



Laura Greco - Alessandro Mantelero

**INDUSTRIA 4.0, ROBOTICA E
*PRIVACY-BY-DESIGN***

Estratto



GIUFFRÈ FRANCIS LEFEBVRE

LAURA GRECO - ALESSANDRO MANTELERO

INDUSTRIA 4.0, ROBOTICA E *PRIVACY-BY-DESIGN*

SOMMARIO: 1. Il contesto applicativo dell'Industria 4.0: interazione uomo-macchina e trattamento dei dati personali. — 2. Gli scenari applicativi dell'interazione uomo-macchina. — 2.1. (*Segue*): dati biometrici. — 2.1.1. (*Segue*): esoscheletri robotici. — 2.1.2. (*Segue*): postazioni di lavoro auto-adattive. — 2.2. (*Segue*): dati geo-referenziati e *smart suit*. — 2.3. (*Segue*): dati relativi alla voce. — 2.3.1. (*Segue*): sistemi di identificazione vocale. — 2.3.2. (*Segue*): Comandi vocali indirizzati a robot o AGV. — 3. Conclusioni.

1. IL CONTESTO APPLICATIVO DELL'INDUSTRIA 4.0: INTERAZIONE UOMO-MACCHINA E TRATTAMENTO DEI DATI PERSONALI.

L'avvento del nuovo Reg. (UE) 2016/679 in materia di trattamento dei dati personali, meglio noto con l'acronimo in lingua inglese GDPR ¹, ha comportato per molti aspetti un mutamento nell'approccio alla gestione dei dati personali ². Il Regolamento, a partire dal 25 maggio 2018, ha preso il posto delle disposizioni nazionali di attuazione della direttiva 95/46/CE ³, che nell'ultimo ventennio ha costituito la normativa di riferimento in materia di

* Il presente contributo è stato elaborato sulla base dei risultati del progetto di ricerca HuManS (Project - Human centered Manufacturing Systems), condotto presso il Politecnico di Torino e finanziato nell'ambito del programma "Smart Factory" della Regione Piemonte con fondi EU European Regional Development Fund 2014/2020. Alessandro Mantelero, professore associato presso il Politecnico di Torino, ha coordinato il disegno della ricerca e l'analisi degli scenari applicativi; Laura Greco, assegnista di ricerca presso il Politecnico di Torino, ha sviluppato l'analisi normativa e giurisprudenziale ed ha concorso allo studio degli scenari applicativi. Ai fini dei processi di valutazione dei prodotti di ricerca, il presente contributo è quindi da attribuirsi in maniera paritetica ad entrambi gli autori.

L'elaborazione del presente contributo è stata parzialmente finanziata dal Ministero dell'Istruzione, dell'Università e della Ricerca ("TESUN-83486178370409 finanziamento dipartimenti di eccellenza CAP. 1694 TIT. 232 ART. 6").

¹ 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.

² Per un'analisi dettagliata del nuovo testo normativo, cfr. G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017.

³ La lunga gestazione del Regolamento (UE) 2016/679 e la difficoltà a trovare una generale convergenza su alcuni dei molti

protezione dei dati personali consentendo all'Unione europea di assumere una posizione di *leadership* globale in questo ambito.

Seppur necessariamente nel solco della previgente normativa comunitaria, il Regolamento apporta un significativo mutamento di prospettiva che sposta il *focus* normativo sulla gestione del rischio e sulla responsabilità, anche in termini di capacità di provare l'efficacia delle soluzioni adottate a tutela dei diritti degli interessati (*accountability*).

Il Regolamento, dunque, innova la disciplina in materia di protezione dei dati personali mirando a tutelare i soggetti interessati in una fase prodromica al trattamento. Nello specifico, il legislatore europeo enfatizza il ruolo della valutazione *ex ante* dei rischi che possono emergere dall'uso di informazioni personali ed accentua le responsabilità degli autori del trattamento (titolare e responsabile del trattamento) rispetto all'adozione delle soluzioni tecniche, logiche e organizzative necessarie ad evitare eventuali situazioni di rischio ⁴.

Progettazione del trattamento *by design*, registro delle attività di trattamento, valutazione d'impatto, consultazione preventiva, adozione di misure di sicurezza proporzionate al rischio, comunicazione dei *data breach*, sono alcuni dei principali adempimenti — nuovi e non — volti a blindare il dato personale entro la cinta di un modello di protezione preminentemente proattivo.

L'impatto di tale mutamento di prospettiva emerge ovviamente in maniera più significativa laddove gli elementi di rischio sono più rilevanti, in ragione della natura degli interessi in gioco, dei dati elaborati e delle modalità di trattamento. Da qui l'importanza di condurre un'analisi delle implicazioni della nuova normativa sullo sviluppo delle soluzioni proprie della c.d. Industria 4.0.

A tal proposito occorre chiarire come la nozione di Industria 4.0 (anche individuata con il termine *smart factory*) costituisca una sorta di categoria-contenitore volta a riassumere un nuovo stadio dello sviluppo delle modalità di produzione industriale, verso il quale stanno evolvendo le imprese. Tale cambiamento si può riassumere nella messa a sistema dei mutamenti di paradigma del settore ICT avvenuti nell'ultima decade (cloud computing, IoT, Big Data, Machine Learning, Artificial Intelligence) e nella loro applicazione nei contesti di produzione e logistici. Questo ha consentito di ripensare la struttura produttiva arricchendola di

aspetti oggetto dello stesso hanno tuttavia indotto il legislatore europeo a lasciare alcuni margini di manovra ai legislatori nazionali, cui diverse norme fanno rinvio. Sulla base di tali disposizioni e, in taluni casi, mossi dall'intento di ampliare le tutele fornite dal Regolamento i diversi legislatori

nazionali hanno adottato o stanno per adottare provvedimenti integrativi *ad hoc*. Cfr. in tal senso il recente d. lgs. 10 agosto 2018, n. 101 che ha modificato il d. lgs. 196/2003.

⁴ Cfr. volendo A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove Leggi Civ. Comm.*, 2017, I, 144 ss.

contenuti informativi inerenti all'interazione uomo-uomo, uomo-macchina e macchina-macchina. Queste informazioni hanno così permesso di avere conoscenza sia in tempo reale sia predittiva della produzione industriale e delle varie attività che si svolgono all'interno del contesto di fabbrica e delle strutture logistiche.

È di tutta evidenza come la mole di dati raccolti all'interno dell'ambiente dalla *smart factory* implichi anche il trattamento di informazioni inerenti ai soggetti che in tale ambiente svolgono la propria attività lavorativa, comportando quindi forme di trattamento di dati personali. Forme che si connotano non solo per la quantità dei dati trattati o per la natura predittiva delle inferenze desumibili ⁵, ma anche e soprattutto per le modalità innovative in cui le informazioni divengono parte di un più complesso ecosistema di fabbrica connotato dall'interazione uomo-macchina.

A tale interazione guarda il presente contributo, che lascia volutamente in secondo piano le istanze più propriamente giuslaburistiche per incentrarsi invece sull'impatto del Regolamento (UE) 2016/679 e sulla cifra che lo contraddistingue, riassumibile nei processi di analisi del rischio e di progettazione *data protection by design* ⁶.

