PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5663 di Martedì 16 luglio 2024

Data protection: un documento di valutazione dei rischi per la privacy?

Un contributo si sofferma sulla data protection e sicurezza sul lavoro e parla della possibilità di un documento di valutazione dei rischi (DVR) anche per la privacy. I rischi connessi alle nuove tecnologie, la valutazione d'impatto e il DVRP.

Urbino, 16 Lug ? Come sottolineato anche nei tanti documenti prodotti per la campagna europea 2023-2025 " Lavoro sano e sicuro nell'era digitale", promossa dall'Agenzia europea per la sicurezza e la salute sul lavoro (EU-OSHA), il sempre più diffuso ricorso, nel mondo del lavoro, a **nuove tecnologie** di **automazione digitalizzata** e/o **robotica**, spesso basate sull' intelligenza artificiale, "indubbiamente arreca enormi vantaggi alla produttività aziendale, in termini sia qualitativi sia quantitativi". Tuttavia, "è un dato oramai acquisito che le nuove tecnologie **impattano sui diritti fondamentali dei lavoratori**, ed è fortemente avvertita l'esigenza di individuare adeguate forme di bilanciamento tra poteri datoriali e diritti dei lavoratori".

A segnalarlo, con particolare riferimento ai problemi connessi alla **privacy**, è un contributo/saggio pubblicato sul numero 1/2024 di "**Diritto della sicurezza sul lavoro**", rivista online dell'Osservatorio Olympus dell' Università degli Studi di Urbino.

Il contributo ? dal titolo "**Data protection e sicurezza sul lavoro: un documento di valutazione dei rischi (DVR) anche per la privacy?**" e a cura di Lucia D'Arcangelo, professore associato di Diritto del lavoro presso il Dipartimento di Giurisprudenza dell'Università di Napoli Federico II ? sottolinea dunque che l'introduzione nell'ambiente di lavoro di nuove tecnologie (automazione digitalizzata, robotica, intelligenza artificiale, ...) pone "l'esigenza di applicare le disposizioni previste dal **Regolamento europeo 2016/679** in materia di tutela dei dati personali".

E in assenza di una "cornice nazionale di riferimento per la protezione e sicurezza dei dati nel rapporto di lavoro", il contributo propone di "adottare la normativa sulla sicurezza del lavoro come modello di riferimento per la **valutazione del rischio privacy**".

Nel presentare il contributo l'articolo si sofferma sui seguenti argomenti:

- Il campo d'indagine e la necessità di tutelare i lavoratori
- Il trattamento dei dati e la redazione del documento di valutazione d'impatto
- La valutazione dei rischi SSL come modello: la prevenzione del rischio privacy

Il campo d'indagine e la necessità di tutelare i lavoratori

Riguardo alla delimitazione del campo d'indagine, il saggio ricorda che sul tema del lavoro automatizzato il quadro regolatorio è caratterizzato da varie fonti normative, ma emerge "il ruolo centrale" del Regolamento sulla protezione dei dati personali (UE) 2016/679 (GDPR).

E con questo lavoro si propone "una riflessione sul problema della sicurezza dell'ambiente di lavoro di una fabbrica intelligente (*smart factory*), dal punto di vista della garanzia dei requisiti minimi di legalità algoritmica, con particolare riguardo alla individuazione di modelli di tutela dei dati personali applicabili al rapporto di lavoro".

In particolare, in questo nuovo ecosistema del lavoro, "emerge la necessità di **tutelare i lavoratori dalla raccolta massiccia e pervasiva di qualsiasi dato che attiene alla loro sfera personale**, sgombrando il campo da tentativi di iper-regolarizzazione legislativa a favore di architetture normative più snelle e, in qualche misura, semplificatorie".

Con questo obiettivo si vuole continuare un percorso, già iniziato in passato, in cui si prospetta "l'accostamento tra la regolamentazione europea sui dati personali e la disciplina in materia di salute e sicurezza nei luoghi di lavoro (d.lgs. n. 81/2008) per quanto attiene al profilo della strumentazione di tutela".

A questo proposito il percorso parte dai profili caratterizzanti l'ambiente di lavoro intelligente, "al fine di metterne in rilievo i vantaggi e soprattutto i potenziali rischi". E successivamente, sempre nel contributo, ci si sofferma "sull'applicabilità nel rapporto di lavoro dei principi posti a garanzia della legalità algoritmica, con l'obiettivo, specifico, di verificare la configurabilità di un modello di data protection del lavoro automatizzato sul paradigma del sistema di sicurezza sul lavoro delineato" nel Decreto legislativo 81/2008.

