azienda, tenuto anche conto dello sviluppo e della grande disponibilità di tecnologie e *tool* di analisi che consentono un'analisi permanente dei lavoratori mediante la raccolta di informazioni relative ai loro amici, relazioni, opinioni, credo, abitudini nella vita familiare, relazionale e privata, ponendosi anche la questione di possibili trattamenti di dati di particolare natura e sensibili.

Dal punto di vista delle regole operative, il Parere:

1. vieta in linea generale lo screening dei social media dei lavoratori durante la vigenza del rapporto di lavoro;
2. vieta altresì ai datori di lavoro di richiedere ad un lavoratore o a un candidato di avere accesso ad informazioni che egli condivide con altri attraverso i *social networks*;
3. vieta ai datori di lavoro di imporre ai lavoratori l'utilizzo di un profilo *social media* personale ma aperto dal datore di lavoro: anche nel caso di ruoli specifici (es: portavoce di un'organizzazione) il datore di lavoro dovrebbe rendere sempre disponibile (e di ciò il contratto dovrebbe menzionare una specifica disciplina) l'opzione tra utilizzo di un profilo non-pubblico e non-lavorativo al posto di un profilo lavorativo ufficiale.

Come caso di possibile *screening* successivo alla cessazione del rapporto di lavoro il Parere indica il seguente esempio. Un datore di lavoro monitora il profilo LinkedIn di un ex lavoratore per verificare – durante il periodo di vigenza dell'accordo di non-concorrenza – il rispetto delle relative clausole *non-compete*. Tale trattamento sarà basato sul legittimo interesse del datore di lavoro nella misura in cui il datore di lavoro può provare che tale *screening* è necessario per perseguire il suo legittimo interesse al rispetto degli accordi, che non vi sono modalità alternative e meno invasive e che l'ex lavoratore è stato a monte informato adeguatamente su tali possibili trattamenti (quindi nella originaria informativa al lavoratore ci si dovrà porre il problema di fornire *ex ante* informazioni su trattamenti anche successivi alla cessazione del rapporto, come ad esempio – tra le finalità perseguite – anche quella specifica della eventuale e regolare valutazione delle sue comunicazioni pubbliche dopo la cessazione del rapporto di lavoro).

§ 3.3. Segue - Scenario n. 3: il trattamento dei dati personali del lavoratore nel contesto delle attività di controllo e monitoraggio attuate dal datore di lavoro circa l'utilizzo di risorse e strumenti ICT sul luogo di lavoro.

Tradizionalmente questo è l'ambito che fin dalla Opinion del 2001 e dal Documento di Lavoro del 2002 i Garanti europei hanno ritenuto più delicato ed esposto ai rischi di violazione dei diritti dei lavoratori. Rispetto alla conclusioni di quei documenti, nel Parere del 2017 sono messi in luce gli sviluppi tecnologici relativi a *tool* e mezzi di monitoraggio e controllo a distanza che in questo contesto possono rappresentare nuovi rischi di aggressione alla privacy dei lavoratori, quali ad esempio:

1. i sistemi DLP (*Data Loss Prevention*), che monitorano le comunicazioni in uscita con lo scopo di verificare potenziali *data breaches*;
2. *Next-Generation Firewalls* (NGFWs) e sistemi *Unified Threat Management* (UTM) che possono fornire una varietà di tecnologie di monitoraggio, inclusi intercettazioni, filtraggio di siti web, filtraggio di contenuti, reporting su applicativi in uso, informazioni sull'identità dell'utente, DLP;
3. misure e applicativi di sicurezza che coinvolgono le operazioni di *logging* alla rete aziendale da parte del lavoratore;
4. tecnologie di tipo *eDiscovery*, che si riferiscono a qualsiasi processo in cui dati elettronici sono ricercati su reti e sistemi allo scopo di costituire mezzi di prova ufficiali;
5. sistemi di *tracking* dell'uso di applicazioni, applicativi e device attraverso l'operatività di software nascosti, sia su desktop che in *cloud*;
6. l'uso sui luoghi di lavoro di applicativi *office* forniti come *cloud service* che in teoria consentono un approfondito reporting sul logging e sulle attività dei lavoratori;
7. controllo e monitoraggio di device personali (PC, smartphone, tablet) che i lavoratori forniscono per lo svolgimento delle loro prestazioni lavorative in osservanza di specifiche *policies* di uso di tipo *Bring-Your-Own_Devices* (BYOD), così come tecnologie di tipo *Mobile Device Management* (MDM) che consentono la distruzione di applicazioni, dati e configurazioni e *patches* aziendali sui device personali (accedendo al device);
8. utilizzo di dispositivi indossabili (es: per scopi di salute o sicurezza sui luoghi di lavoro);
9. utilizzo di soluzioni di monitoraggio e controllo "*all-in-one*" ("*security packages*") inclusivi di tutte le funzioni sopra elencate.

