LCA

•ALERT•

10 FEBBRAIO 2023

Decreto Trasparenza e protezione dei dati personali

L'Autorità Garante per la protezione dei dati personali (il "Garante") ha fornito al Ministero del Lavoro e all'Ispettorato Nazionale del Lavoro alcune indicazioni preliminari in merito ai profili relativi alla protezione dei dati personali emersi a seguito dell'introduzione del D. Lgs. 27 giugno 202, n. 104 (c.d. "Decreto Trasparenza").[1]

Quest'ultimo ha introdotto una serie di obblighi per i datori di lavoro che utilizzino sistemi decisionali o di monitoraggio automatizzati per ricavare informazioni ai fini:

- .dell'assunzione o del conferimento di un incarico lavorativo;
- della gestione o cessazione del rapporto di lavoro;
- dell'assegnazione di mansioni e, in generale, della valutazione sulle prestazioni eseguite e sull'adempimento delle obbligazioni contrattuali.

I casi in cui possono trovare applicazione gli obblighi previsti dal Decreto Trasparenza possono ricomprendere diversi strumenti e tecnologie, quali:

- software per il riconoscimento emotivo;
- strumenti di data analytics o machine learning, rete neurali, deep-learning; nonché
- sistemi per il riconoscimento facciale, sistemi di rating e ranking (come, ad esempio, meccanismi di Key Performance Indicator) che, specie se impiegati nel contesto lavorativo, determinano un elevato livello di rischio per i diritti e le libertà degli interessati.

Il Garante ha precisato che l'adozione di tali sistemi nel contesto lavorativo (anche in fase preassuntiva) deve sempre essere oggetto di una preliminare verifica, da parte del datore di lavoro, delle condizioni di liceità stabilite dalla disciplina in materia di controlli a distanza, della valutazione dei rischi per verificarne l'impatto sui diritti e sulle libertà degli interessati nonché della proporzionalità del trattamento e del rispetto dei principi generali di cui all'art. 5 del GDPR.

In particolare, nel caso in cui i datori di lavoro eseguano trattamenti che ricadano nel perimetro applicativo della normativa esaminata, dovranno osservare i seguenti obblighi:

1. Predisporre o integrare un'informativa ai sensi degli artt. 13 e 14 GDPR
   Ciascun datore è tenuto a fornire ai lavoratori le informazioni relative agli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi decisionali o di monitoraggio automatizzati, con particolare riguardo:
   a. al funzionamento dei sistemi utilizzati;
   b. ai parametri principali utilizzati per programmare o addestrare i sistemi decisionali o di monitoraggio automatizzati, inclusi i meccanismi di valutazione delle prestazioni;
   c. alle misure di controllo adottate per le decisioni automatizzate, gli eventuali processi di correzione e il responsabile del sistema di gestione della qualità;
   d. al livello di accuratezza, robustezza e cybersicurezza dei sistemi e le metriche utilizzate per misurare tali parametri, nonché gli impatti potenzialmente discriminatori delle metriche stesse.

[1] A questo link è pubblicato l'Alert con gli approfondimenti sul Decreto Trasparenza a cura del Team Labour.

Le disposizioni del Decreto Trasparenza si applicano a **tutti i rapporti di lavoro**, anche a quelli **instaurati anteriormente alla data del 1° agosto 2022** (per cui è previsto che i dipendenti possano ottenere i predetti elementi informativi a seguito di specifica richiesta scritta rivolta al datore di lavoro che dovrà dare riscontro entro 60 giorni).
Con riferimento, invece, ai **rapporti di lavoro instaurati successivamente a tale data** gli obblighi informativi aggiuntivi devono essere adempiuti **prima dell'inizio dell'attività lavorativa.**
Per tali ragioni, le specifiche informazioni sui sistemi decisionali o di monitoraggio automatizzati possono (e il Garante ha espressamente raccomandato che ciò avvenga) essere fornite **congiuntamente,** e quindi all'interno **dello stesso testo dell'informativa privacy rivolta ai dipendenti** ai sensi degli artt. 13 e 14 del GDPR.