Il trattamento dei dati e la redazione del documento di valutazione d'impatto

Veniamo subito a quanto indicato dall'autore sugli obblighi connessi alla redazione del **documento di valutazione d'impatto** (**DPIA**) (art. 35, paragrafo 1, Gdpr), che "prevede una valutazione delle conseguenze negative sui diritti e le libertà fondamentali delle persone fisiche interessate da un trattamento di dati derivante dall'uso di nuove tecnologie".

Tale la valutazione d'impatto "si rende obbligatoria per il datore di lavoro, ai sensi dell'art. 35, paragrafo 3, nei seguenti casi:

- se si tratta di un trattamento di dati svolto con modalità automatizzate (lett. a);
- se riguarda categorie particolari di dati (lett. b);
- in presenza di una videosorveglianza svolta in maniera sistematica che comprende spazi accessibili al pubblico (lett. c)".

E se il legislatore UE "non precisa in maniera esplicita se tali condizioni devono ricorrere contestualmente ai fini dell'obbligo del DPIA o se deve ritenersi sufficiente anche una sola di esse", l'autore opta "per questa seconda soluzione in considerazione della incidenza sulle libertà fondamentali e sui diritti dei lavoratori".

Infatti ci possono essere **trattamenti automatizzati** "che danno luogo ad effetti discriminatori, ad esempio, le attività di recruiting del personale attraverso la selezione di curricula o anche la raccolta di dati sanitari relativamente alle visite mediche periodiche svolte dal medico competente in azienda, compresa la conservazione e l'aggiornamento delle relative cartelle sanitarie. O anche, la profilazione dei lavoratori tramite il trattamento di dati attinenti ad aspetti comportamentali come le informazioni sul rendimento professionale rilevabili da modelli di profilazione con sistemi GPS e *wereable device* per agevolare

i lavoratori durante l'esecuzione della prestazione, e ancora, le attività di timbratura degli ingressi e delle uscite dei dipendenti attraverso la sorveglianza di spazi eventualmente esposti al pubblico che determina la raccolta di una mole indiscriminata di informazioni".

Anche l'**Autorità Garante per la privacy**, relativamente alle ipotesi di lavoro automatizzato, ha precisato che "il documento d'impatto è obbligatorio in presenza di «*trattamenti nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti*» (Provvedimento 11 ottobre 2018, n. 467)".

IL **DPIA** deve "indicare anzitutto le tipologie di strumenti utilizzati per la raccolta dei dati dei lavoratori, le relative caratteristiche, nonché le finalità che intende perseguire e la ratio del trattamento ovvero deve specificare qual è l'interesse legittimo del datore di lavoro (nuove assunzioni, tutela del patrimonio aziendale, aumento della produttività, salute e sicurezza dei lavoratori) (art. 35, paragrafo 7, lett. a), Gdpr); deve altresì motivare la necessità del trattamento e la sua proporzionalità rispetto agli scopi da perseguire (lett. b), individuando i rischi possibili di lesione del diritto alla protezione dei dati dei lavoratori (lett. c), e le misure che intende predisporre per evitare o ridurre il rischio d' impatto negativo (lett. d)".

La valutazione dei rischi SSL come modello: la prevenzione del rischio privacy

Si indica poi che sotto il profilo procedurale tale valutazione d'impatto (art. 35, Gdpr) "sembra, in parte, simile alla **valutazione dei rischi** contemplata dal d.lgs. n. 81/2008 (artt. 28 e 29), ma se ne differenzia sul piano dei soggetti che vi partecipano".

Se la valutazione dei rischi (DVR) si basa sul coinvolgimento di vari attori della sicurezza (RSPP, RLS, medico competente, ...) che collaborano alla stesura del relativo documento, la valutazione d'impatto (DPIA) "è svolta invece dal **titolare del trattamento** che «*si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno*» (art. 35, par. 2, Gdpr)".

Tuttavia (paragrafo 9), si legge anche «*Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto*», di tal che si intende che "è mera facoltà del titolare avviare una «*consultazione*» sulle misure da intraprendere, con gli interessati o i loro rappresentanti".

E questa disposizione ? continua l'autore - può essere letta "congiuntamente con l'art. 88 Gdpr, paragrafo 1, quando afferma che gli Stati membri «*possono prevedere, con legge o tramite contratti collettivi disposizioni 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*», se non altro nella prospettiva di ribadire il ruolo di centralità che potrebbe avere il fenomeno sindacale nella *data protection*, sul presupposto che la previsione di un modello di prevenzione del rischio privacy partecipata consentirebbe una condivisione democratica della tutela dei lavoratori sul piano della garanzia di integrità dei propri diritti fondamentali".