Proprio nella prospettiva dei sopra citati sviluppi tecnologici relativi a *tool* e mezzi di monitoraggio e controllo a distanza dei lavoratori, i Garanti UE illustrano esempi pratici di impiego nelle realtà aziendali di strumenti IT che comportano o possono indirettamente comportare un trattamento dei dati personali dei lavoratori come effetto (o finalità diretta) del monitoraggio.

Nel primo esempio, un datore di lavoro intende lanciare sulla propria rete aziendale un'applicazione di *TLS inspection* per decrittare flussi di comunicazione di dati criptati onde verificare la presenza di eventuali anomalie o minacce. L'uso di comunicazioni criptate è sempre più diffuso per proteggere le comunicazioni e i dati contro illecite intercettazioni: il protocollo TLS (*Transport Layer Security*) è appunto un protocollo crittografico che previene la manomissione dei dati, la falsificazione e l'intercettazione e permette una comunicazione sicura dalla sorgente al destinatario (*end-to-end*) su reti TCP/IP (come ad esempio Internet) fornendo autenticazione,

integrità dei dati e cifratura. Tuttavia, lo svantaggio delle tecnologie di crittazione è che rende impossibile monitorare dati in entrata e in uscita. Le tecnologie di *TLS inspection* decrittano i flussi, analizzano il contenuto per scopi di sicurezza e re-crittano i flussi dopo l'analisi.

Nell'esempio illustrato dai Garanti UE, l'uso di tale tecnologia rende il datore di lavoro in grado altresì di registrare ed analizzare interamente l'attività *on line* di un lavoratore all'interno della rete aziendale. Il datore di lavoro – al contrario – potrebbe richiamarsi al proprio legittimo interesse alla protezione della rete e delle informazioni relative a clienti e lavoratori ivi registrate avverso accessi abusivi o diffusione non autorizzata di informazioni. Tuttavia, la possibilità che l'impiego di tecnologie di *TLS inspection* determini un controllo di ogni attività svolta dai lavoratori sulla rete aziendale od *on line* è considerato un trattamento non proporzionato. Dunque i Garanti UE suggeriscono come effettuare operativamente – in casi del genere - un corretto bilanciamento tra legittimo interesse datoriale ei diritti dei lavoratori:

1. il datore di lavoro dovrebbe primariamente ricercare strumenti, applicazioni o tecnologie meno invasive che gli consentano il perseguimento del suo legittimo interesse senza sacrificare sproporzionalmente i diritti dei lavoratori;
2. nella misura in cui l'ispezione *TLS* sia considerata come strettamente necessaria, la relativa tecnologia dovrebbe essere configurata in modo tale da impedire la registrazione permanente e integrale dell'attività svolta dai lavoratori sulla rete aziendale od *on line*; nel caso sia bloccato traffico in entrata o in uscita, il lavoratore dovrebbe essere reindirizzato ad una pagina intranet aziendale interna per supporto;
3. ove una generale e integrale registrazione delle attività svolta dai lavoratori sulla rete aziendale od *on line* non possa essere esclusa in quanto strettamente necessaria, allora la tecnologia/tool dovrebbe essere configurata in modo tale da non consentire la conservazione di *log* a meno che l'applicativo non segnali che ciò sia necessario in caso di incidente, procedendo comunque a minimizzare le informazioni raccolte.

I Garanti UE suggeriscono inoltre di adottare in ogni caso una *policy interna* (che dovrebbe essere soggetta a revisione per lo meno annuale) che spieghi e informi i lavoratori circa le modalità operative della tecnologia di *TLS inspection* impiegata.

