

FRANCESCA CONTE

IL TRATTAMENTO DEI DATI BIOMETRICI NEI LUOGHI DI LAVORO. ANALISI COMPARATA TRA L'ESPERIENZA ITALIANA E TEDESCA

SOMMARIO: 1. Il dato biometrico: definizione e applicazione nel contesto lavorativo. — 2. La disciplina del GDPR: tra principi comuni e autonomia degli Stati Membri. — 3. L'impiego della biometria in ambito lavorativo nella normativa italiana: lo Statuto dei lavoratori e il Codice privacy. — 4. I principi e le garanzie per il trattamento dei dati biometrici dei lavoratori individuati dal Garante italiano per la protezione dei dati personali. — 5. Il trattamento dei dati biometrici in ambito lavorativo nella normativa tedesca: la nuova Legge federale sulla protezione dei dati personali. — 6. Le condizioni di legittimità nella legislazione tedesca: l'alternatività tra consenso e contratto collettivo. — 7. Un difficile punto di incontro tra i due quadri normativi. — 8. Considerazioni conclusive.

1. IL DATO BIOMETRICO: DEFINIZIONE E APPLICAZIONE NEL CONTESTO LAVORATIVO.

Le modalità di impiego delle tecnologie biometriche nei contesti lavorativi sono numerose. Queste possono comportare considerevoli aumenti di produttività e, al contempo, possono dare luogo ad un generale miglioramento delle condizioni di lavoro, garantendo una maggior tutela al lavoratore. Si pensi, a titolo esemplificativo, all'impiego di esoscheletri robotici a supporto delle attività manuali dei lavoratori, alla possibilità di gestire i sistemi di accesso o di controllo delle presenze mediante sensori biometrici o, ancora, alla personalizzazione delle postazioni di lavoro tramite tecnologie ergonomiche auto-adattive¹. I diversi impieghi delle tecnologie biometriche devono, tuttavia, essere temperati con la necessità di tutelare la sfera personale dell'individuo. Infatti, il grado di invasività derivato dal trattamento del dato biometrico è particolarmente elevato, in quanto tale dato presenta un collega-

¹ L. GRECO, A. MANTELERO, *Industria 4.0, robotica e privacy-by-design*, in questa *Rivista*, n. 6, 2018, 876 e ss.. Sui sistemi di autenticazione attraverso dati biometrici,

cfr. B. RUBIS, *Sistemi di autenticazione mediante l'utilizzo di dati biometrici*, in questa *Rivista*, 2023.

mento permanente con l'individuo. Per questa ragione, il quadro normativo attualmente vigente prevede una serie di misure multilivello a tutela del lavoratore in caso di trattamento dei suoi dati biometrici, che saranno esaminate nel presente lavoro.

Procedendo per gradi nell'analisi della disciplina, pare utile iniziare con l'inquadramento normativo del dato biometrico. L'art. 4 comma 1 n. 14² del Regolamento 2016/679 lo definisce in base alla funzione teleologica di consentire o confermare l'identificazione univoca della persona³. È incluso all'interno delle categorie di dati particolari ai sensi dell'art. 9 comma 1, il cui trattamento è generalmente vietato⁴. Il Regolamento prevede però determinate eccezioni al divieto, esplicitate al comma 2⁵. In virtù del margine di autonomia riconosciuto agli Stati Membri ai

² Regolamento europeo n. 2016/679, « Regolamento generale sulla protezione dei dati », art. 4, 1° co. n. 14: « Dato personale derivato da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici ».

³ C. JASSERAND, *Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data*, in *European Data Protection Law Review*, n. 2, 2016, 302.

⁴ Regolamento europeo n. 2016/679, « Regolamento generale sulla protezione dei dati », art. 9, 1° co.: « È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona ».

⁵ Regolamento europeo n. 2016/679, « Regolamento generale sulla protezione dei dati », art. 9, 2° co.: « Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è 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; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitano le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista

sensi dell'art. 9 comma 4⁶, poi, la disciplina si compone ulteriormente delle legislazioni nazionali.

Tra gli Stati Membri, la Germania ha storicamente sviluppato per prima una forte cultura della *privacy*, divenendo portatrice prodromica di una serie di principi e valori poi divenuti europei⁷. Il riconoscimento del potere di controllo sulle proprie informazioni quale diritto assoluto dell'individuo da parte della Corte Federale Tedesca⁸ ha contribuito a formare un consolidato quadro normativo riguardante la protezione dei dati personali⁹. L'Italia ha seguito invece un'evoluzione differente, adottando una propria normativa solamente dopo la Direttiva 95/46/CE¹⁰.

Dal punto di vista giuridico pare quindi utile analizzare le modalità con cui i due ordinamenti disciplinano il trattamento dei dati biometrici nei luoghi di lavoro, ponendoli, infine, a confronto. La comparazione che si propone permette di porre in luce le differenze e le somiglianze tra i due ordinamenti nel tentativo di individuare il miglior bilanciamento tra il diritto alla protezione dei dati personali dei lavoratori e l'interesse alla produttività aziendale del datore.

2. LA DISCIPLINA DEL GDPR: TRA PRINCIPI COMUNI E AUTONOMIA DEGLI STATI MEMBRI.

Come anticipato, i trattamenti dei dati biometrici compiuti nei contesti lavorativi sono soggetti all'applicazione del Regolamento 2016/679. In primo luogo, il datore è responsabile del rispetto dei

della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato ».

⁶ Regolamento europeo n. 2016/679, « Regolamento generale sulla protezione dei

dati », art. 9, 4° co.: « Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute ».

⁷ Come approfondito da M. WEISS, B. GECK, *Worker privacy in Germany*, in *Comparative Labour Law Journal*, n. 17, 1995, 75 ss.

⁸ BVERFG, 13 aprile 1983, in *Neue Juristische Wochenschrift*, 1984, 385 ss.

⁹ T. HOEREN, *Teil 1: Technische Grundlagen*, in T. Hoeren, U. Sieber, B. Holznager (a cura di), *Handbuch Multimedia-Recht*, München, 2022, 6.

¹⁰ Fino a quel momento, infatti, era riconosciuta tutela solo come precipitato dell'identità personale e del diritto alla riservatezza, non rilevando come diritto autonomo e a sé stante, si veda G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia - Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, 9.

principi di cui all'art. 5 in quanto titolare del trattamento ¹¹, ed è obbligato a dar prova della loro corretta attuazione in tutte le fasi di utilizzo dei dati. Ai fini della liceità del trattamento, è necessario che questo si fondi su una base legittima, che può essere individuata dal Regolamento o dal diritto dei singoli Stati Membri.