Proprio questo *continuum* fra analisi del rischio e progettazione orientata alla tutela dei diritti viene enfatizzato nel Regolamento e assume notevole rilevanza nel disegnare in nuovi ambienti delle *smart factories*. L'approccio prettamente ingegneristico volto all'efficienza dei sistemi deve, infatti, necessariamente coniugarsi con il rispetto dei diritti e delle libertà fondamentali ⁷ dei soggetti che in tali sistemi sono chiamati ad operare ⁸, specie laddove tali ambienti siano incentrati proprio sulla componente umana, come ad esempio nel caso del progetto HuManS (Project - Human centered Manufacturing Systems), che ha consentito lo sviluppo della presente ricerca.

A tal riguardo, va osservato come la natura prevalentemente empirica di questo studio costituisca la modalità necessaria per poter affrontare il tema in esame. Sia l'analisi del rischio sia le soluzioni *by design*, che di tale analisi rappresentano l'applicazione concreta, non costituiscono infatti temi di cui è necessaria una particolare elaborazione teorica, quanto piuttosto aspetti di

⁵ Cfr. volendo A. MANTELERO, *Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection*, in *Computer Law and Security Review*, 2016, 32 (2), 238 ss.

⁶ Non sono invece oggetto della presente analisi gli aspetti inerenti alla base giuridica del trattamento dati nei diversi contesti esaminati.

⁷ Cfr. anche l'intervento di Antonello Soro al convegno "Uomo e macchine. Protezione dei dati per un'etica digitale" del 30 gennaio 2018, qui reperibile *on line* <https://www.garanteprivacy.it/en/home/docweb/-/docweb-display/docweb/7598686>.

⁸ Cfr. art. 1, par. 2, Reg. (UE) 2016/679.

cui si avverte la necessità di una più chiara e puntuale definizione delle modalità applicative concrete.

Certamente residuano ampi spazi per l'elaborazione di nuove e più complete forme di *risk assessment*, che guardano oltre i (limitati) confini del Regolamento (UE) 2016/679⁹; tuttavia, rimanendo nel perimetro di analisi del rischio delineato dalle autorità garanti europee, la sfida maggiore consiste nel contestualizzare il quadro regolatorio e teorico esistente¹⁰. In questo senso il presente scritto vuole offrire un contributo concreto al dibattito, guardando agli scenari applicativi di quelle tecnologie proprie della Industria 4.0 che maggiormente possono avere un impatto sull'impiego dei dati personali.

Se, come si è accennato, la gestione integrata delle informazioni si trova al centro del nuovo ecosistema tecnologico dell'Industria 4.0, l'informazione — che oggi rivive sotto forma di nuova ricchezza e merce di scambio¹¹ — diviene in concreto il motore che muove la *smart factory*, ossia il nuovo modello di *manufacturing* digitale e interconnesso.

Nello specifico, l'informatizzazione dell'interazione uomo-macchina attraverso l'introduzione dei moderni modelli di robot collaborativi ha creato una maggior simbiosi fra le due componenti di tale binomio, non solo chiamate a condividere lo stesso

⁹ Per un approfondimento a riguardo, si rinvia ad A. MANTELERO, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Computer Law & Security Review*, 2018, 34 (4), 754 ss.

¹⁰ In questo senso, le Autorità per la protezione dei dati europee e internazionali hanno emanato talune linee strategiche, nel corso della quarantesima conferenza internazionale (*The International Conference of Data Protection and Privacy Commissioners* - ICDPPC) dal titolo "Debating Ethics: Respect and Dignity in Data Driven Life" che si è tenuta a Bruxelles dal 22 al 26 ottobre scorso. In particolare, nel corso dell'incontro è stata approvata la "Dichiarazione su etica e protezione dei dati nell'intelligenza artificiale" (qui consultabile: https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf) ove sono stati definiti sei principi cardine, a tutela dei diritti fondamentali e della dignità della persona, che dovrebbero essere rispettati da ogni soggetto coinvolto nello sviluppo o nell'utilizzo di sistemi di intelligenza artificiale. Tra questi principi sono stati inclusi i principi di *privacy-by-design* e di *privacy-by-default*, ritenuti essenziali ai fini di una "progettazione responsabile".

¹¹ L'informazione è oggi considerata un bene giuridico suscettibile di valutazione economica ex art. 810 c.c. Sul valore economico e commerciale dell'informazione, cfr. RESTA, *Autonomia privata e diritti della personalità*, Napoli, Jovene, 2005; V. ZENO-ZENCOVICH, *Una lettura comparatistica della L. n. 675/96 sul trattamento dei dati personali*, in *Riv. trim. dir. proc. civ.*, 1998, pp. 740-741. Anche sul fronte giurisprudenziale è ormai pacifica la valutazione economica dell'informazione, come emerge anche da alcune decisioni della Corte di Giustizia europea, cfr. le sentenze Corte Giustizia UE, 13 maggio 2014, C 131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González e Corte di Giustizia dell'Unione europea, 6 ottobre 2015, C-362/14, Maximilian Schrems v Data Protection Commissioner, Digital Rights Ireland Ltd., su cui cfr. anche G. RESTA e V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma, 2016; G. RESTA e V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015; GIUSELLA FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in questa Rivista, 2015, 779 ss.

spazio di lavoro, ma finanche ad integrarsi fisicamente e meccanicamente. In questo senso proprio l'impiego di sensori biometrici e di esoscheletri robotici¹² costituisce uno degli aspetti più innovativi delle soluzioni delineate nell'Industria 4.0, oggetto dell'analisi svolta nelle pagine che seguono.

L'interazione uomo-macchina, al pari delle interazioni macchina-macchina (anch'esse connotanti l'Industria 4.0), si basa e si alimenta di informazioni, che sono relative al contesto di lavoro, all'attività da svolgere, nonché all'operatore con cui la macchina è chiamata ad interagire. Sono questi dati essenziali che vanno raccolti e trattati non solo nella fase operativa concernente il funzionamento della macchina, ma già tenuti adeguatamente in conto nella progettazione stessa del *device*.

La centralità della componente informativa, unita alla lata nozione di dato personale propria della legislazione europea¹³, comportano un'ampiezza delle potenziali ricadute operative del Regolamento (UE) 2016/679 sulle tecnologie proprie dell'Industria 4.0 a cui, in un prossimo futuro, si aggiungeranno anche

¹² Gli esoscheletri sono strutture elettromeccaniche esterne in grado di potenziare o compensare le capacità fisiche dell'utilizzatore, di cui rivestono parti del corpo supportandone i movimenti.

¹³ Cfr. art. 4, par. 1, Reg. (UE) 2016/679. Cfr. anche a riguardo GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 4/2007 sul concetto di dati personali*, adottato il 20 giugno 2007, consultabile *on line* all'indirizzo <<http://194.242.234.211/documents/10160/10704/ARTICOLO+29+-+WP+136.pdf>>. Nello specifico, il collegamento fra informazione e persona è stato interpretato a livello di normativa europea e nazionale in maniera estensiva, tale da non richiedere che il dato debba riguardare direttamente la persona fisica. Quando, ad esempio, vengono raccolti dati di processo per finalità organizzative e produttive ovvero per la sicurezza sul lavoro ed il trattamento è comunque idoneo a rivelare informazioni sullo stato o sul comportamento di una persona, tali dati devono considerarsi "concernenti" la persona. Un esempio in tal senso è dato dai sistemi di geolocalizzazione installati con finalità logistiche o di ottimizzazione dei servizi: frequentemente, infatti, nell'ambito di servizi che prevedono l'impiego di veicoli come attività di trasporto di persone o cose, vengono installati a bordo sistemi di localizzazione e di comunicazione (anche in tempo reale) ai fini menzionati. L'impiego di tali sistemi comporta inevita-