2. **Effettuare una valutazione d'impatto sulla protezione dei dati (DPIA)**
   La predisposizione di una valutazione d'impatto è **sempre obbligatoria** – ricorda il Garante – ove si faccia ricorso ad una **valutazione sistematica e globale** di aspetti personali relativi a persone fisiche, basata su un **trattamento automatizzato**, compresa la profilazione, e sulla quale si fondano decisioni che hanno **effetti giuridici** o **incidono in modo analogo** significativamente su dette persone fisiche.

Ciascun datore è, pertanto, **tenuto a valutare** se i trattamenti che intende effettuare possano presentare un **rischio elevato per i diritti e le libertà delle persone fisiche** – alla luce delle tecnologie impiegate e considerati la natura, l'oggetto, il contesto e le finalità perseguite - che renda necessaria una preventiva **valutazione di impatto** sulla **protezione dei dati personali**.

Deve inoltre tenere conto della "vulnerabilità" degli interessati nel contesto lavorativo, nonché del fatto che l'impiego nell'ambito lavorativo di tali sistemi potrebbe sfociare in un monitoraggio sistematico dell'attività dei dipendenti.

In aggiunta, dovranno essere presi in considerazione i **criteri individuati dal Comitato europeo per la protezione dei dati (EDPB)**: valutazione o assegnazione di un punteggio; processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente; trattamento di dati su larga scala; creazione di corrispondenze o combinazione di insiemi di dati; uso innovativo o applicazione di nuove soluzioni tecnologiche o organizzative; trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.
Nella maggior parte dei casi, deve considerarsi che un **trattamento che soddisfi almeno due criteri** debba formare **oggetto di un DPIA** e che maggiore è il numero di criteri soddisfatti dal trattamento, maggiore è la probabilità che questo configuri un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati.

3. **Eseguire un'analisi dei rischi in attuazione dei principi di privacy by default e privacy by design**
   Tale analisi deve essere svolta anche laddove si utilizzino sistemi tecnologici di terzi, avvalendosi del supporto del responsabile del trattamento. L'analisi deve essere diretta, fra l'altro, a verificare caso per caso che i trattamenti condotti per mezzo di tali sistemi:
   a. siano fondati su una corretta base di liceità;
   b. siano compatibili con le finalità perseguite;
   c. rispondano ai principi applicabili alla normativa in materia di protezione dei dati personali.

4. Aggiornare il registro dei trattamenti
Il registro dei trattamenti deve essere aggiornato con tutte le informazioni relative ai trattamenti svolti – anche con riferimento ai sistemi decisionali o di monitoraggio adottati - e documentarne la conformità alla disciplina in materia di protezione dei dati personali.

5. Garantire le tutele previste per i processi decisionali automatizzati
Ciascun datore deve valutare se i sistemi impiegati diano luogo a un **processo decisionale unicamente automatizzato**, compresa la **profilazione**, che produca **effetti giuridici** o che **incida significativamente sull'interessato**; in questi casi trova applicazione l'art. 22 del GDPR, il quale stabilisce le ipotesi in cui il diritto di non essere sottoposto a tali trattamenti può essere derogato a condizione che vengano assicurate alcune garanzie per l'interessato, tra cui, in particolare il **diritto** di:
   a. ottenere l'intervento umano da parte del titolare del trattamento;
   b. esprimere la propria opinione;
   c. contestare la decisione.

6. Garantire l'esercizio dei diritti agli interessati
Fermo restando l'obbligo riguardo ai rapporti di lavoro instaurati anteriormente al 1° agosto 2022 già esaminato, il datore di lavoro dovrà anche assicurare l'esercizio dei diritti per l'interessato di ottenere l'accesso ai propri dati personali, comprese le ulteriori informazioni previste dal Decreto Trasparenza, alle condizioni e nei tempi previsti dall'art. 15 del GDPR.

Il team privacy di LCA è a disposizione per qualsiasi supporto in relazione all'implementazione delle misure previste dal Decreto Trasparenza.

CONTATTI

Giulio Vecchi
giulio.vecchi@lcalex.it
Sergio Amato
sergio.amato@lcalex.it