Nei luoghi di lavoro, molti dei trattamenti sui dati biometrici appaiono riconducibili all'ipotesi prevista all'art. 9 comma 2 lett. b). Tale norma consente il trattamento di categorie particolari di dati per l'assolvimento di obblighi o l'esercizio di diritti del titolare o dell'interessato in materia di diritto del lavoro e della sicurezza sociale ¹². Così, a titolo esemplificativo, può essere consentito il trattamento basato sui dati biometrici per limitare l'utilizzo di macchinari pericolosi ai soli lavoratori qualificati.

Individuata la base legittima, il titolare deve procedere all'adozione di misure tecniche ed organizzative adeguate alla protezione dei dati biometrici. A seconda del tipo di trattamento, le tecniche utilizzabili possono variare. La loro scelta è rimandata al titolare o al responsabile di trattamento alla luce del principio di *accountability*. Ciononostante, il Gruppo di Lavoro Articolo 29 ¹³ ha individuato alcune tipologie di misure da considerarsi adeguate nel contesto dei dati biometrici. In particolare, nella fase di conservazione del dato, l'utilizzo di tecnologie a crittazione biometrica consentirebbe al dato biometrico di essere immediatamente codificato, impedendo la riferibilità dell'informazione alla parte del corpo (es. impronta digitale, iride, voce) da cui deriva ¹⁴. Ulteriore garanzia di sicurezza è costituita dalla *smart card*, che permette l'isolamento dei dati ivi contenuti, diminuendo sensibilmente il rischio di eventuali fughe di dati.

Dall'esame della disciplina applicabile ¹⁵ emerge che il Regola-

¹¹ L'individuazione del titolare di trattamento nella persona del datore di lavoro è affermata in GARANTE PRIVACY, *Linee guida sul trattamento di dati personali dei lavoratori privati*, 23 novembre 2006, (doc. web 1364939), 5: « In linea di principio, per individuare il titolare del trattamento rileva l'effettivo centro di imputazione del rapporto di lavoro, al di là dello schema societario formalmente adottato ».

¹² Regolamento europeo n. 2016/679, « Regolamento generale sulla protezione dei dati », art. 9, 2° co., lett. b).

¹³ Il Gruppo di Lavoro Articolo 29 è stato il gruppo di lavoro europeo indipendente « per la tutela delle persone con riguardo al trattamento dei dati personali », come definito all'art. 29 dir. 46/95/CE, la cui disciplina era fissata dalla Direttiva 46/95/CE. Con l'entrata in vigore del Regola-

mento 2016/679, è stato sostituito dal Comitato Europeo per la Protezione dei Dati Personali (CEPDP). I Pareri forniti in passato dal Gruppo di Lavoro Articolo 29 sono stati approvati dal CEPDP e rimangono quindi valide linee guida per la miglior applicazione dei principi stabiliti dal Regolamento.

¹⁴ Gruppo di Lavoro Articolo 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, WP193, adottato il 27 aprile 2012.

¹⁵ Al fine di completare il quadro normativo è opportuno richiamare i diritti riconosciuti all'interessato e che si applicano anche al caso specifico. L'individuo è tutelato dalla disciplina del Regolamento anche mediante il riconoscimento di una serie di diritti, che gli consentono di esercitare un effettivo controllo sui suoi dati personali.

mento non presenta disposizioni unicamente dedicate al trattamento dei dati biometrici nell'ambito dei rapporti di lavoro né tenta di armonizzare le normative nazionali in materia ¹⁶. Come si avrà modo di illustrare nei paragrafi successivi, le discipline nazionali riguardanti le condizioni di trattamento dei dati biometrici nell'ambito lavorativo sono diversificate, essendo queste definite dai singoli Stati Membri sulla base delle proprie norme di diritto del lavoro.

3. L'IMPIEGO DELLA BIOMETRIA IN AMBITO LAVORATIVO NELLA NORMATIVA ITALIANA: LO STATUTO DEI LAVORATORI E IL CODICE PRIVACY.

Insieme all'art. 9 comma 2 lett. b) del Regolamento, nello scenario italiano è opportuno considerare le previsioni di cui al titolo I dello Statuto dei Lavoratori ¹⁷ e il d.lgs. 196/2003 (di seguito sempre "Codice Privacy") ¹⁸. Il Codice Privacy come modificato dal d.lgs. 101/2018 all'art. 114 fa espressamente salva la disciplina prevista all'art. 4 Stat. Lav. sul trattamento dei dati dei lavoratori effettuato per finalità di controllo a distanza. La disposizione statutaria contempera l'interesse datoriale all'organizzazione e alla produttività dell'azienda con la protezione della dignità e riservatezza del lavoratore. Il comma 1 dell'articolo 4 Stat. Lav. prevede, infatti, che l'utilizzo di strumenti da cui possa derivare un controllo a distanza sia legittimo solo quando finalizzato all'organizzazione, alla sicurezza del lavoro e alla tutela del patrimonio aziendale, in presenza di un accordo con le rappresentanze sindacali ¹⁹. Tale accordo non è però richiesto quando i dispositivi sono utilizzati dal lavoratore per la propria presta-

Così, l'interessato può richiedere l'accesso (art. 15), la rettifica (art. 16) e la cancellazione (art. 17) dei suoi dati e ha diritto a ricevere informazioni inerenti al trattamento (art. 12). Nell'ottica di un trattamento trasparente, il titolare è altresì tenuto ad informare l'interessato nei casi in cui la violazione di dati personali comporti un rischio particolarmente elevato per i suoi diritti e libertà.

¹⁶ P. GOIA, *Handbuch Beschäftigten-datenschutz - aktuelle Rechtsfragen und Umsetzungshilfen*, Köln, 2020, 181.

¹⁷ Riguardanti più in generale la libertà e la dignità del lavoratore, A. TROISI, *Il diritto del lavoratore alla protezione dei dati personali*, Torino, 2013, 108.

¹⁸ D.lgs. 30 giugno 2003, n. 196, « Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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 », pubblicato in G. U. 29 luglio 2003, n. 174.

¹⁹ Legge 20 maggio 1970, n. 300, « Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento », art. 4, 1° co.: « Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale

zione o sono installati per registrare gli accessi e le presenze del personale²⁰. La disposizione statutaria²¹ prevede quindi condizioni differenti a seconda dello scopo perseguito²².