bilmente la possibilità di localizzare la posizione dei lavoratori assegnatari dei veicoli medesimi, potendo pertanto concludere che i dati relativi all'ubicazione dei veicoli, in quanto (direttamente o indirettamente) associati ai lavoratori, costituiscono anche informazioni personali riferibili a questi ultimi. Cfr., e.g., GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, provvedimento del 4 ottobre 2011, doc web n. 1850581, consultabile *on line* al sito <<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1850581>>. A ciò si aggiunga che l'evoluzione delle tecnologie di analisi dei dati (Big Data) ha sostanzialmente minato la possibilità di disegnare sistemi informativi incentrati su dati anonimi, essendo sempre più elevata la possibilità di re-identificazione, cfr., *ex multis*, A. NARAYANAN, J. HUEY, E. W. FELTEN, *A Precautionary Approach to Big Data Privacy*, in S. GUTWIRTH, R. LEENES, P. DE HERT (a cura di), *Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection*, Dordrecht, Springer, 2016, 357 ss.; Y-A. DE MONTJOYE, L. RADAELLI, V. KUMAR SINGH, A. « SANDY » PENTLAND, *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, in Science, 2015, 347(6221), 536 ss.; P. OHM, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, in UCLA L. Rev., 2010, 57, 1701 ss.; UNITED STATES GENERAL ACCOUNTING OFFICE, *Record*

quelle derivanti dall'adozione del Regolamento sui flussi di dati non personali¹⁴.

Con riguardo alla tipologia dei dati trattati nel contesto della *smart factory*, va tenuto in considerazione come l'impiego di sensori atti a monitorare la condizione di lavoro del dipendente o la realizzazione di dispositivi calibrati sulle componenti biometriche dell'individuo¹⁵ comportino una particolare attenzione per il trattamento di informazioni che ricadono nelle c.d. categorie particolari di dati personali di cui all'art. 9 del Regolamento (UE) 2016/679.

Analogamente ad ogni trattamento di dati personali, anche l'utilizzo dei dati in ambito industriale soggiace ai principi fondamentali in materia di trattamento. In questo contesto, oltre ai ben noti principi di liceità, finalità e necessità, assumono particolare rilevanza i principi di proporzionalità, minimizzazione e conservazione, posto che proprio a tal riguardo il precetto normativo solitamente si scontra con un'idea di efficienza ingegneristica che vede nella natura estensiva della raccolta, sia in termini quantitativi sia temporali, un pregio piuttosto che una criticità.

In contrasto con questa propensione, il principio di proporzionalità impone invece di verificare se il trattamento, unitamente alle modalità ed ai mezzi con cui viene effettuato, sia proporzionato rispetto alle finalità da perseguire. Al fine di tale valutazione,

Linkage and Privacy. Issues in creating New Federal Research and Statistical Information, 2011, 68 ss., consultabile al seguente indirizzo: <<http://www.gao.gov/assets/210/201699.pdf>>; P. GOLLE, *Revisiting the uniqueness of simple demographics in the US population*, in A. JUELS (a cura di), *Proc. 5th ACM workshop on Privacy in electronic society*, New York, ACM, 2006, 77 ss.; L. SWEENEY, *Simple Demographics Often Identify People Uniquely*, Carnegie Mellon University, 2000, consultabile al seguente indirizzo: <<http://dataprivacylab.org/projects/identifiability/paper1.pdf>>; L. SWEENEY, *Foundations of Privacy Protection from a Computer Science Perspective*, in *Proc. Joint Statistical Meeting, AAAS, Indianapolis*, 2000, consultabile al seguente indirizzo: <<http://dataprivacylab.org/projects/disclosurecontrol/paper1.pdf>>. Con riguardo alla dottrina italiana si veda: G. FINOCCHIARO (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, in F. GALGANO (diretto da), *Tratt. dir. comm. e dir. pubbl. ec.*, XLVIII, Padova, 2008. Cfr. anche a riguardo GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 4/2007 sul concetto di dati personali*, adottato il 20 giugno 2007, nonché Consiglio d'Europa, *Guidelines on the pro-*

tection of individuals with regard to the processing of personal data in a world of Big Data, 23 gennaio 2017 ("The controller should assess the risk of re-identification taking into account the time, effort or resources needed in light of the nature of the data, the context of their use, the available re-identification technologies and related costs").

¹⁴ Cfr. Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

¹⁵ Cfr. a riguardo anche art. 2-septies, d. lgs. 196/2003 così come riformato dal d.lgs. 101/2018. Con riferimento al quadro regolatorio elaborato sulla base del precedente testo del d.lgs. 196/2003, va ricordato il *Provvedimento generale prescrittivo in tema di biometria* emanato dal Garante per la protezione dei dati personali il 12 novembre 2014, nonché l'*Autorizzazione n. 8/2016 al trattamento dei dati genetici* del 15 dicembre 2016 rilasciata dalla stessa Autorità, che, recentemente, ha provveduto ad un riesame dell'autorizzazione ai fini dell'adeguamento alla normativa dettata dal Reg. (UE) 2016/679 e dal d. lgs. n. 101/2018. Cfr. Garante, provvedimento n. 957 del 13 dicembre 2018, doc. not. n. 9068972.

andranno tenuti in debito conto il contesto del trattamento, la natura dei dati trattati, i soggetti interessati, nonché l'eventuale esistenza e l'adottabilità di misure meno invasive rispetto ai diritti degli interessati.

Il diritto alla protezione dei dati personali non è infatti una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va temperato con altri diritti fondamentali. In tale contesto, il principio di proporzionalità si inserisce nell'istituto del c.d. bilanciamento degli interessi, che impone di soppesare le esigenze contrapposte e trovare il giusto equilibrio tra gli interessi in gioco.

Guardando alla realtà in esame, un eventuale bilanciamento di interessi potrebbe vedere contrapposti, da un lato, l'interesse del datore di lavoro che intende implementare tecnologie *human-robot based* fondate sull'utilizzo di dati biometrici dei lavoratori e, dall'altro, il diritto alla protezione dei dati personali dei dipendenti. Affinché l'uso di dispositivi progettati e funzionanti attraverso il trattamento di dati biometrici sia legittimo, occorrerà tuttavia che sussista una reale necessità del ricorso a tali soluzioni e che non sia possibile raggiungere i medesimi obiettivi utilizzando soluzioni meno invasive¹⁶.

Analogamente il principio di minimizzazione costituisce un ulteriore vincolo che dovrà essere considerato nello sviluppo delle soluzioni tecnologiche per l'Industria 4.0. Il trattamento dei dati personali dovrà infatti essere effettuato in modo tale da ridurre al minimo l'uso degli stessi, ricorrendo a soluzioni che non ne prevedano l'impiego o che utilizzino dati anonimi con un basso rischio di re-identificazione. Ne consegue che l'applicazione dei principi di *data protection by design*¹⁷ dovrà indurre ad un'attenta valutazione della reale necessità di adottare soluzioni incentrate sui dati personali, ove i medesimi risultati possono essere conseguiti in maniera differente. Un esempio in tale senso è dato dal caso degli esoscheletri impiegati nelle *smart factories*, rispetto ai quali un meditato *design* può ridurre l'impiego di dati biometrici, connotati da un potenziale alto impatto in termini di rischio, ai sensi dell'art. 35 del Regolamento (UE) 2016/679¹⁸.

Infine, è coerente con la medesima impostazione anche il principio di limitazione della conservazione dei dati, che contrasta con l'enfasi posta in molte pratiche aziendali sulla raccolta di lunga

¹⁶ Per un'esemplificazione concreta, cfr. *infra* §§ 2.1 ss.