In sostanza (e anche in ciò risiede la utilità pratica del Parere), i Garanti UE indicano in concreto come dovrebbe essere svolta in casi del genere una valutazione di impatto preventiva (DPIA) in merito alla introduzione di nuove tecnologie in grado di comportare quell'“*elevato rischio*” per i diritti e le libertà dei lavoratori menzionato dall'articolo 35 (“*Valutazione d'impatto sulla protezione dei dati*”) del RGPD. Il Parere, cioè, individua nelle valutazioni preliminari sulla proporzionalità delle misure/tecnologie da introdurre per il monitoraggio basato sul legittimo interesse, sulle misure per ridurre o mitigare l'impatto sui trattamenti dei dati dei lavoratori un tipico caso di DPIA. L'esito della DPIA potrebbe essere appunto incluso e documentato in una specifica *policy* interna, integrativa di altre *privacy policies* (le “politiche del trattamento” ai sensi

dell'art. 24, comma 2 RGPD) che illustri modalità, finalità e controlli di reti e sistemi aziendali. La partecipazione, ove presenti, di rappresentanze sindacali aziendali nel corso di tutto il processo è raccomandata dai Garanti UE.

Nel secondo esempio un datore di lavoro impiega un sistema di *Data Loss Prevention* (DLP) per monitorare i messaggi *email* in uscita onde verificare in automatico se vi sia trasmissione non autorizzata di dati proprietari nelle email (es: la lista dei clienti), indipendentemente dal fatto che tale trasmissione email all'esterno sia intenzionale o meno da parte del lavoratore mittente. Il legittimo interesse è quello datoriale alla *detection* di eventuali *data breaches*.

Tuttavia il sistema può anche evidenziare "falsi positivi", evidenziando come *data breach* email legittime inviate dai lavoratori o accedendo ad email che contengono dati personali privati del lavoratore mittente.

Come bilanciamento tra il legittimo interesse datoriale e i diritti dei lavoratori, un sistema di DLP dovrebbe:

1. essere reso quanto più trasparente possibile ai lavoratori quanto all'utilizzo delle regole che il *tool* segue per caratterizzare una email come potenziale *data breach*;
2. nel caso in cui il sistema riconosca una email in uscita come possibile *data breach*, inviare un messaggio di avviso/allarme che informi il mittente - prima che la email sia inviata - dandogli la possibilità di cancellare la trasmissione.

Non solo dunque, i Garanti UE richiamano l'attenzione dei datori di lavoro a svolgere le obbligatorie valutazioni preventive circa la proporzionalità dei trattamenti previsti, conducendo le dovute valutazioni di impatto e il conseguente *assessment* richiesto dal RGPD, ma altresì essi indicano come momento altrettanto fondamentale quello della redazione di informative ai lavoratori che - lungi dall'essere format burocratici e inutili (oltre che non conformi) - devono essere improntate alla massima trasparenza e personalizzazione, indicando con linguaggio chiaro tutti i possibili dettagli che i lavoratori hanno il diritto di conoscere in merito al trattamento dei loro dati personali.

§ 3.4. *Segue - Scenario n. 4: trattamento dei dati personali del lavoratore nel contesto delle attività di controllo e monitoraggio attuate dal datore di lavoro circa l'utilizzo di risorse e strumenti ICT al di fuori della sede lavorativa e dell'orario di lavoro.*

L'utilizzo di tecnologie e mezzi al di fuori della sede lavorativa è diventato negli anni fenomeno abbastanza diffuso, tra *smart working* (per cui da poco è entrata in vigore in Italia la specifica legge 22 Maggio 2017, n. 81 sul c.d. lavoro agile), *homeworking* o *remote working*, unitamente alla *policies* adottate da alcune aziende di tipo *Bring Your Own Device* (BYOD). La rischiosità è insita nell'aspetto che in tali casi il datore di lavoro può estensivamente accedere – attraverso i sistemi di monitoraggio esistenti sul luogo di lavoro – alla sfera privata e domestica dei lavoratori che utilizzano i propri dispositivi in modalità BYOD.