L'art. 4 Stat. Lav. si coordina con il Codice Privacy, che all'art. 2-septies prevede il rispetto delle misure di garanzia come ulteriore condizione per il legittimo trattamento dei dati biometrici. Dal dettato normativo si evince che il Garante per la protezione dei dati personali può infatti indicare ulteriori condizioni sulla base delle quali il trattamento di tali dati è consentito²³. Le misure di garanzia completano quindi il quadro normativo attualmente vigente in materia di trattamento dei dati biometrici.

accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi».

²⁰ Legge 20 maggio 1970, n. 300, «Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento», art. 4, 2° co.: «La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze».

²¹ Per completezza espositiva si richiama anche il 3° co. dell'art. 4, riguardante il riutilizzo dei dati: «Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196».

²² Sul punto è opportuno considerare che le tecnologie biometriche sollevano rilevanti dubbi circa l'applicazione del regime semplificato di cui al comma 2, quando sono utilizzate per la rilevazione degli accessi e per l'utilizzo degli strumenti di lavoro. Una parte della dottrina ritiene che la loro idoneità a rivelare i movimenti del personale durante l'attività lavorativa si tradurrebbe in un potenziale monitoraggio a distanza, come tale legittimo solo in presenza di un accordo con le rappresentanze sindacali ai

sensi del comma 1. Si veda C. COLOSIMO, *La moderna declinazione del potere di controllo*, in AA.VV., *Diritti e doveri nel rapporto di lavoro*, Milano, 2018, 67. Tuttavia, come da ISPETTORATO NAZIONALE DEL LAVORO, *Circolare n. 5/2018*, 19 febbraio 2018, 5, si deve ritenere che il trattamento dei dati biometrici sia legittimo in assenza dell'accordo sindacale, quando la finalità unicamente perseguita consiste nell'accesso ad aree riservate o nell'utilizzo di determinati strumenti considerati pericolosi. Per maggiori approfondimenti si veda I. ALVINO, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *Labour & Law Issues*, n. 2, 2016, 3 ss.

²³ D.lgs. 196/2003, art. 2-septies, 1°-5° co.: «In attuazione di quanto previsto dall'articolo 9, paragrafo 4, del regolamento, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo. Il provvedimento che stabilisce le misure di garanzia di cui al comma 1 è adottato con cadenza almeno biennale e tenendo conto: a) delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali; b) dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure; c) dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea. Lo schema di provvedimento è sottoposto a consultazione pubblica per un periodo non inferiore a sessanta giorni. Le misure di garanzia sono adottate nel rispetto di quanto previsto dall'articolo 9, paragrafo 2, del Regolamento, e riguardano anche le cautele da adottare relativamente a: a) contrassegni

Come risulta dall'analisi delle norme, il legislatore non ha fatto uso del margine di autonomia previsto all'art. 9 comma 2 lett. b) per introdurre nuove condizioni di trattamento dei dati biometrici in materia di diritto del lavoro. Tale lacuna²⁴ è stata da ultimo sottolineata dal Garante in riferimento al rilevamento degli accessi e delle presenze dei lavoratori sia nel settore pubblico²⁵ che in quello privato²⁶. Secondo l'Autorità, la finalità di controllo degli ingressi potrebbe rientrare nell'ambito di applicazione dell'art. 9 comma 2 lett. b), perché il trattamento dei dati degli interessati permetterebbe di adempiere l'obbligo di sicurezza sul lavoro che sorge in capo al datore. Affinché risulti legittimo, è necessario che il trattamento trovi fondamento in una norma del diritto nazionale o dell'Unione, che individui le condizioni per le quali tale trattamento risulti proporzionato rispetto alla finalità perseguita. Allo stato, tuttavia, una simile disposizione non è presente nell'ordinamento italiano. Di conseguenza, l'art. 9 comma 2 lett. b) non è applicabile al trattamento dei dati biometrici per questa finalità. Nemmeno le restanti condizioni di trattamento offerte dall'art. 9 possono, nel caso di specie, sostituirsi all'assenza normativa²⁷. In mancanza di una base giuridica riconosciuta come idonea, il Garante ha stabilito quindi l'illegittimità del trattamento dei dati biometrici per la rilevazione degli accessi e delle presenze dei lavoratori²⁸.

sui veicoli e accessi a zone a traffico limitato; b) profili organizzativi e gestionali in ambito sanitario; c) modalità per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute; d) prescrizioni di medicinali. Le misure di garanzia sono adottate in relazione a ciascuna categoria dei dati personali di cui al comma 1, avendo riguardo alle specifiche finalità del trattamento e possono individuare, in conformità a quanto previsto al comma 2, ulteriori condizioni sulla base delle quali il trattamento di tali dati è consentito. In particolare, le misure di garanzia individuano le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonimizzazione, le misure di minimizzazione, le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a garantire i diritti degli interessati ».

²⁴ Con la Legge 19 giugno 2019, n. 56, « Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo », era stato previsto all'art. 2 l'obbligo di rilevazione delle presenze tramite il trattamento dei dati biometrici dei dipendenti della Pubblica Amministrazione, a cui si aggiungeva la verifica

dell'identità tramite videocamere di sorveglianza. A seguito dei pareri negativi dell'Autorità Garante per la Protezione dei Dati Personali, tuttavia, la legge non ha ricevuto attuazione ed è stata dopo poco tempo abrogata. Per maggiori approfondimenti, si veda GARANTE PRIVACY, *Audizione del Presidente dell'Autorità Garante per la protezione dei dati personali sul disegno di legge n. 920, recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo* del 27 novembre 2018 (doc. web n. 9064421).

²⁵ GARANTE PRIVACY, provvedimento del 14 gennaio 2021 (doc. web n. 9542071).

²⁶ GARANTE PRIVACY, provvedimento del 10 novembre 2022 (doc. web n. 9832838).

²⁷ Il consenso, in particolare, non costituisce un valido presupposto di legittimità, in quanto nei contesti lavorativi permane un forte squilibrio tra l'interessato e il titolare, si veda GARANTE PRIVACY, provvedimento del 13 febbraio 2020 (doc. web n. 9285411).

²⁸ La questione rimane aperta per quanto riguarda il caso in cui il datore di lavoro stipuli un contratto collettivo con le rappresentanze sindacali aziendali che re-

4. I PRINCIPI E LE GARANZIE PER IL TRATTAMENTO DEI DATI BIOMETRICI DEI LAVORATORI INDIVIDUATI DAL GARANTE ITALIANO PER LA PROTEZIONE DEI DATI PERSONALI.