¹⁷ Cfr. a riguardo G. D'ACQUISTO, M. NALDI, *Big Data e privacy by design. Anonimizzazione, Pseudonimizzazione, Sicurezza*, Torino, 2017.

¹⁸ Tale casistica è più dettagliatamente analizzata *infra* § 2.1.1. Cfr. anche

EUROPEAN DATA PROTECTION BOARD, *Opinion 12/2018 on the draft list of the competent supervisory authority of Italy regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)*, adottata il 25 settembre 2018.

durata e su ampia scala dei dati, anche laddove poi concretamente tali informazioni vengano scarsamente utilizzate. Il principio secondo cui i dati personali non devono essere conservati per un periodo di tempo superiore a quello necessario al perseguimento delle finalità per i quali sono stati raccolti o successivamente trattati, non solo garantisce una migliore tutela dei diritti degli interessati, ma diventa anche un fattore tale da indurre ad una più attenta valutazione del concreto impiego delle informazioni in azienda e dell'utilità delle stesse, comportando potenziali vantaggi non solo in termini di conformità alla disciplina in materia di trattamento dati ma anche di efficienza organizzativa e risparmi di costi di gestione ¹⁹.

2. GLI SCENARI APPLICATIVI DELL'INTERAZIONE UOMO-MACCHINA.

L'interazione uomo-macchina calata nella realtà aziendale può generare una serie di scenari applicativi distinti in ragione del diverso grado di incisività sul trattamento dati e delle diverse esigenze che le aziende possono trovarsi a fronteggiare. In particolare, verranno qui esaminate alcune soluzioni innovative attualmente allo studio in fase sperimentale o di prima implementazione, ma destinate ad avere nel breve periodo un'ampia diffusione, in quanto basate su tecnologie già mature e disponibili allo stato dell'arte.

Obiettivo dell'indagine è dunque l'individuazione delle soluzioni operative compatibili con la normativa in materia di *data protection*, prendendo in considerazione le diverse esigenze aziendali che potrebbero talvolta giustificare il trattamento di dati identificativi e che talaltra potrebbero essere compatibili con approcci maggiormente *privacy oriented*. Sempre in considerazione dei casi specifici sono state delineate diverse soluzioni in termini di anonimizzazione dei dati, conservazione degli stessi, architettura dei *database* e tempi di *data retention*.

Nell'affrontare gli scenari che verranno esposti di seguito emerge dunque il chiaro intento di elaborare soluzioni operative concrete che pongano in essere il necessario bilanciamento fra la funzionalità nell'interazione uomo-macchina e l'esigenza di porre dei limiti a tutela degli operatori e del loro diritto alla protezione dei dati personali.

¹⁹ Con riferimento al legame fra conformità alla normativa in materia di trattamento dei dati personali e costi, sia consentito rinviare ad A. MANTELERO, *Il costo della privacy tra valore della persona e ragione*

d'impresa, Milano, 2007, che costituisce l'unico contributo di analisi empirica in ambito giuridico in materia con riferimento al contesto normativo nazionale.

2.1. (segue). *Dati biometrici.*

Numerose tecnologie dell'Industria 4.0 si fondano sul trattamento di dati biometrici, ossia quei dati personali "ottenuti da un trattamento tecnico specifico relativi 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"²⁰, secondo la definizione fornita dal Regolamento (UE) 2016/679, in linea con quella precedentemente elaborata dal Gruppo di lavoro Articolo 29 per la protezione dei dati, ripresa anche dal Garante per la protezione dei dati personali²¹.

Si tratta dunque di dati che, derivando dalle caratteristiche fisiche, fisiologiche o comportamentali dell'individuo²², hanno un profondo legame con il corpo e l'identità della persona a cui si riferiscono e, per tale ragione, vengono spesso impiegati nelle procedure di autenticazione e di riconoscimento, come ad esempio nel campo della *security* ai fini del controllo dell'accesso fisico e logico²³ ovvero anche con riferimento alla sottoscrizione di documenti informatici²⁴.

Tale tipologia di dati non va confusa con la diversa categoria dei dati relativi alla salute che, secondo la definizione contenuta nel GDPR, sono quei "dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute"²⁵.

In particolare, due sono i tratti peculiari e distintivi dei dati biometrici. In primo luogo, i dati biometrici non possono essere rilevati sulla base di una semplice raccolta dati, ma sono il frutto

²⁰ Cfr. art. 4, n. 14, Reg. (UE) 2016/679.

²¹ Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, adottato il 27 aprile 2012 ("proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità") e Garante per la protezione dei dati personali, *Linee Guida in materia di riconoscimento biometrico e firma grafometrica*, di cui all'allegato A del *Provvedimento generale prescrittivo in tema di biometria*, adottato il 12 novembre 2014.

²² A titolo esemplificativo, dalle caratteristiche fisiche è possibile ricavare i tratti biometrici che compongono l'impronta digitale, la forma dell'iride oppure la fisionomia

del volto; dalla considerazione delle caratteristiche biometriche comportamentali può invece evincersi la dinamica di apposizione della firma autografa, anch'essa da considerarsi, nel suo insieme, un dato biometrico.

²³ Tali tecniche, come ad esempio il riconoscimento facciale o l'impronta digitale, possono aggiungersi ovvero sostituire i comuni strumenti di autenticazione tramite identificativo e parola chiave (*user id e password*) oppure tramite dispositivi a varia tecnologia (tessere magnetiche, ottiche, dispositivi OTP ossia *one-time password*).

²⁴ Si pensi alla firma grafometrica ove i dati biometrici rilevati sono, ad esempio, la velocità di tracciamento, l'accelerazione del tratto, la pressione, l'inclinazione e così via. Per approfondimenti sulla qualificazione e sull'efficacia probatoria di tale firma, cfr. G. FINOCCHIARO, *La metafora e il diritto nella normativa sulla cosiddetta "firma grafometrica"*, in questa *Rivista*, 2013, 1 ss.

²⁵ Art. 4, n. 15, Reg. (UE) 2016/679.

di uno specifico processo tecnico volto ad estrapolare il dato biometrico a partire dalle caratteristiche del soggetto²⁶. In secondo luogo, i dati biometrici si riferiscono a caratteristiche uniche del soggetto e, pertanto, sono gli unici dati che consentono un'identificazione univoca della persona a cui si riferiscono.

Da quanto sopra discende che, qualora mediante un processo tecnico si generino informazioni che riguardano aspetti fisici, fisiologici o comportamentali dell'individuo, ma non idonee a identificare univocamente il soggetto, non si potrà parlare di dati biometrici. Così, a titolo esemplificativo, la semplice misurazione strumentale della circonferenza toracica di un soggetto, in quanto non idonea a consentirne l'identificazione univoca, non potrà essere considerata alla stregua di un dato biometrico. Questo non esclude che, tuttavia, il dato in questione (nell'esempio, la circonferenza toracica) possa avere carattere di dato personale ove, unito ad altre informazioni (ad esempio età, sesso, appartenenza ad un dato reparto aziendale), possa essere ricondotto ad un soggetto specifico²⁷, ovvero quando l'elevato livello di precisione della misurazione di una parte del corpo ne implichi l'univocità in termini di identificazione.

Considerata l'intima connessione dei dati biometrici con l'identità dell'individuo, la disciplina in materia di protezione dei dati personali tutela in modo più stringente l'impiego di tali dati, imponendo adempimenti e obblighi di protezione rigorosi e ulteriori rispetto a quelli previsti per il trattamento di semplici dati personali, sia a livello europeo che nazionale²⁸.