Con riferimento al possibile monitoraggio attuato dal datore di lavoro su sistemi e strumenti di lavoro conferiti al lavoratore che scelga di rendere la propria prestazione lavorativa in modalità *homeworking* o *remote working*, i Garanti UE indicano quanto segue. L'opzione di lavoro da remoto o da casa si sostanzia nella possibilità di impiegare mezzi per consentire al lavoratore l'accesso all'infrastruttura del datore di lavoro, come se si lavorasse in sede. Proprio per la mancanza di misure di sicurezza tecniche appropriate per gestire – da remoto – il rischio di accessi non autorizzati o di perdita di informazioni (che più probabilmente si possono verificare in un ambiente – come quello domestico o esterno – meno protetto della sede fisica di lavoro), i datori di lavoro potrebbero essere portati a ritenere che sia possibile richiamare come base giuridica di legittimo interesse l'installazione di pacchetti software (*on premise* o in *cloud*) con capacità di registrare la digitazione dei tasti o i movimenti del mouse o di catturare *screenshot* dello schermo di dispositivi (randomicamente o a intervalli predefiniti), registrare l'accesso ad applicazioni ed applicativi (e registrare il tempo di utilizzo), abilitare *webcam* dei dispositivi a distanza e catturare video o immagini dell'attività lavorativa da remoto. Al contrario (ed abbastanza ovviamente per un paese come l'Italia che dal 1970 vieta il controllo indiscriminato e continuo) tutto ciò è ritenuto dai Garanti UE vietato in quanto sproporzionato: nessun legittimo interesse può essere richiamato dai datori di lavoro per l'impiego di tali sistemi.

Diversa, e ben più aperta, è la posizione dei Garanti UE circa il controllo di dispositivi personali dei lavoratori che nell'ambito di politiche di tipo BYOD accettino il cosiddetto "uso promiscuo" dei propri dispositivi personali (smartphone, tablet, PC, etc), che diventano così parzialmente anche "strumenti per rendere la prestazione lavorativa". I rischi privacy in materia sono comunemente associati alle tecnologie di monitoraggio (come la raccolta di identificativi quali il *MAC address* del dispositivo) che il datore di lavoro può giustificare nell'ambito della operatività (sul dispositivo personale del lavoratore) di scansioni di sicurezza. Molte tecnologie consentono potenzialmente di accedere anche a sezioni e dati del dispositivo tipicamente "private", come il *folder* delle foto e video, che sono tipicamente sezioni che non possono essere oggetto di accesso da parte delle tecnologie di monitoraggio impiegate dal datore di lavoro.

Inoltre, per i Garanti UE la registrazione di dati di ubicazione e di traffico sul dispositivo personale del lavoratore è vietata se include dati privati, ma può essere basata sul legittimo interesse se il monitoraggio a monte è impostato sulla netta e chiara distinzione tra parti/sezioni lavorative e parti/sezioni private del dispositivo personale del lavoratore.

Dunque ancora una volta saranno le valutazioni d'impatto preventivo e il conseguente *assessment* del datore di lavoro a tracciare la linea di demarcazione tra trattamenti di monitoraggio proporzionati, leciti e basati sul legittimo interesse e controlli vietati dei lavoratori.

Con riferimento al monitoraggio nell'ambito di politiche di *Mobile Device Management* (MDM), tali *policies aziendali* consentono ai datori di lavoro di localizzare i dispositivi (anche personali dei lavoratori) da remoto, di attivare particolari configurazioni e/o applicazioni, di cancellare dati *on demand*, di tracciare in tempo reale il dispositivo anche se non è segnalato come rubato. Un datore di lavoro può impiegare tali funzionalità in proprio o anche avvalendosi di terze parti.

Per i Garanti UE, una appropriata valutazione di impatto preventivo deve essere sempre attuata in tali casi, sia in caso di impiego di una nuova tecnologia, sia in caso di tecnologia che è nuova per quel datore di lavoro/titolare del trattamento in particolare.

Se l'esito della DPIA è che la tecnologia MDM è necessaria in determinate circostanze, allora va implementato lo specifico *assessment* per garantire che i relativi trattamenti dei dati siano conformi ai principi di proporzionalità e sussidiarietà. Ad esempio, le funzionalità di localizzazione a distanza e di *tracking*, anche ove ammesse per scopi specifici e funzionalità predeterminate, vanno comunque mitigate: ad esempio i sistemi di *tracking* vanno impostati (anche in aderenza al principio della *privacy by design* come previsto dal RGPD) in modo tale che registrino i dati di localizzazione senza visualizzarli al datore di lavoro. La visualizzazione potrebbe essere consentita *ex post*, ad esempio nei soli casi in cui il dispositivo sia perso o rubato.