I recenti provvedimenti del Garante sollevano rilevanti dubbi circa l'utilizzo dei dati biometrici per finalità di accesso ai locali aziendali. *In primis*, l'interpretazione restrittiva dell'art. 9 comma 2 lett. b) da parte dell'Autorità porterebbe a sostenere che il trattamento dei dati biometrici sia legittimo solo in presenza di una disposizione normativa che lo disciplini. A tal proposito pare utile ricordare che il legislatore ha stabilito all'art. 2-*septies* la legittimità del trattamento dei dati biometrici quando basato su una delle condizioni previste dall'art. 9 comma 2 del Regolamento. A parere di chi scrive, l'art. 2-*septies* integra idonea base giuridica ai sensi dell'art. 9 comma 2 lett. b), perché implicitamente richiama la stessa condizione di legittimità con riguardo al diritto interno. Cosicché, non risulta imprescindibile l'intervento del legislatore nella definizione espressa delle finalità, bastando che dall'interpretazione delle norme applicabili emerga la sussistenza di un obbligo da adempiere o di un diritto da esercitare nell'ambito lavorativo per cui il trattamento si renda necessario²⁹.

In secondo luogo, se anche si seguisse l'orientamento restrittivo del Garante, risulterebbe incerto in quali casi il controllo degli accessi sia funzionale all'adempimento dell'obbligo di tutela della sicurezza dei dipendenti. Principale rilevanza assumono a tal

golamenti il trattamento dei dati biometrici del personale.

²⁹ Tale considerazione pare essere supportata dalla C.G.U.E., Sentenza del 26 gennaio 2023, « V.S. » contro « Ministerstvo na vutreshnite raboti », C-205/21, EU:C:2023:49, ove, nel valutare la legittimità del trattamento di dati biometrici compiuto dalle forze di polizia ai sensi della Dir. (UE) 2016/680, si afferma che l'esistenza di una chiara, precisa e inequivocabile base giuridica derivante dall'interpretazione di tutte le norme applicabili al trattamento dei dati biometrici per finalità di prevenzione e ricerca dei reati sia sufficiente ad autorizzare il trattamento, anche in assenza di un preciso riferimento alla fonte normativa principale. Dalla sentenza in commento: « Alla luce di tutte le suseposte considerazioni, occorre rispondere alle prime due questioni dichiarando che l'articolo 10, lettera a), della direttiva 2016/680, letto alla luce dell'articolo 52 della Carta, deve essere interpretato nel senso che il trattamento di dati biometrici e genetici da parte delle autorità di polizia per le loro attività di ricerca, a fini

di lotta contro la criminalità e di tutela dell'ordine pubblico, è autorizzato dal diritto dello Stato membro, ai sensi dell'articolo 10, lettera a), di tale direttiva, se il diritto di tale Stato membro contiene una base giuridica sufficientemente chiara e precisa per autorizzare detto trattamento. La circostanza che l'atto legislativo nazionale contenente una simile base giuridica faccia, inoltre, riferimento al RCPD, e non alla direttiva 2016/680, non è di per sé idonea a rimettere in discussione l'esistenza di una simile autorizzazione, purché dall'interpretazione di tutte le disposizioni applicabili del diritto nazionale risulti in modo sufficientemente chiaro, preciso e inequivocabile che il trattamento di dati biometrici e genetici in questione rientra nell'ambito di applicazione di tale direttiva, e non di tale regolamento ». Calato nel contesto lavorativo, l'ordinamento italiano individua espressamente all'art. 2-*septies* Cod. Privacy le condizioni di trattamento dei dati biometrici, consistenti nella presenza di una base giuridica ex art. 9, 2° co., reg. 2016/679 e nel rispetto delle misure di garanzia del

proposito i provvedimenti generali adottati dal Garante³⁰, a cui il legislatore ha demandato di individuare i contesti in cui il trattamento di alcune categorie particolari³¹ è considerato lecito. In particolare, l'Autorizzazione Generale 1/2016³² disciplina l'utilizzo dei dati biometrici, genetici e relativi alla salute in riferimento ai rapporti di lavoro. Il provvedimento include la sicurezza dell'interessato o di un terzo tra le finalità per le quali il trattamento deve risultare « indispensabile »³³. Così, non si può escludere a priori che il trattamento dei dati biometrici finalizzato a proteggere il lavoratore da situazioni o macchinari pericolosi sia considerato legittimo, quando, secondo un giudizio di proporzio-

Garante. La sussistenza di una norma del diritto del lavoro, che definisce l'obbligo o il diritto per cui è necessario trattare i dati sensibili dell'interessato risponde al requisito definito all'art. 9, 2° co., lett. b) reg. 2016/679, così come l'Autorizzazione Generale 1/2016 definisce le misure di garanzia che il titolare è tenuto a rispettare.

³⁰ D.lgs. 10 agosto 2018, n. 101, « Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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) », art. 21 ne disciplina il contenuto. In particolare: « Il Garante per la protezione dei dati personali, con provvedimento di carattere generale [...] individua le prescrizioni contenute nelle autorizzazioni generali già adottate, relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 2, lettera b) e 4, nonché al Capo IX del regolamento (UE) 2016/679, che risultano compatibili con le disposizioni del medesimo regolamento e del presente decreto e, ove occorra, provvede al loro aggiornamento ».

³¹ Si fa riferimento ai dati biometrici, ai dati genetici e ai dati relativi alla salute, ex Regolamento europeo n. 2016/679, « Regolamento generale sulla protezione dei dati », art. 9, 4° co.

³² Di recente l'Autorità ne ha riconosciuto il contenuto come compatibile con le disposizioni del Regolamento 2016/679 e del novellato Codice Privacy. A tal proposito, ai sensi del d.lgs. 101/2018, art. 21, 4° co. l'Autorizzazione Generale 1/2016 continua a produrre effetti nell'ordinamento fino all'adozione delle misure di garanzia ex art. 2-septies d.lgs. 196/2003.

³³ GARANTE PRIVACY, *Autorizzazione generale 1/2016* del 15 dicembre 2016, (doc. web n. 5800451): « Il trattamento delle categorie particolari di dati personali è effettuato solo se necessario (art. 9, par. 2 Regolamento UE 2016/679): a) per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa dell'Unione europea, da leggi, da regolamenti o da contratti collettivi anche aziendali, ai sensi del diritto interno, in particolare ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro (art. 88 del Regolamento UE 2016/679), nonché del riconoscimento di agevolazioni ovvero dell'erogazione di contributi, dell'applicazione della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro, nonché in materia fiscale e sindacale; b) anche fuori dei casi di cui alla lettera a), in conformità alla legge e per scopi determinati e legittimi, ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori; c) per perseguire finalità di salvaguardia della vita o dell'incolumità fisica del lavoratore o di un terzo; d) per far valere o difendere un diritto, anche da parte di un terzo, in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione, nei casi previsti dalle leggi, dalla normativa dell'Unione europea, dai regolamenti o dai contratti collettivi, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose; resta salvo quanto stabilito dall'art. 60 del Codice; e) per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsa-

nalità, esso risulti necessario al raggiungimento dello scopo ³⁴. La finalità di sicurezza sul lavoro, in quanto richiamata dall'Autorizzazione Generale 1/2016, può dunque consentire il trattamento dei dati biometrici ai sensi dell'art. 9 comma 2 lett. b). Resta quindi incerto il confine tra la rilevazione degli accessi per interesse di controllo e quella per finalità di sicurezza dei lavoratori.