2.1.1. (segue). *Esoscheletri robotici.*

Il trattamento di dati biometrici è alla base delle soluzioni tecnologiche di robotica indossabile, quali gli esoscheletri per applicazioni industriali volti ad aumentare le capacità operative dei lavoratori che svolgono attività manuali e di movimentazione.

Tali strumenti vengono applicati direttamente al corpo dell'operatore e sono controllati dal movimento della persona²⁹. Hanno la finalità di sgravare l'operatore dai carichi lavorativi tipici del

²⁶ A titolo esemplificativo, il dato biometrico non è il volto di un individuo, quanto l'immagine del volto elaborata da un algoritmo di *face detection*.

²⁷ C. JASSERAND, *Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data*, in *Eur. Data Prot. L. Rev.*, 2016, 2, 311, specifica che "Contrary to 'generic' personal data, biometric data must relate to an identified individual. The other 'biometric data', i.e. those that relate to an identifiable individual, do not legally qualify as biometric data, but can still be

considered as personal data if they fulfil the other criteria applicable to personal data".

²⁸ Cfr. art. 9 Reg. (UE) 2016/679 e art. 2-septies d.lgs. 196/2003.

²⁹ Non sono qui presi in considerazione nel dettaglio i diversi tipi di esoscheletri dotati di automazione predittiva attualmente allo studio. Questi ultimi sono caratterizzati dalla capacità di predire alcuni movimenti dell'operatore, anticipandoli e facilitandoli. Rispetto a questa diversa tipologia di manufatti le criticità maggiori non riguardano tanto il trattamento dati, quanto

lavoro manuale sia per effetto dell'amplificazione della forza esercitata dalla persona, sia per effetto del supporto che l'esoscheletro è in grado di fornire agli arti nelle posture incongrue. Proprio al fine di garantire una migliore efficienza dell'integrazione fra struttura corporea e meccanica, lo sviluppo di tali prodotti può orientarsi verso esoscheletri personalizzati realizzati sulla base di informazioni biometriche riguardanti il soggetto che dovrà indossarli.

Attraverso sensori installati sugli esoscheletri è possibile poi un'ulteriore acquisizione di dati volti al controllo delle funzioni biologiche della persona che indossa il dispositivo, monitorando il suo stato di salute e il livello di affaticamento, compensandone progressivamente il calo di prestazioni in maniera da evitare possibili accumuli di fatica.

Tanto nella fase di progettazione quanto in quella di implementazione e utilizzo dell'esoscheletro possono quindi essere poste in essere attività di trattamento di dati biometrici inerenti all'operatore, oltre al trattamento di dati attinenti alle funzioni biologiche e pertanto potenzialmente relativi alla salute di quest'ultimo.

Onde applicare i menzionati principi di analisi del rischio e di *data protection by design* a questa implementazione delle soluzioni di *smart factory*, occorrerà quindi una più attenta analisi della casistica concreta a partire dalla fase di progettazione, che dovrà ispirarsi ai principi di cui all'art. 5 del Regolamento (UE) 2016/679. In tal modo, applicando i principi di finalità, necessità e proporzionalità, sarà possibile distinguere fra due differenti scenari, connotati da una diversa necessità di trattamento dei dati di natura biometrica.

È infatti tecnicamente possibile ricorrere alla realizzazione dell'esoscheletro sulla base di mere misure approssimative del corpo (o di parti di esso) onde creare un esoscheletro che sia non perfettamente aderente al fisico del singolo operatore, ma risulti variabile e adattabile grazie a componenti regolabili. Tale tipologia verrà di seguito indicata come "esoscheletro di Tipo A".

In un secondo diverso scenario, l'esoscheletro potrebbe invece essere realizzato sulla base di precisi rilevamenti e acquisizioni dei

piuttosto i rischi per l'utilizzatore in termini di sicurezza ed incolumità fisica. A tal proposito, manca altresì un definito quadro normativo riguardante la progettazione di tali esoscheletri, specie con riferimento alle modalità con cui condurre la fase di test e sperimentazione, volta ad escludere potenziali conseguenze in termini di mal funzionamento. Evidente è la necessità di realizzare delle commissioni *ad hoc* per la valutazione delle implicazioni etiche della sperimentazione e dell'impiego dei robot desti-

nati ad interagire con gli esseri umani. Cfr. a riguardo PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL))* e gli allegati Codice etico-deontologico degli ingegneri robotici e Codice per i Comitati Etici di Ricerca (CER), consultabili al seguente indirizzo: <<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//IT>>.

dati biometrici (*screening*) dell'operatore e sarà di seguito indicato come "esoscheletro di Tipo B". A differenza degli esoscheletri di Tipo A, che potrebbero comportare un certo margine di imperfezione nella compatibilità fra esoscheletro e caratteristiche fisiche dell'utilizzatore, l'impiego di immagini biometriche del corpo dell'utilizzatore o di parti di esso (con ricorso a tecniche di *body scan*) per realizzare il singolo esoscheletro consentirebbe di ottenere un manufatto in grado di adattarsi in maniera perfetta alle fattezze dello stesso.

Le due soluzioni differiscono in termini di trattamento dati. Mentre, infatti, nel Tipo A è necessario acquisire alcune misure corporee, che (come si vedrà in seguito) potrebbero anche consistere in dati anonimi, nel Tipo B si ha un rilevamento dei caratteri biometrici dell'individuo, di indubbio maggior impatto in termini di tutela dei dati personali, tanto più quanto maggiore sarà la superficie corporea o la sensibilità delle aree (e.g. volto) oggetto di scansione. Per queste ragioni, in linea con i principi in materia di trattamento dati, nella fase di studio delle soluzioni da adottarsi, occorrerà preliminarmente valutare se le finalità di ausilio agli operatori possano essere perseguite in maniera ugualmente soddisfacente mediante esoscheletri di Tipo A, piuttosto che ricorrendo al modello di Tipo B incentrato sul rilevamento biometrico.

In ragione della natura contestuale della *data protection*, la scelta dell'una o dell'altra soluzione dipenderà dalle esigenze e dalle finalità perseguite in concreto e richiederà, dunque, un bilanciamento degli interessi onde valutare la necessità e la proporzionalità del trattamento di dati biometrici. Questa valutazione non si ridurrà alla mera alternativa fra Tipo A e Tipo B, ma, una volta scelta l'opzione coerente con il quadro normativo, richiederà anche per ciascuna di esse un'analisi delle diverse fasi di trattamento dati. Ovviamente queste ultime saranno maggiormente presenti e rilevanti nel contesto della realizzazione di esoscheletri di Tipo B, riguardo, ad esempio, all'ampiezza della superficie corporea oggetto di scansione, alle modalità di archiviazione dei dati e alla durata del trattamento³⁰.

Qualora, a seguito del bilanciamento di interessi, l'adozione di un esoscheletro perfettamente aderente al profilo corporeo dell'operatore (Tipo B) non risulti necessaria in relazione alle caratteristiche dell'attività da svolgersi con l'ausilio dell'esoscheletro ovvero dell'ambiente lavorativo (e.g. elevata entità dei carichi portati, tali da richiedere una perfetta aderenza fra esoscheletro

³⁰ In termini generali, conformemente al principio di minimizzazione del trattamento dei dati personali, il sistema di rilevazione dovrà sempre essere configurato in modo tale da raccogliere un numero circo-

scritto di informazioni, escludendo l'acquisizione di dati ultronei rispetto a quelli necessari per la finalità perseguita nel caso concreto.

e corpo) o, ancora, in ragione delle condizioni degli operatori a cui dovrà essere applicato l'esoscheletro (e.g. esoscheletri volti a compensare deficit o disabilità dell'operatore), si potrebbe optare per soluzioni di *data protection by design* che escludano nella realizzazione degli esoscheletri la raccolta, anche in fase progettuale, di dati biometrici. Ciò potrebbe avvenire, ad esempio, progettando la struttura con meccanismi in grado di consentire una regolazione manuale dell'esoscheletro, una volta indossato dall'operatore (esoscheletri di Tipo A).