Infine, i lavoratori i cui dispositivi sono registrati nei servizi MDM devono ricevere una completa e trasparente informativa su tutte le funzionalità tecniche di tali tecnologie: dal *tracking*, alla localizzazione, alle altre funzionalità, inclusi i casi in cui si attivano e le conseguenze che possono avere tali rilevazioni sui lavoratori.

In materia di dispositivi indossabili e di correlati trattamenti di dati dei lavoratori il Parere pone una sorta di divieto assoluto: dal momento che tali dispositivi indossabili spesso registrano dati relativi alla salute, nessun presupposto (quale il consenso o il legittimo interesse) potrebbe validamente applicarsi quale base giuridica del trattamento. Ciò neanche applicando le tecniche di anonimizzazione più sofisticate o adottando servizi di terzi che raccolgano in modalità aggregata e complessiva i dati da tutti i dispositivi indossabili in uso. In realtà tale posizione dei Garanti UE appare eccessivamente rigida: si pensi al caso dei cosiddetti "lavoratori isolati" e dei dispositivi cc.dd. "uomo a terra" per la tutela e salvaguardia di tutti quei lavoratori che si trovano

a lavorare da soli. Tra l'altro, la posizione espressa dai Garanti UE appare mal conciliarsi – per quanto riguarda l'Italia – con gli obblighi in materia di sicurezza del lavoratore isolato espressamente previsti da disposizioni normative che prescrivono che in linea generale i lavoratori, se impossibilitati a chiedere aiuto in caso di pericolo, non possono operare da soli in luoghi isolati e pertanto è sempre indispensabile la presenza di un collega vicino, oppure essi devono essere dotati di un dispositivo uomo a terra che possa allertare i soccorsi in caso di necessità.

§ 3.5. Segue - Scenario n. 5: trattamento dei dati personali del lavoratore nel contesto delle attività di verifica delle presenze e dell'orario lavorativo.

Il caso affrontato dal Parere riguarda i sistemi che consentono ai datori di lavoro di controllare chi può entrare nei luoghi di lavoro e/o in certe aree delicate, monitorando e tracciando sia tali accessi che il tempo di permanenza nelle aree. I Garanti UE prendono in particolare in esame il caso specifico di sistemi di controllo degli accessi e della presenza dei lavoratori basati su trattamenti di immagini video incrociate con dati biometrici, che si sono ampiamente diffusi negli anni. Mentre tali sistemi possono costituire una importante componente nei sistemi di *audit* del datore di lavoro, al tempo stesso pongono il rischio di un livello invasivo di conoscenza e controllo delle attività del lavoratore mentre si trova nel luogo di lavoro.

L'esempio è quello tipico del controllo accessi ad una sala *server* (con sistemi di ripresa video di lavoratori che accedono ai locali mediante dispositivi di lettura di impronte digitali) in cui vi è *storage* di dati aziendali delicati. Il controllo degli accessi – in caso di *data breach* – consente al datore di lavoro di ricostruire tutti gli accessi e gli orari dei lavoratori autorizzati. Questa ipotesi è considerata dai Garanti UE come uno dei casi in cui il legittimo interesse datoriale prevale sui diritti privacy dei lavoratori, a patto che ai lavoratori sia data informativa chiara e dettagliata circa tali possibili trattamenti e investigazioni successive e a patto che il continuo monitoraggio e tracciatura degli accessi non si risolva nel controllo dell'attività lavorativa, ai fini di valutazioni di altro tipo del lavoratore.

L'esempio e le indicazioni operative fornite per tale specifico caso sono di grande importanza pratica: in sostanza, in tutti questi e simili casi i Garanti UE forniscono nel Parere una sorta di generale valutazione di impatto preventiva già svolta a monte, concludendo con la prevalenza dell'interesse legittimo del datore di lavoro sui diritti dei lavoratori.

§ 3.6. Segue - Scenario n. 6: trattamento dei dati personali del lavoratore nel contesto della operatività di sistemi di videosorveglianza nei luoghi di lavoro.

Le criticità privacy dei sistemi di videosorveglianza sono le medesime già da anni affrontate e disciplinate da vari provvedimenti dei Garanti europei, non solo in relazione al contesto lavorativo (per l'Italia, il riferimento è al Provvedimento generale sulla videosorveglianza del 2010).