Tutto ciò considerato, sembra opportuno ricordare il « Provvedimento generale prescrittivo in tema di biometria » ³⁵ pubblicato dal Garante nel 2014, che completa la normativa al momento vigente ³⁶. L'Autorità ha inteso delineare un quadro di misure organizzative e tecniche per aumentare la sicurezza dei dati biometrici durante tutte le fasi di trattamento. Nella fase di registrazione, per esempio, il titolare deve utilizzare dei sistemi biometrici che permettano di raccogliere una quantità di dati adeguata alla finalità perseguita ³⁷. Una volta raccolti, i dati devono essere cifrati e conservati preferibilmente in un dispositivo in possesso dell'interessato, come un *token* o una *smart card*. In questo modo, i dati biometrici ivi contenuti rimangono separati dalle informazioni che consentono l'identificazione dell'interessato, limitando i rischi di furto di identità. La conservazione dei dati e il loro utilizzo devono essere limitati per il tempo strettamente necessario al raggiungimento della finalità. Quando questa viene meno, tutte le informazioni devono essere rimosse dai supporti di memorizzazione. Infine, dall'Autorità è particolar-

bilità del datore di lavoro in materia di salute e sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale; f) per garantire le pari opportunità nel lavoro; g) per perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi, in materia di assistenza sindacale ai datori di lavoro ».

³⁴ Nell'esperienza del Garante per la protezione dei dati personali, si richiama a titolo esemplificativo GARANTE PRIVACY, provvedimento del 1° febbraio 2007 (doc. web n. n. 1381983).

³⁵ Garante Privacy, *Provvedimento generale prescrittivo in tema di biometria* del 12 novembre 2014 (doc. web n. 3556992).

³⁶ Il Garante per la protezione dei dati personali ha definito nel corso degli anni un sistema di regole inerenti al trattamento dei dati biometrici in azienda in un'ottica di « sostanziale funzione di suppletiva legislativa », come approfondito da M. DEL CONTE, *Internet, posta elettronica e oltre: il Garante della privacy rimodula i poteri del*

datore di lavoro, in *Diritto dell'Informatica*, n. 2, 2007, 509. I primi provvedimenti di carattere generale adottati dal Garante per la Protezione dei Dati Personali sancivano il divieto di trattamento generalizzato e incontrollato dei dati biometrici dei lavoratori con particolare riferimento alle impronte digitali. Per maggiori approfondimenti, GARANTE PRIVACY, *Linee guida sul trattamento di dati personali dei lavoratori privati*, cit. A titolo esemplificativo, il dato biometrico del lavoratore poteva essere trattato per limitare l'accesso ad aree di produzione considerate pericolose per la sua incolumità, ma non anche per il controllo della sua presenza quotidiana in azienda. Si veda GARANTE PRIVACY, provvedimento del 15 giugno 2006 (doc. web n. 1306523).

³⁷ Un sistema inefficiente, infatti, si espone a un numero maggiore di errori nel riconoscimento degli interessati; al contrario, grandi quantità di dati portano alla ricostruzione del tratto fisico da cui l'informazione biometrica deriva, con ciò spesso violando la proporzionalità del trattamento rispetto alla finalità perseguita. GARANTE PRIVACY, *Provvedimento generale prescrittivo in tema di biometria*, cit.

mente consigliata la nomina di amministratori di sistema abilitati a svolgere attività di supporto tecnico, di manutenzione e gestione dei *server* dei sistemi biometrici.

Dalla disamina compiuta, si evince che il titolare non possa prescindere dall'osservanza delle prescrizioni del Garante per trattare lecitamente i dati biometrici. Le Linee Guida contribuiscono infatti ad individuare le modalità necessarie affinché il trattamento possa considerarsi conforme alle disposizioni del Regolamento e del Codice Privacy, al punto che la giurisprudenza riconosce una "colpa di organizzazione" per il titolare del trattamento che non le rispetti³⁸. Queste assumono quindi rilevanza centrale, integrando la disciplina nazionale vigente per il trattamento dei dati biometrici dei lavoratori.

5. IL TRATTAMENTO DEI DATI BIOMETRICI IN AMBITO LAVORATIVO NELLA NORMATIVA TEDESCA: LA LEGGE FEDERALE SULLA PROTEZIONE DEI DATI PERSONALI.

Il quadro normativo tedesco riguardante i trattamenti di categorie particolari di dati nell'ambito dell'instaurazione, prosecuzione ed estinzione del rapporto di lavoro si compone, insieme alle disposizioni del Regolamento, dei parr. 22 e 26 *Bundesdatenschutzgesetz* (BDSG). Il par. 26 è centrale, perché individua i soggetti interessati³⁹, le basi giuridiche e gli obblighi in capo al titolare⁴⁰. La disposizione trova applicazione nei casi di trattamento di dati appartenenti esclusivamente ai « *Beschäftigte* [di-

³⁸ Cass. Civ., Sez. I, ord. n. 6642/2023, *motivi della decisione*, punto 2, ove la mancata verifica degli adempimenti richiesti dal Garante per il trattamento dei dati biometrici nell'ambito del controllo degli accessi e delle presenze dei propri dipendenti ha comportato la responsabilità per colpa da organizzazione del datore di lavoro titolare del trattamento.

³⁹ *Bundesdatenschutzgesetz*, par. 26, 8° co.: « *Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeiterinnen und Leiharbeiternehmer im Verhältnis zum Entleiher; 2. zu ihrer Berufsbildung Beschäftigte; 3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeiterprobung (Rehabilitandinnen und Rehabilitanden); 4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte; 5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstgesetz oder dem Bundesfreiwilligendienstgesetz leisten; 6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichge-*

stellten; 7. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte ».