In alternativa, al fine di conseguire una maggiore efficacia degli esoscheletri, questi ultimi potrebbero essere progettati sulla base di *range* morfologici relativi, ad esempio, all'altezza o alla circonferenza toracica dei lavoratori o delle altre parti del corpo che risultino destinate ad interagire con il dispositivo nel caso specifico ³¹, o sulla base di categorie di soggetti (ad esempio, uomo-donna ³²). In questo secondo scenario, il processo di realizzazione vedrà una prima fase di raccolta di dati volta a definire i *range* di interesse rispetto alla popolazione dei lavoratori (ad esempio, rilevamento dell'altezza e circonferenza toracica, con successiva ripartizione della popolazione in classi omogenee). In questa fase i dati potrebbero essere raccolti in forma anonima, anche se in taluni casi la necessità di verificare che tutti i lavoratori interessati siano stati sottoposti ai controlli, nonché le eventuali esigenze di documentare la correttezza delle soluzioni adottate, potrebbero indurre al ricorso a soluzioni di pseudonimizzazione ³³, mantenendo i dati identificativi dei lavoratori in un *database* separato da quello relativo alle caratteristiche morfologiche degli stessi (ossia le misurazioni).

Una volta poi progettati gli esoscheletri, tali dati dovrebbero essere anonimizzati per aggregazione, qualora non sussista alcuna necessità di re-identificazione dei lavoratori e, dunque, di successiva conservazione dei dati in forma pseudoanonima ³⁴. Seguendo

³¹ Si noti che in questi casi, dovendosi ricavare dei *range* di misura, non occorre che la misurazione del singolo sia abbinata all'identità dello stesso, né il ricorso a strumenti ad elevata precisione, che potrebbero fornire un dato univoco e tale da individuare indirettamente il soggetto.

³² In termini di anonimato dei dati trattati, chiaramente l'individuazione dei *range* o delle categorie di soggetti va valutata in ragione del contesto specifico. Qualora, ad esempio, nell'impresa del titolare del trattamento lavori solo una donna, non sarà possibile utilizzare la categoria uomo-donna in quanto indirettamente identificativa dell'unico soggetto a cui i dati contenuti nella categoria "donna" si riferiscono.

³³ La definizione di "pseudonimizzazione" è stata introdotta per la prima volta dal Regolamento (UE) 2016/679 che all'art. 4, n. 5 la descrive come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

³⁴ Tuttavia, si consideri che anche una mera attività di raccolta ed elaborazione temporanea di dati biometrici costituisce a tutti gli effetti un trattamento di dati biome-

questa procedura non si otterranno esoscheletri *taylor-made*, ma strutture standard e variabili grazie a meccanismi regolabili, progettate sulla base di misure tradizionali senza l'utilizzo di immagini biometriche.

La sussistenza di particolari esigenze potrebbe, tuttavia, imporre o indurre a privilegiare l'impiego di dati personali biometrici. Tali esigenze potrebbero inerire al contesto lavorativo (ove, ad esempio, alcuni lavoratori debbano operare con o sollevare carichi pericolosi o speciali o nei casi in cui la personalizzazione sia necessaria per far fronte adeguatamente a sforzi fisici significativi, tali da necessitare un'alta conformità dell'esoscheletro al corpo dell'operatore a tutela della sicurezza di quest'ultimo) ovvero agli operatori stessi (qualora si tratti di soggetti affetti da patologie specifiche, ad esempio cardiache o vertebrali, oppure portatori di *handicap* ³⁵).

In questi casi, il trattamento di dati biometrici potrebbe apparire proporzionato e necessario in un'ottica di tutela dei diritti dell'interessato, in relazione alla pericolosità dell'attività lavorativa ovvero alla necessità di assicurare la salute del lavoratore ³⁶ o, ancora, per creare esoscheletri *ad hoc* che garantiscano una maggior occupazione o mobilità a soggetti svantaggiati. Tuttavia, anche in queste evenienze — nel rispetto del principio di minimizzazione dei dati — non si dovrebbero raccogliere dati eccedenti e non pertinenti alle finalità, pertanto potrebbe essere sproporzionato procedere con l'impiego di tecniche di *body scan* che acquisiscano dati relativi a tutto il corpo dell'operatore, quando i dati biometrici necessari siano solo quelli relativi alla parte del corpo (ad esempio, braccio o torace) su cui andrà applicato il dispositivo.

A tal riguardo, può anche farsi l'esempio delle *smart suit* ³⁷: come per gli esoscheletri, qualora non vi siano particolari esigenze da soddisfare inerenti al contesto lavorativo oppure al lavoratore,

trici. Così ha statuito recentemente la Corte di Cassazione con sentenza del 15 ottobre 2018, n. 25686, ritenendo che un sistema di rilevamento delle presenze dei dipendenti basato sulla lettura dei dati biometrici della mano costituisca un trattamento di dati biometrici, a prescindere dalla loro mancata registrazione in apposita banca dati.

³⁵ Occorre infatti considerare le ulteriori applicazioni dell'esoscheletro, oltre a quelle di ausilio nel sollevamento pesi: questo tipo di strutture offre la possibilità di supportare personale a ridotta capacità lavorativa o addirittura persone con disabilità, compensando o integrando in tutto o in parte specifici aspetti funzionali. Analogamente, in funzione del livello di perdita di

prestazioni fisiche correlato all'età, l'esoscheletro può divenire anche strumento di compensazione per il personale di più elevata anzianità.

³⁶ In questi casi potrebbe procedersi altresì ad un trattamento di dati inerenti ai parametri biologici, reso possibile o più agevole dall'impiego di dati biometrici per realizzare il dispositivo in dotazione al lavoratore (si pensi ad esempio ad un dispositivo per ridurre il peso di carichi sollevato da un lavoratore cardiopatico, che debba quindi tenere necessariamente conto del livello di stress cardiaco nel bilanciare l'interazione fra forza espressa dal soggetto ed apporto integrativo offerto dall'esoscheletro).

³⁷ Cfr. *infra* par. 2.2.

non risulterà proporzionato — ai fini della realizzazione della tuta — procedere ad una scansione del corpo per acquisire l'immagine biometrica del lavoratore, essendo sufficiente procedere con le tradizionali misurazioni del profilo e delle fattezze dello stesso, secondo classificazioni per gruppi, seguendo il modello di cui si è detto in precedenza.

Nei casi in cui sia giustificato il ricorso al trattamento di dati personali biometrici, questo comporterà, oltre al rispetto degli adempimenti previsti in materia, la valutazione di alcuni profili concernenti le modalità di trattamento, come la conservazione e l'archiviazione dei dati. A tal proposito, una limitazione inerente ai tempi di conservazione dei dati biometrici potrebbe essere in linea con l'approccio *by design* richiesto dal Regolamento (UE) 2016/679.

