RISK MANAGEMENT 360

08/04/2021
Sito Web

riskmanagement360.it

Dati biometrici e P.A.: netto stop del Garante

LINK: https://www.riskmanagement360.it/analisti-ed-esperti/dati-biometrici-e-p-a-netto-stop-del-garante/

Alessandro Vasta Partner, Tonucci & Partners Nicola Sandon Associate, Tonucci & Partners Un recente provvedimento del Garante per la Protezione dei Dati Personali mina la liceità del trattamento di dati biometrici nell'ambito del pubblico impiego, a prescindere dalle concrete modalità di trattamento e dalle misure di sicurezza adottate dagli enti pubblici coinvolti. Il motivo è la totale assenza di una valida eccezione al divieto di trattamento di categorie particolari di dati personali ai sensi del Regolamento (UE) 2016/679 Nel 2019 un'azienda sanitaria siciliana, con presidi territoriali in 22 diversi comuni facenti parte della provincia di Enna, decide di dotarsi di un sistema di rilevazione delle presenze dei propri dipendenti che prevede il trattamento di dati biometrici, mediante scansione dell'impronta digitale di questi. La scelta - dettata dall'oggettiva complessità di gestione del personale, spesso operante su più turni all'interno delle 24 ore in presidi ospedalieri e territoriali diversi - viene effettuata anche in considerazione di quanto stabilito dalla neo-approvata l. 56/2019 (la c.d. "Legge concretezza", contenente interventi diretti a contrastare il fenomeno dell'assenteismo nelle p.a.), la quale all'art. 2 impone ad una serie di enti pubblici di introdurre "sistemi di identificazione biometrica e di videosorveglianza" proprio ai fini della "verifica dell'osservanza dell'orario di lavoro". Indice degli argomenti Il provvedimento nei confronti dell'Azienda sanitaria Le contestazioni del Garante Le conseguenze del provvedimento del Garante Il provvedimento nei confronti dell'Azienda sanitaria Forte del presupposto normativo, l'azienda sanitaria sceglie di adottare un sistema in grado di offrire elevate garanzie dal punto di vista della tutela dei dati personali dei lavoratori, prendendo a riferimento, secondo quanto emerge dagli scritti difensivi, le linee guida fornite dall'Autorità con il Provvedimento generale prescrittivo in tema di biometria del 12.11.2014 e un precedente provvedimento autorizzativo[1] emesso dal Garante stesso nei confronti di un'azienda ospedaliera a seguito di verifica preliminare ex art. 17 del D.Lgs. 196/2003. La soluzione prescelta prevede infatti la memorizzazione in forma cifrata del dato biometrico sul badge personale del dipendente, con contestuale cancellazione del dato a livello centralizzato. A quel punto, l'operatore non deve fare altro che apporre il dito su un apposito dispositivo e contestualmente avvicinare il badge al rilevatore delle presenze: il software procede al confronto della stringa cifrata conservata nel badge con l'impronta acquisita localmente e, in caso di riscontro positivo, si limita a memorizzare il numero di matricola del dipendente, l'ora e la data di presenza. WEBINAR Approccio Zero Trust: quanto è importante in un progetto di security? Scoprilo nel live Sicurezza Cybersecurity Leggi l'informativa sulla privacy Email Email aziendale Consente l'invio di comunicazioni promozionali inerenti i prodotti e servizi di soggetti terzi rispetto alle Contitolari che appartengono al ramo manifatturiero, di servizi (in particolare ICT) e di commercio, con modalità di contatto automatizzate e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati.