⁴⁰ La sua applicazione si coordina con il *Betriebsverfassungsgesetz* (lett. Legge sulla costituzione delle opere), il cui par. 75, 2° co. prevede il diritto in capo al dipendente di non vedersi ristretta la propria sfera di diritti nell'ambito dell'attività lavorativa: « *Arbeitgeber und Betriebsrat haben die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Sie haben die Selbständigkeit und Eigeninitiative der Arbeitnehmer und Arbeitsgruppen zu fördern* ». Come approfondito da A. ALBRECHT, *Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz*, Frankfurt am Main, 2003, 197, il datore di lavoro e il comitato d'azienda hanno dunque l'obbligo di tutelare e promuovere il libero sviluppo della personalità del lavoratore, dovendosi astenere dal commettere azioni che potrebbero comportare il

pendenti] »⁴¹. Nella definizione fornita dalla norma sono ricompresi anche i dipendenti federali, i militari e i giudici⁴².

Il par. 26 inoltre richiama⁴³ il par. 22 comma 2 BDSG per quanto concerne le misure tecniche ed organizzative da adottare per tutelare le categorie particolari di dati⁴⁴. La disposizione è finalizzata a fornire un elenco non esaustivo di modalità attra-

restringimento della sfera dei suoi diritti. Tale esigenza è sentita soprattutto per i dati biometrici, il cui trattamento è considerato particolarmente invasivo.

⁴¹ A titolo esemplificativo, vengono inclusi come tali ai sensi del *Bundesdatenschutzgesetz*, par. 26, 8° co., i lavoratori, anche temporanei, caratterizzati da un rapporto di dipendenza economica con il datore; le persone impiegate a scopo di formazione professionale; i partecipanti ai test attitudinali o prove di lavoro; i volontari come definiti dalla *Jugendfreiwilligendienstgesetz* o dalla *Bundesfreiwilligendienstgesetz*; i lavoratori impiegati nel lavoro a domicilio, i funzionari federali, i giudici federali, i militari e le persone che prestano servizio civile.

⁴² Nell'ordinamento tedesco i dipendenti federali, i militari e i giudici non sono soggetti ad un contratto di lavoro regolato dalle norme civilistiche. L'inclusione di queste categorie, caratterizzate da un rapporto di lavoro pubblico, ha acceso discussioni in dottrina circa la conformità della previsione con il Regolamento. Secondo F. MASCHIMANN, *Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht*, in *Neue Zeitschrift für Arbeitsrecht*, n. 4, 2018, 120, l'inclusione di queste categorie si porrebbe in contrasto con l'obiettivo di armonizzazione perseguito dalla normativa europea. Si sostiene che l'applicazione del par. 26 a tutti i rapporti di lavoro, sia pubblici che privati, porterebbe ad una ulteriore frammentazione della disciplina di protezione dei dati. L'art. 88 del Regolamento, facendo diretto riferimento ai contratti collettivi, permetterebbe agli ordinamenti nazionali di definire ulteriori condizioni di trattamento solo in relazione ai rapporti di lavoro tra privati, non esistendo contratti collettivi applicabili ai rapporti di lavoro pubblico. La dottrina maggioritaria considera tuttavia l'allargamento della portata applicativa del BDSG ai dipendenti pubblici legittimo. Come spiegato da M. Korr, *Der Beschäftigtendatenschutz gem. §26 BDSG-neu: ist die Ausfüllung der Öffnungsklausel des Art. 88 DSGVO geglückt?*, in *Zeitschrift für Datenschutz*, n. 2, 2017, 322, il legislatore europeo autorizza gli Stati Membri a disciplinare autonomamente il trattamento per finalità inerenti al rapporto di lavoro ex artt. 88 e 9 comma 2 lett. b). Dunque, l'allargamento della portata applicativa ai dipen-

denti pubblici da parte della normativa nazionale è considerato ammissibile in virtù del margine di autonomia offerto. Ne consegue che gli Stati Membri possono estendere gli standard di protezione ad altre categorie di soggetti non impiegati nel settore privato. Per maggiori approfondimenti, K. STAMER, M. KUHNKE, *Datenverarbeitung im Beschäftigungskontext*, in K. Plath (a cura di) *DSGVO BDSG - Kommentar*, Köln, 2018, 693.

⁴³ Par. 26 c. 3 ultima parte BDSG: « § 22 Absatz 2 gilt entsprechend ».

⁴⁴ *Bundesdatenschutzgesetz*, par. 22, 2° co.: « In den Fällen des Absatzes 1 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören: 1. technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt; 2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind; 3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten; 4. Benennung einer oder eines Datenschutzbeauftragten; 5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern; 6. Pseudonymisierung personenbezogener Daten; 7. Verschlüsselung personenbezogener Daten; 8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; 9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen

verso le quali proteggere gli interessi del lavoratore⁴⁵. A titolo esemplificativo, si richiamano la pseudonimizzazione del dato e la crittografia. Poiché la norma in esame non distingue i tipi di accorgimenti da adottare in relazione alla categoria di dati trattata, i Garanti per la protezione dei dati personali dei *Land* tedeschi sono intervenuti per meglio specificare le misure ritenute adeguate, con particolare riferimento ai dati biometrici. Tra queste rientra la conservazione dei dati in un sistema non centralizzato, possibilmente in una carta in possesso del lavoratore, e l'utilizzo di tecnologie che permettono di tracciare il percorso di raccolta e trattamento dei dati personali⁴⁶.

6. LE CONDIZIONI DI LEGITTIMITÀ NELLA LEGISLAZIONE TEDESCA: L'ALTERNATIVITÀ TRA CONSENSO E CONTRATTO COLLETTIVO.

Come accennato poc'anzi, il par. 26 definisce le basi giuridiche per il trattamento delle categorie particolari di dati dei lavoratori. Al primo periodo della norma è riportato letteralmente il dettato normativo dell'art. 9 comma 2 lett. b) del Regolamento, con cui si stabilisce che il trattamento è consentito per l'adempimento di un obbligo o per l'esercizio di un diritto contenuto in una disposizione giuslavoristica nazionale o dell'Unione⁴⁷. Secondo i primi indirizzi giurisprudenziali in materia⁴⁸, non è necessario che il legislatore preveda norme unicamente riferibili alla categoria particolare di dati per poter legittimare il trattamento, essendo sufficienti le norme generali presenti nell'ordinamento. Il vaglio riguardante la necessità del trattamento per l'assolvimento degli obblighi imposti per legge dovrà essere compiuto quindi dal titolare e, eventualmente, dal giudice in sede di giudizio.

Il trattamento è considerato altresì legittimo quando basato sul

Maßnahmen oder 10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen ».

⁴⁵ E. M. FRENZEL, art. 9 dsGvo, in B. P. Paal, D. A. Pauly (a cura di), *Datenschutz Grundverordnung Bundesdatenschutzgesetz*, Frankfurt am Main, 2021, 167.