In tale ottica, una volta realizzato l'esoscheletro di Tipo B, i dati biometrici a quest'ultimo associati potrebbero essere distrutti. Va però rilevato come, in ragione della natura del prodotto e del suo impiego, potrebbe invece trovar giustificazione — sotto un profilo di necessità e proporzionalità — la conservazione ulteriore dei dati biometrici qualora si ipotizzassero successivi *upgrade* dell'esoscheletro ovvero un adattamento dello stesso in ragione delle mutate condizioni fisiche e di salute dell'operatore. Tali esigenze potrebbero inoltre giustificare un'archiviazione centralizzata dei dati ³⁸, in quanto permetterebbe di recuperare agevolmente i modelli senza dover nuovamente sottoporre l'operatore all'acquisizione di tali dati, operazioni che ove effettuate tramite *scanner* potrebbero risultare potenzialmente lesive della salute dell'operatore stesso.

Anche in questa ipotesi di conservazione del modello biometrico, in osservanza del principio di necessità, la durata di tale conservazione dovrebbe essere comunque commisurata alla durata del rapporto di lavoro. Trattandosi di dati univoci di un determinato individuo, qualora questi non sia più vincolato contrattualmente e l'impiego di tali dati sia connesso esclusivamente alle esigenze lavorative e concernenti il mantenimento dell'esoscheletro, non troverebbe giustificazione la conservazione prolungata dei dati biometrici dell'operatore non più alle dipendenze del titolare del trattamento ³⁹.

Va, infine, menzionata la possibilità di delineare un ulteriore scenario applicativo che potrebbe essere ancor più soddisfacente in termini di *data protection by design*. È questo il caso della

³⁸ Cfr. anche a riguardo GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee-guida in materia di riconoscimento biometrico e firma grafometrica*, Allegato A, 12 novembre 2014.

³⁹ Potrebbe invece conservarsi documentazione del processo eseguito per la realizzazione dell'esoscheletro in previsione di eventuali sopravvenienze in materia di danni lungolatenti alla salute del lavoratore.

realizzazione di esoscheletri rispetto ai quali la raccolta di dati biometrici potrebbe essere evitata in virtù dell'impiego di tecnologie dei materiali avanzate, tali da consentire di creare una struttura in grado di adattarsi spontaneamente e autonomamente al corpo dell'operatore in assenza di una modellizzazione a monte basata sui dati biometrici (i.e.: materiale composito termoinducente).

2.1.2. (segue). *Postazioni di lavoro auto-adattive.*

Nell'ambito della realizzazione delle *smart factories* un ruolo importante è attribuito alla qualità della postazione di lavoro ed alla sua realizzazione sulla base delle caratteristiche proprie di chi è chiamato ad utilizzarla, anche in termini di condizioni fisiche e di affaticamento (c.d. postazioni auto-adattive)⁴⁰. Questo comporta in vari casi l'acquisizione di dati personali, anche di tipo biometrico. Nel contempo, però, altri diritti del lavoratore, *in primis* quello alla salute, possono giustificare l'adozione di tali soluzioni e del correlato trattamento dati. Si ripropone quindi, anche in questo caso, la necessità di una valutazione dei rischi inerenti al trattamento che tenga in conto di un adeguato bilanciamento fra interessi ed i diritti contrapposti.

Nello specifico, con riguardo alla realizzazione delle postazioni auto-adattive si potrebbe ricorrere all'uso di dati anonimi progettando una postazione di lavoro regolabile direttamente dall'operatore, come nel caso sopra analizzato degli esoscheletri regolabili. Rispetto alle postazioni di lavoro, però, una simile soluzione risulterebbe penalizzante con riguardo alle potenziali utilità di tali postazioni, che verrebbero ad essere personalizzabili solo in termini ergonomici, mentre non verrebbe implementata l'ulteriore funzione consistente nella possibilità di variare la postazione e le condizioni di utilizzo della stessa in ragione delle condizioni fisiche momentanee dell'operatore, stimate mediante la rilevazione e l'analisi dei parametri vitali dell'operatore che la occupa.

Escludendo quindi l'impiego di dati anonimi⁴¹, qualora non vi siano esigenze che impongano o facciano propendere per l'utilizzo

⁴⁰ Oltre a supportare l'operatore nelle attività e nei processi manifatturieri, tali postazioni di lavoro auto-adattive sono in grado di rispondere alle esigenze degli operatori, in quanto flessibili e riconfigurabili in relazione alle condizioni fisiologiche di questi ultimi. Ciò significa che le postazioni in oggetto non saranno disegnate secondo standard che tengono conto delle caratteristiche fisionomiche della popolazione media, bensì calibrate sulle caratteristiche an-

tropometriche e biometriche del singolo operatore, comportando quindi un trattamento di dati biometrici.

⁴¹ Per quanto tecnicamente possibile, l'utilizzo di dati anonimi nel presente contesto non risulterebbe utile dal momento che, come già accennato, la finalità di tali postazioni è quella di "adattarsi" alle condizioni fisiologiche del soggetto che occupa quella postazione. Pertanto, sebbene tale soggetto non debba essere necessariamente

di dati personali in maniera diretta, potrebbe optarsi per l'impiego di dati oggetto di pseudonimizzazione. A tal fine occorrerà elaborare due *database* separati, contenenti l'uno i dati biometrici e fisiologici dell'operatore e l'altro i dati relativi alla postazione, prevedendo che solo procedure *ad hoc* eccezionali e soggette a controllo (e.g. tracciamento dell'operatore che le pone in essere mediante file di *log*) consentano l'abbinamento delle informazioni (ad esempio in caso di infortunio), mentre non sarà diversamente possibile associare i dati in questione rilevati in una postazione di lavoro (e.g. frequenza cardiaca, temperatura corporea) con l'identità del lavoratore che la occupa.

Ove invece le caratteristiche o le condizioni degli operatori rendano necessario un monitoraggio costante ed in tempo reale dei dati biometrici e fisiologici (e.g. operatore affetto da specifiche patologie), occorrerà poter ricollegare questi dati ad un soggetto individuato (sovente in tempo reale) e, dunque, trattarli senza alcun processo di pseudonimizzazione o anonimizzazione. Valgono poi qui le stesse regole e gli stessi vincoli esaminati per il trattamento di dati biometrici nell'ambito degli esoscheletri: oltre agli adempimenti previsti dalla normativa, dovranno rispettarsi i principi di necessità, proporzionalità e minimizzazione, in virtù dei quali si dovranno decidere le modalità di trattamento, compresa la conservazione delle informazioni ⁴².

Nello specifico, con riferimento ai tempi di conservazione, considerato che la finalità potrebbe essere quella di monitorare in tempo reale i parametri vitali dell'operatore che occupa la postazione, i dati potrebbero essere cancellati subito dopo la fine del turno di lavoro alla postazione, nel caso in cui non vi siano alterazioni di tali parametri e, dunque, non vi sia necessità di una loro conservazione. Qualora invece i parametri risultino fuori dalla norma e si renda necessario analizzarli per un periodo più prolungato per ragioni di tutela della salute del lavoratore, tali informazioni potrebbero essere conservate per il più ampio lasso di tempo utile a compiere le opportune verifiche, in ragione delle condizioni di lavoro, dei parametri considerati e delle possibili patologie associate.

Si può, infine, giustificare una più lunga conservazione, che vada oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in raccolti. Questo è ammissibile quando si sia in presenza di un trattamento esclusivamente a fini statistici. Tale finalità, stante la centralità degli *asset* informativi

identificato, devono potersi ricollegare i dati biometrici o i parametri vitali rilevati ad una determinata postazione ed al suo occupante. L'impiego di dati anonimi è altresì da escludere dal momento che in uno stabili-

mento produttivo si è in grado di risalire facilmente al soggetto che occupa una posizione in un dato momento.