Il Parere si occupa in realtà delle più recenti (ed invasive) tecnologie, come ad esempio quelle in grado di accedere da remoto e di raccogliere dati e immagini (anche in alta definizione) attraverso le singole fotocamere dei dispositivi, associando poi i dati raccolti a software di *video analytics*. Mediante tali software, ad esempio, un datore di lavoro può analizzare espressioni facciali del lavoratore e verificarne la devianza rispetto a *patterns* predefiniti. Similari trattamenti sono ovviamente vietati in quanto sproporzionati. Inoltre tali trattamenti implicano la profilazione automatica del lavoratore (ed eventuali decisioni basate su trattamenti automatizzati). I datori di lavoro dovrebbero astenersi dall'impiego di simili tecnologie, a meno di casi eccezionali che comunque non possono essere invocati come generale base per un legittimo uso di tali tecnologie.

Inoltre, va ricordato che ai sensi dell'art. 9 GDPR è vietato trattare dati personali biometrici intesi a identificare in modo univoco una persona fisica, a meno che il trattamento non sia necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato.

§ 3.7. Segue - Scenario n. 7: trattamento dei dati personali del lavoratore raccolti nel contesto di utilizzo di veicoli geolocalizzabili assegnati a dipendenti.

Particolarmente utili e interessanti sono le indicazioni operative e di liceità che i Garanti UE forniscono circa i trattamenti di geolocalizzazione mediante uso di tecnologie su veicoli aziendali. La geolocalizzazione è resa possibile da normali antifurti satellitari fino a sistemi GPS ed *event data recorder* dotati di tecnologie che non solo geolocalizzano permanentemente il veicolo, ma registrano altrettanto permanentemente abitudini di guida e persino status psico-fisico del guidatore.

L'impiego di tali sistemi di *tracking* può essere un obbligo legale-assicurativo del datore di lavoro (es: per l'Italia nel settore dell'autotrasporto o in caso di veicoli in leasing) per

dimostrare la conformità a vincoli di legge, anche in materia di sicurezza dei lavoratori/guidatori. Il datore di lavoro può anche avere un legittimo interesse alla localizzazione dei veicoli – proprio patrimonio aziendale – in ogni dato momento.

Tuttavia, il Parere evidenzia come anche in presenza di tali presupposti di legittimità, il datore di lavoro deve prima valutare la necessità e proporzionalità di tali tecnologie/trattamenti e soprattutto se i sistemi che intende implementare sui veicoli aziendale rispondono ai principi di proporzionalità e liceità.

Nel caso sia consentito un utilizzo privato del veicolo aziendale, la conformità con il principio di proporzionalità è attestata dalla presenza nel veicolo di un sistema di *opt-out* attivabile dal guidatore per disattivare temporaneamente il sistema di geolocalizzazione (es: se sta andando a fare una visita medica).

La localizzazione del veicolo aziendale utilizzato dal lavoratore al di fuori dell'orario di lavoro rispetta il principio di proporzionalità (e il legittimo interesse del datore di lavoro, ad esempio per prevenire il furto del veicolo utilizzato al di fuori dell'orario di lavoro) se la localizzazione si attiva in caso il veicolo lasci una zona predeterminata (una regione o il paese).

Il Parere ricorda anche importanti principi in materia di geolocalizzazione già stabiliti in passato da provvedimenti dei Garanti UE. Ad esempio, il principio contenuto nel Parere 13/2011 sui servizi di geolocalizzazione su *mobile smart devices*, in base al quale *“i sistemi di geolocalizzazione di veicoli sono pensati per la tracciatura della ubicazione dei veicoli in quanto tali, e il datore di lavoro non dovrebbe guardare ad essi come strumenti di tracciatura del lavoratore e del suo comportamento, come ad esempio per mandare alerts in tempo reale in relazione al superamento di limiti di velocità da parte del guidatore”*.

Oppure come nel caso del Parere 5/2005 sull'utilizzo di dati di ubicazione per la fornitura di servizi a valore aggiunto, nel quale i Garanti UE specificano che *“il trattamento di dati relativi alla ubicazione può essere giustificato laddove sia parte di un sistema di monitoraggio di un sistema di trasporto di persone e merci in zone pericolose o laddove comunque emergano oggettive esigenze di sicurezza in relazione al lavoratore o ai beni o al medesimo veicolo sotto la sua responsabilità. Non esistono tali oggettive necessità quando il lavoratore è libero di organizzare il viaggio o la finalità del datore di lavoro sia solo quella di monitorare il veicolo e il guidatore”*.