⁴⁶ DATENSCHUTZKONFERENZ, *Positionspapier zur biometrischen Analyse*, in *Orientierungshilfe* 2019, 2019, 27.

⁴⁷ Bundesdatenschutzgesetz, par. 26, 3° co.: « Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig,

wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt ». In conformità con quanto previsto dal Regolamento, è previsto che l'interessato sia informato della finalità del trattamento e del diritto di revoca garantogli ex art. 7 co. 3 del Regolamento n. 2016/679. Par. 26, 2° co. ultima parte: « Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 679/2016 in Textform aufzuklären ».

⁴⁸ LAG Berlin-Brandenburg, 4 giugno 2020, in *Neue Zeitung für Arbeitsrecht*, 2021, 86 ss.

consenso libero, volontario ed espresso del lavoratore ⁴⁹. Tuttavia, secondo i Garanti tedeschi, questo può fungere da base legittimante il trattamento dei dati biometrici solo nel caso in cui il datore abbia prima proposto all'interessato di utilizzare altri strumenti, quali *chip card*, codice PIN o *password* per il suo riconoscimento ed egli abbia preferito ricorrere a sistemi di rilevamento biometrico ⁵⁰.

Soddisfare i requisiti del consenso posti dalla legge e dal Regolamento si rivela complesso ai fini dell'utilizzo di dati biometrici ⁵¹. La possibilità di revoca senza alcun giustificato motivo costringe il datore a ricercare un'altra base legittima ovvero a modificare la tipologia di trattamento all'occorrenza ⁵². Inoltre, ai fini della determinazione della volontarietà, il titolare deve tenere conto del grado di dipendenza del lavoratore ⁵³ e delle circostanze in cui è stato prestato ⁵⁴. Per queste ragioni, il consenso viene generalmente richiesto all'interessato in via eccezionale ⁵⁵.

Più agevole risulta, quindi, ricorrere alla stipulazione di un contratto collettivo aziendale con il comitato d'azienda (*Betriebsrat*) ⁵⁶, come previsto dal par. 26 comma 4 *BDSG* ⁵⁷. Con riguardo al trattamento dei dati biometrici, la giurisprudenza di

⁴⁹ *Bundesdatenschutzgesetz*, par. 26, 3° co.: « Absatz 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen ».

⁵⁰ DATENSCHUTZKONFERENZ, *Positionspapier zur biometrischen Analyse*, cit., 27.

⁵¹ S. SCHINDLER, T. GOEBLE, J. SCHNEIDER, *Die Vermessung des Arbeitnehmers*, in D.A.C.H. Security, 2018, 258.

⁵² W. DÄUBLER, *Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses*, in W. Däubler, P. Wedde, T. Weichert, I. Sommer (a cura di), *EU-Datenschutz-Grundverordnung und BDSG-neu*, Frankfurt am Main, 2018, 1078.

⁵³ Come specificato in BUNDESTAG, *Bundestag Drucksache 16/13657 - Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss)*, in *Deutscher Bundestag Wahlperiode*, n. 19, 2009, secondo il legislatore tedesco l'interessato si ritroverebbe in uno stato di maggiore costrizione durante le trattative di stipulazione del contratto, rispetto alle altre fasi successive del rapporto di lavoro.

⁵⁴ *Bundesdatenschutzgesetz*, par. 26, 3° co.: « Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen ». La vo-

lontarietà del consenso non viene però aprioristicamente esclusa dal dettato normativo, nel caso in cui un vantaggio economico o giuridico possa derivare per il lavoratore dal trattamento dei suoi dati. *Bundesdatenschutzgesetz*, par. 26, 2° co., secondo periodo: « Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen ».

⁵⁵ A titolo esemplificativo, si richiama la finalità di accesso ai sistemi informatici tramite rilevamento dell'impronta digitale del lavoratore qualificato. Per maggiori approfondimenti, si veda W. DÄUBLER, *Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses*, cit., 1075.

⁵⁶ Il comitato d'azienda assume un ruolo fondamentale nella gestione aziendale, perché gran parte delle scelte datoriali riguardanti l'organizzazione e la gestione del personale deve essere sottoposta a sua consultazione e approvazione. Il potere di codeterminazione (*Mitbestimmung*) è disciplinato ai sensi del par. 87 *Betriebsverfassungsgesetz*. Si veda A. JUNKER, *Grundkurs Arbeitsrecht*, Frankfurt am Main, 2013, 815. Come approfondito da R. WALTERMANN, *Arbeitsrecht*, München, 2021, 340, l'elenco degli ambiti per i quali il comitato deve essere consultato ex par. 87 è tassativo.

⁵⁷ *Bundesdatenschutzgesetz*, par. 26, 4° co.: « Die Verarbeitung personenbezogener

merito ha riconosciuto ampia centralità alla contrattazione collettiva. In particolare, il comitato deve essere consultato anche nei casi in cui il datore di lavoro richiede ai dipendenti di sottoporsi al controllo biometrico degli accessi istituito presso la sede di un cliente ⁵⁸.

Dunque, poiché il comitato ha maggior potere contrattuale rispetto ai singoli lavoratori ⁵⁹, gli accordi collettivi sono considerati la base legittima principale per il trattamento dei dati biometrici del personale, mentre il consenso individuale viene relegato ad ipotesi alternativa e, soprattutto, residuale.

7. UN DIFFICILE PUNTO DI INCONTRO TRA I DUE QUADRI NORMATIVI.

La compiuta disamina rende evidente il differente approccio alla materia da parte dei due sistemi normativi. Nell'ordinamento tedesco la conformità del consenso prestato dal lavoratore ai principi regolamentari costituisce da sempre uno dei più controversi problemi affrontati dalla dottrina ⁶⁰. Ciononostante, il legislatore nazionale lo riconosce tra le basi giuridiche che legittimano il trattamento di dati biometrici. Secondo la dottrina maggioritaria, il consenso rappresenta la principale forma di esercizio del proprio diritto all'autodeterminazione informativa (*informationelle Selbstbestimmung*), inteso come il diritto a determinare autonomamente le modalità di utilizzo dei propri dati personali ⁶¹. Tale è stata la *ratio* che ha portato il legislatore a prevedere condizioni più stringenti per la sua validità nei contesti lavorativi ⁶². È opinione diffusa in Italia, invece, che il consenso del lavoratore non può considerarsi scevro da costrizioni, a causa della sussistenza del rapporto di dipendenza con il datore ⁶³.