Il sistema entra ufficialmente in funzione nel novembre del 2019, accolto da vari articoli pubblicati sulla stampa locale e nazionale. Articoli che non tardano a attirare l'attenzione del Garante, il quale - a seguito di specifica istruttoria tempestivamente avviata - emette nel gennaio 2021 un'ordinanza nei confronti dell'Azienda sanitaria provinciale di Enna con cui eleva una sanzione amministrativa da 30.000 euro, corredata dalla pubblicazione del testo del provvedimento sul proprio sito web, nonché ingiunge la cancellazione dei dati biometrici dei dipendenti entro sessanta giorni dall'emissione dello stesso, avendo posto in essere il relativo trattamento di dati "in assenza di un idoneo presupposto di liceità". Le contestazioni del Garante Tralasciando alcune contestazioni di minor rilievo, l'Autorità incentra il proprio provvedimento sulla violazione da parte dell'ente siculo dell'art. 9 del GDPR, che disciplina il trattamento delle categorie particolari di dati personali, definizione in cui rientrano anche i 'dati sensibili', come definiti dalla precedente normativa. Nel far ciò, il Garante ricostruisce in maniera dettagliata il quadro normativo applicabile al trattamento di dati biometrici nel pubblico impiego, offrendo interessanti spunti di riflessione. In primo luogo, l'Autorità sottolinea come a seguito dell'entrata in vigore del GDPR, e a differenza di quanto avveniva nel previgente regime, i dati biometrici siano a tutti gli effetti da considerarsi quali 'dati sensibili'; ciò significa che per procedere al trattamento il titolare è tenuto a individuare non solo un'adeguata base giuridica, ma anche un'eccezione al divieto generale di trattamento contenuto al primo comma dell'art. 9. L'implementazione presso un ente pubblico di un sistema di rilevazione delle presenze e di verifica dell'osservanza dell'orario di lavoro basato su dati biometrici - prosegue l'Autorità - potrebbe in linea di principio rientrare in due delle deroghe previste dall'art. 9, trattandosi di un trattamento: necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare "in materia di diritto del lavoro"[2]; o, in alternativa necessario per "motivi di interesse pubblico rilevante"[3], da individuarsi nell'efficientamento della pubblica amministrazione. Entrambe le succitate deroghe richiedono però espressamente un fondamento normativo: nel primo caso, infatti, il trattamento di dati biometrici è consentito solo "nella misura in cui sia autorizzato" dal diritto dell'Unione o del singolo Stato membro, mentre nel secondo caso l'art. 2-sexies del Codice privacy ha condizionato l'applicazione della deroga prevista dal GDPR al fatto che l'interesse rilevante sia previsto "dal diritto dell'Unione Europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento". Il problema - non di poco momento - è che una simile norma semplicemente non esiste nel nostro ordinamento. Già, perché non solo l'iter normativo legato all'art. 2 della Legge concretezza - che prevedeva l'adozione di un regolamento attuativo destinato a individuare "specifiche garanzie per circoscrivere e specificare la portata della norma" - non è mai stato concluso, ma la Legge di bilancio 2021 ha completamente abrogato i commi che imponevano alle pubbliche amministrazioni l'obbligo di dotarsi di soluzioni tecnologicamente avanzate per la verifica dell'orario di lavoro. Lampante esempio di cortocircuito normativo connesso a un impianto legislativo ipertrofico e sempre più complesso. Ma il

Garante non si ferma a questa considerazione, e, quasi a stroncare definitivamente qualsiasi speranza residua degli operatori, specifica come a tale lacuna non sia possibile porre rimedio nemmeno ricorrendo alla deroga del consenso dell'interessato al trattamento dei propri 'dati sensibili'[4]: come più volte sottolineato sia a livello nazionale[5] che europeo[6], infatti, nell'ambito del contesto lavorativo il consenso non costituisce un valido presupposto di liceità del trattamento, in considerazione della natura del rapporto tra datore di lavoro e dipendente. Le conseguenze del provvedimento del Garante L'impatto pratico del provvedimento è senz'altro di notevole rilevanza. Il Garante stabilisce infatti che a oggi non esiste in Italia un presupposto normativo in grado di rendere lecito il trattamento di dati biometrici nell'ambito del pubblico impiego, quanto meno con riferimento alla rilevazione delle presenze dei dipendenti. Il tutto a distanza di nemmeno due anni dall'approvazione di una legge che identificava le tecnologie basate sul trattamento di tale tipologia di dati come uno strumento indispensabile per l'efficientamento degli enti pubblici e la lotta all'assenteismo. A ciò si aggiunga che quanto all'utilizzo di tali dati per ulteriori finalità connesse alla gestione del rapporto di lavoro andrà comunque individuata una disposizione normativa ad hoc, eventualmente facendo leva sulla pur ambigua formulazione dell'art. 2-septies, comma 7, del Codice Privacy (che ammette l'utilizzo di dati biometrici "con riguardo alle procedure di accesso fisico e logico da parte dei soggetti autorizzati nel rispetto delle misure di garanzia di cui al presente articolo") o ad altre norme specifiche quali quelle che consentono l'uso della firma grafometrica ai sensi del D. lgs. 82/2005. In assenza, il trattamento risulterebbe illegittimo e fonte di un concreto rischio sanzionatorio da parte dell'Autorità. Ma a ben vedere le conclusioni del Garante, contenute nel provvedimento in esame, hanno una carica dirompente ben più elevata, in grado di valicare i confini del settore del pubblico impiego, andando a interessare imprese ed enti privati: anche i trattamenti da questi effettuati nei confronti dei propri dipendenti sono senz'altro da considerarsi potenzialmente illegittimi in assenza di una disposizione normativa di rango adeguato a supporto e con il Provvedimento generale in tema di biometria adottato nel 2014 dal Garante - guida insostituibile per gli operatori più accorti e attenti alla tutela dei dati dei propri dipendenti - che appare ridimensionato, se non relegato all'irrilevanza. Si auspica quindi un intervento legislatore che fornisca in tempi brevi un supporto normativo idoneo a colmare il vuoto venutosi a creare e garantisca che enti pubblici e privati possano quanto meno valutare con serenità e certezza l'adozione di sistemi tecnologicamente avanzati nell'ambito del rapporto di lavoro. Note Provvedimento del 15 settembre 2016, n. 357. art. 9, c.2, lett. b) del GDPR. art. 9, c.2, lett. g) del GDPR. art. 9, c.2, lett. a) del GDPR. Cfr. Provvedimento del 13 febbraio 2020, n. 35. "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", WP29, 'Parere 2/2017 sul trattamento dei dati sul posto di lavoro', 8 giugno 2017.