Nel caso di sistemi avanzati di *event data recorder* il Parere richiama con forza la valutazione preventiva del rispetto del principio di proporzionalità. Ad esempio, sarebbe del tutto vietato installare nei veicoli sistemi di registrazione audio-video che conservino le immagini in caso di incidente.

§ 3.8. Segue - Scenario n. 8: trattamento dei dati personali del lavoratore nel contesto delle attività di comunicazione dei dati dei lavoratori a terze parti.

Negli anni è diventato sempre più frequente per le aziende trasmettere i dati dei propri lavoratori ai clienti, ad esempio per garantire la fornitura di un servizio affidabile. La valutazione dell'eventuale legittimo interesse quale base legittima per la comunicazione a terzi dei dati dei lavoratori va però sempre condotta con estrema cautela. Il Parere fornisce l'esempio di un'azienda che invia una email ad un cliente che deve ricevere una spedizione, contenente il *link* ai dati anagrafici ed alla foto del passaporto del lavoratore incaricato della spedizione e della consegna, in modo che il destinatario possa fare il confronto e controllare che il soggetto sia proprio la persona indicata dall'azienda. Questo è un caso di comunicazione a terzi sproporzionata e non basata sul legittimo interesse, poiché non è necessario il trattamento di dati anagrafici e foto del lavoratore per conseguire la finalità della affidabilità del servizio di consegna.

§ 3.9. Segue - Scenario n. 9: trattamento dei dati personali nel contesto delle attività di trasferimento internazionale di informazioni riferite ai lavoratori.

I Garanti UE ricordano come sempre più spesso i datori di lavoro utilizzino applicazioni e servizi *cloud-based* specificatamente progettati per la gestione dei dati HR. Così come è frequente l'impiego di applicativi *office* utilizzati *on line* che registrano dati dei lavoratori che li utilizzano. Tali servizi, applicazioni e tecnologie possono spesso comportare un trasferimento internazionale extra UE dei dati dei lavoratori (stante il funzionamento dei servizi *cloud* e la frequente localizzazione dei relativi server di fornitori e sub-fornitori dei servizi *cloud* al di fuori della Unione Europea). Ciò implica la necessità di valutare attentamente gli aspetti tecnici dei relativi contratti che il datore di lavoro stipula con i fornitori di servizi *cloud*, non solo nella prospettiva delle adeguate misure tecniche di protezione, ma anche nella prospettiva degli obblighi, delle condizioni, dei requisiti di liceità e dei divieti che il RGPD pone in materia di trasferimento dei dati al di fuori della UE. Come è noto, gli articoli 44-50 del RGPD dettano

specifiche condizioni per il trasferimento dei dati extra UE: in tale ambito, i Garanti specificano nel Parere alcuni suggerimenti:

1. anche laddove la normativa prevede delle deroghe che consentono il trasferimento (ad esempio l'art. 49 RGPD prevede ipotesi di trasferimento comunque consentito in base a diversi presupposti - come ad esempio il consenso dell'interessato - se non è possibile basarlo su decisioni di adeguatezza, *data transfer agreement*, norme vincolanti d'impresa, ect), sarebbe sempre preferibile fondare il trasferimento sugli istituti di adeguata protezione previsti (dunque *data transfer agreement*, norme vincolanti d'impresa, codici di condotta, certificazioni, etc) piuttosto che sulle deroghe;
2. nel caso il datore di lavoro si richiami ad una delle deroghe previste, e cioè il consenso dell'interessato, egli dovrà dimostrare che il consenso prestato dal lavoratore è "*specifico, liberamente espresso e non ambiguo*" (si ricordi però che nello stesso Parere i Garanti UE evidenziano che il consenso del lavoratore, stante la natura del lavoratore quale "soggetto debole", quasi mai è realmente libero e dunque validamente prestato);
3. il datore di lavoro deve assicurare che i dati condivisi al di fuori della UE e gli accessi susseguenti da parte di altre aziende del medesimo gruppo societario siano limitati allo stretto necessario e per finalità a monte specificate e definite nella informativa ai lavoratori.