Entrambi i sistemi normativi italiano e tedesco riconoscono tuttavia il potere alle rappresentanze aziendali di stabilire insieme

ner Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten ».

⁵⁸ BAG, 27 gennaio 2004, in *Neue Zeitschrift für Arbeitsrecht*, 2004, 556 ss.

⁵⁹ I. SCHMIDT, *Mitbestimmungsrechte*, in K. Fitting, G. Engels, I. Schmidt, Y. Trebinger, W. Linsenmaier (a cura di) *Betriebsverfassungsgesetz mit Wahlordnung*, München, 2016, 1393.

⁶⁰ M. SCHMIDT, *Datenschutz für "Beschäftigte": Grund und Grenzen bereichsspezifischer Regelung*, Baden, 2016, 298.

⁶¹ Ibidem.

⁶² Ibidem.

⁶³ A. LEVI, *Il controllo informatico sull'attività del lavoratore*, Torino, 2013, 144; M. SOFFIENTINI, *Sistema di videosorveglianza in azienda: progettazione ed errori comuni da evitare*, in *Diritto e Pratica del Lavoro*, n. 5, 2023, 323; GARANTE PRIVACY, provvedimento del 13 febbraio 2020 (doc. web n. 9285411); GARANTE PRIVACY, provvedimento del 13 dicembre 2018 (doc. web n. 9068983).

al datore le modalità di trattamento⁶⁴. Il coinvolgimento dei lavoratori mediante le proprie rappresentanze permette, infatti, di contrastare i possibili pericoli derivanti dalla sorveglianza generalizzata in azienda⁶⁵. La principale differenza tra i due ordinamenti si fonda quindi sul livello di coinvolgimento: in Germania la giurisprudenza è uniforme nel sostenere che il potere di codeterminazione debba essere esercitato ogni qualvolta si proceda all'introduzione di dispositivi tecnologici o *software* in azienda⁶⁶. In Italia, invece, l'accordo sindacale è richiesto *ex lege* solo nei casi di potenziale monitoraggio dell'attività lavorativa, con espressa esclusione degli strumenti di lavoro e di controllo degli accessi e delle presenze. Al momento, il legislatore italiano non ha inteso dedicare una disciplina specifica per il trattamento dei dati biometrici, confermando così il ridimensionamento del ruolo delle RSA in materia di protezione dei dati personali. Di conseguenza, mentre in Germania la disciplina ha raggiunto un certo grado di stabilità e di certezza giuridica, in Italia molti punti rimangono ancora aperti.

8. CONSIDERAZIONI CONCLUSIVE.

L'analisi svolta evidenzia il differente approccio alla materia da parte degli ordinamenti italiano e tedesco. L'evoluzione del diritto alla protezione dei dati personali avvenuta a livello europeo ha certamente inciso in entrambi i sistemi normativi, prevedendo misure di sicurezza più elevate, la responsabilizzazione dei titolari e la necessità di una precisa regolamentazione a livello nazionale che vada oltre gli strumenti di *soft law*. Ciò, tuttavia, non ha condotto i due ordinamenti ad un approccio comune, fondato su uguali condizioni di trattamento dei dati dei lavoratori. Al contrario, si denota ancora oggi una forte identità nazionale sul piano della normativa giuslavoristica.

Nell'attuale scenario normativo emergono dunque alcune questioni ancora aperte: nell'ordinamento italiano, l'interpretazione restrittiva delle disposizioni del Regolamento da parte del Garante per la protezione dei dati personali impedirebbe il trattamento dei dati biometrici in tutti i casi, con l'eccezione della sicurezza sul lavoro in quanto prevista dall'Autorizzazione Generale 1/2016. Come si è potuto notare, invece, il par. 26 *BDSG* individua le basi di legittimità negli obblighi previsti dalla legge, nel consenso e nell'accordo collettivo, senza porre limitazioni con

⁶⁴ BAG, 27 gennaio 2004, cit., 556.

⁶⁵ R. KRAUSE, *The protection of employees' right to privacy: the German legal system*, in C. Pisani, G. Proia, A. Topo (a cura di), *Privacy e lavoro: la circolazione*

dei dati personali e i controlli nel rapporto di lavoro, Milano, 2022, 250.

⁶⁶ BAG, 23 ottobre 2018, in *Zeitschrift für Datenschutz*, 2019, 131 ss.

riguardo alla finalità perseguibile con il trattamento. Un tale modello potrebbe risultare applicabile anche nell'ordinamento italiano. Per quanto concerne la base giuridica fondata su una norma di legge, ad opinione di chi scrive, si potrebbe considerare come soluzione l'interpretazione estensiva dell'art. 9 comma 2 lett. b) e dell'art. 2-septies del Codice Privacy. Tali norme, infatti, non impongono al legislatore di intervenire per determinare le finalità per le quali il trattamento dei dati biometrici si rende necessario. Al contrario, sanciscono che ove il diritto del lavoro preveda un obbligo da adempiere o un diritto da esercitare, si possa procedere con il trattamento delle categorie particolari di dati. Il giudizio riguardante la necessità dell'utilizzo dei dati biometrici rispetto alla finalità perseguita non verrebbe previsto da una disposizione normativa, bensì verrebbe demandato al datore di lavoro. Seguendo questo indirizzo, non sarebbe quindi necessario l'intervento mirato del legislatore.

Per ciò che concerne la ricerca del consenso del lavoratore, tale base legittima potrebbe rivelarsi onerosa per il titolare: da un lato, la sua revocabilità rende il trattamento dei dati biometrici temporaneo ed incerto; dall'altro, come nel modello tedesco, il datore dovrebbe sempre dimostrare la volontarietà del consenso prestato.

Infine, l'accordo aziendale potrebbe essere richiesto solo per individuare caso per caso le misure tecniche ed organizzative a protezione dei dati personali. La soluzione prospettata permetterebbe quindi il trattamento dei dati biometrici solo all'avverarsi di specifiche condizioni stabilite dalla contrattazione collettiva, limitandone così l'uso diffuso e garantendo maggiore protezione alla sfera personale del lavoratore.

Abstract

The paper focuses on the development of the Italian and German regulatory systems concerning the processing of biometric data in the workplace. In particular, it refers to the ways in which the national laws have specified the European regulations: from the different conception of the worker's consent as a legal basis for the processing of particular data to the different role played by company representatives through collective bargaining. The study, therefore, proposes to analyse how the Member States, in this case, Italy and Germany, have made use of the autonomy recognised by supranational legislation. The comparison between the two legal systems leads to an attempt to formulate a possible balancing act between the right to the protection of workers' biometric data and the employer's interest in their processing.