Volendo "cedere a qualche ulteriore suggestione interpretativa", si può dunque pensare di considerare come "**modello per la prevenzione partecipata del rischio privacy il sistema della sicurezza e salute dei lavoratori delineato nel d.lgs. n. 81/2008**".

In parole povere al datore di lavoro - in qualità di titolare del trattamento dei dati dei lavoratori ? "spetterebbe il compito di redigere un '**documento di valutazione del rischio privacy** (DVRP)' analogamente a quanto stabilito in materia di sicurezza sul lavoro sulla redazione del documento di valutazione dei rischi (DVR) (art. 28 del d.lgs. n. 81/2008)".

E in esso "andrebbero indicate anzitutto le generali **misure tecniche e organizzative** valutate dal datore di lavoro come «*adeguate*» a «*dimostrare che il trattamento è effettuato conformemente al Regolamento*» (art. 24 Gdpr), nonché le misure volte ad assicurare la protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 Gdpr), che consiste nell'obbligo di indicare le tipologie delle misure da adottare (pseudonomizzazione, minimizzazione dei dati) finalizzate a garantire la concreta attuazione dei principi generali di legittimità del trattamento di cui all'art. 5 Gdpr".

Inoltre in questo documento di valutazione dei rischi andrebbe prevista "l'indicazione del soggetto responsabile della protezione dei dati (DPO) (art. 37 Gdpr), che deve essere individuato 'in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa in materia di protezione dei dati (...)' oltre che della capacità di assolvere i compiti specificati al successivo art. 39 del regolamento".

Quanto poi alla "partecipazione sindacale nel sistema di protezione dei dati", e tenendo presente la figura del/i rappresentante/i per la sicurezza (D.lgs. 81/2008), "si potrebbe immaginare un meccanismo analogo per la **individuazione del/i rappresentante/i dei lavoratori per la privacy** (RLP)".

Con riguardo poi alla valutazione d'impatto di cui all'art. 35 Gdpr, "anch'essa potrebbe confluire nel **documento dei rischi** (**DVRP**) oppure, in considerazione della complessità di tale obbligo che viene imposto essenzialmente nelle ipotesi di trattamenti automatizzati di dati che generano la profilazione dei soggetti interessati, il relativo documento, volendo, potrebbe costituire un addendum della valutazione dei rischi (DVRP)".

Si segnala che un'obiezione che si può sollevare ad un tale modello di valutazione partecipata del rischio privacy "è che, così facendo, si rischia di procedimentalizzare in modo eccessivo l'esercizio del potere datoriale. Tuttavia, si può affermare che il potere del datore di lavoro è già procedimentalizzato nello Statuto dei lavoratori, con particolare riferimento ai controlli a distanza (art. 4) e agli accertamenti sanitari (art. 5), attraverso un gioco di rinvii normativi con il Codice (artt. 113, 114)". E in tale cornice, "la regolamentazione europea sui dati personali interviene, da un lato, con disposizioni procedimentali finalizzate a rendere operativi gli obblighi a carico del titolare del trattamento", e dall'altro lato. come indicato sopra, attribuisce agli Stati membri la "facoltà di prevedere attraverso leggi o contratti collettivi norme più specifiche con riferimento all'ambito dei rapporti di lavoro (art. 88 Gdpr)".

Rimandiamo in conclusione alla lettura integrale del contributo che si sofferma anche sulla veste giuridica che "potrebbe avere un impianto di tutele basato sulla valutazione del rischio privacy", ma si sofferma anche su altri argomenti: i vantaggi e rischi dell'ambiente di lavoro intelligente, la "legalità algoritmica" e i rapporti di lavoro, il principio di accountability, i criteri di trasparenza algoritmica, ...

Tiziano Menduto

Scarica il documento da cui è tratto l'articolo:

Università di Urbino Carlo Bo, Osservatorio Olympus, Diritto della sicurezza sul lavoro, "Data protection e sicurezza sul lavoro: un documento di valutazione dei rischi (DVR) anche per la privacy?", a cura di Lucia D'Arcangelo (professore associato di Diritto del lavoro presso il Dipartimento di Giurisprudenza dell'Università di Napoli Federico II), Diritto della Sicurezza sul Lavoro (DSL) n. 1/2024.

---

www.puntosicuro.it