⁴² Cfr. art. 5, par. 1, lett. e, Reg. (UE) 2016/679.

nel contesto dell'Industria 4.0 e del conseguente monitoraggio dei processi produttivi anche in maniera diacronica, potrebbe essere conseguita ricorrendo a soluzioni di anonimizzazione per la conservazione delle serie storiche di dati. Qualora, invece, per ragioni contingenti il ricorso all'anonimizzazione non sia possibile (e.g. rischio di patologie lungolatenti riconducibili all'attività lavorativa presso la postazione), si potrebbe optare per l'adozione di tecniche di pseudonimizzazione che consentano la conservazione delle informazioni a fini statistici in due *database* disgiunti, ove i dati identificativi sono archiviati separatamente da ogni altro dato, in modo da permettere differenti livelli di accesso e l'analisi statistica dei soli dati pseudonimizzati.⁴³

2.2. (Segue): *dati geo-referenziati e smart suit.*

Oltre all'implementazione di sistemi robotici fondati sull'utilizzo di dati biometrici, si possono ipotizzare altresì soluzioni tecnologiche che impieghino dati geo-referenziati, ossia quei dati che permettono di rilevare la posizione geografica, nonché il percorso del soggetto o dell'oggetto su cui sono installati i sensori⁴⁴.

Molteplici possono essere gli impieghi dei dati geo-referenziati, a partire da quelli inerenti ai servizi di mappe e navigazione, *geotagging*, pubblicità basata sulla localizzazione fino a quello di monitoraggio e sorveglianza. Queste ultime due funzionalità paiono particolarmente rilevanti e critiche in ambito lavorativo, ove l'impiego di dispositivi in grado di rilevare la posizione geografica dei veicoli o degli *smartphone* aziendali in dotazione ai dipendenti può in realtà tradursi in una forma di controllo delle attività di questi ultimi.

⁴³ Cfr. anche art. 89, Reg. (UE) 2016/679, nonché art. 97 ss., d. lgs. 196/2003.

⁴⁴ In termini definitori, manca una indicazione normativa specifica con riferimento a tale categoria di dati. Giova sottolineare che l'art. 121, c. 1-*bis*, lett. i), d. lgs. 196/2003, definisce dato relativo all'ubicazione "ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico". Tale definizione è tuttavia necessariamente riduttiva dal momento che venne adottata in attuazione della Direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche, circoscrivendo quindi la nozione in esame ai dati rilevabili me-

diante il dispositivo in dotazione ad un soggetto nell'ambito di un servizio di comunicazione elettronica accessibile al pubblico. Il Regolamento (UE) 2016/679 non disciplina i dati relativi alla localizzazione, in previsione della futura adozione di un Regolamento in materia di tutela della vita privata e dei dati personali nelle comunicazioni elettroniche destinato a ridefinire il quadro normativo incentrato sulla vigente Dir. 2002/58/CE. Cfr. a riguardo anche GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Opinion 1/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*, adottata il 4 aprile 2017, secondo cui "i dati di localizzazione derivanti dall'apparecchiatura terminale di una persona fisica sono dati personali e quindi il loro trattamento è soggetto agli obblighi del Regolamento (UE) 2016/679".

I dispositivi dotati della funzionalità di localizzazione “seguono” inoltre la persona che li detiene, indipendentemente dalla distinzione tra tempo di lavoro e tempo libero. Per tale motivo il trattamento dei dati personali relativi alla geolocalizzazione può presentare diversi rischi specifici per le libertà, i diritti e la dignità dei lavoratori. Il trattamento dei dati geo-referenziati deve pertanto rispettare i principi e le disposizioni in materia di protezione dei dati personali e prevedere misure di sicurezza adeguate rispetto alla peculiarità di tali dati.

Coerentemente con l’ambito di indagine delineato, tali applicazioni vengono qui considerate nell’ottica della definizione di soluzioni di *data protection by design*, tralasciando invece le implicazioni giuslaburistiche del ricorso all’impiego di dispositivi di geo-localizzazione.

Nel contesto delle c.d. *smart factories* un primo ambito di applicazione innovativo concernente dati geo-referenziati riguarda l’impiego di *smart suit* o tute intelligenti. Tali dispositivi incorporano una serie di sensori che permettono di monitorare i parametri vitali dell’operatore⁴⁵ e di rilevarne altresì la posizione.

Il dato della posizione geografica dell’operatore è necessario per una duplice finalità inerente alla collaborazione uomo-macchina. Da un lato, occorre poter individuare esattamente la posizione dell’operatore in modo che il *robot* che lo assiste moduli i propri movimenti in base agli spostamenti dell’operatore⁴⁶. Dall’altro, la rilevazione dell’esatta posizione dell’operatore è presupposto necessario per l’utilizzo di sistemi AVG (*Automated Vehicle Guided*), ossia veicoli a guida autonoma (solitamente carrelli o simili) volti alla movimentazione dei prodotti all’interno dello stabilimento e, ove necessario, anche destinati alla cooperazione con i lavoratori. Sia per evitare incidenti con gli esseri umani, sia per assistere correttamente i lavoratori si rende dunque necessaria la conoscenza della posizione di questi ultimi⁴⁷.

Anche in questo caso il *design* della strategia in materia di trattamento dati dovrà partire dalla valutazione della possibilità di ricorrere a dati anonimi per il perseguimento di tali finalità, ovvero dal considerare se sia quantomeno ipotizzabile l’impiego di tecniche di psuedoanonimizzazione.

⁴⁵ Si vedano in proposito le considerazioni espresse nel precedente paragrafo con riferimento alle postazioni auto-adattive.

⁴⁶ In tal modo si potrebbero evitare situazioni rischiose e pericolose in cui il *robot*, o qualsivoglia macchina automatizzata, provochi un incidente o un danno fisico all’operatore a causa di una mancata rilevazione della sua presenza nello spazio operativo circostante.

⁴⁷ Si prevede lo scenario in cui l’operatore necessiti di un determinato componente ovvero di assistenza nello svolgimento della mansione e richieda l’intervento di un robot AGV. A tal fine occorre che il *robot* sia in grado di raggiungere autonomamente l’operatore nella sua esatta posizione.

Un primo scenario al riguardo è rappresentato dall'utilizzo di tute non personalizzate. In tal caso, non risultando necessario l'impiego di tute *ad hoc*, le stesse potrebbero essere attribuite in modo randomico agli operatori.

Ove la procedura di assegnazione della tuta non preveda l'associazione dei dati identificativi dell'operatore, l'attribuzione casuale permetterebbe l'utilizzo di dati anonimi, dal momento che la rilevazione dei dati di geolocalizzazione consentirebbe soltanto l'individuazione della posizione della tuta mentre non sarebbe idonea a rivelare l'identità dell'operatore che la indossa. Tale scenario rischia però di rivelarsi di limitata applicazione, essendo solitamente possibile nel contesto lavorativo di uno stabilimento risalire facilmente al soggetto che lavora in una determinata area ad una certa ora. Tuttavia, tale limite potrebbe essere superato ove i sensori presenti nella tuta “dialoghino” direttamente con i vari dispositivi esterni presenti nella fabbrica (e.g. robots, sensori), senza che la comunicazione transiti per un *server* centrale che ne tenga traccia. In questo caso, ad esempio, un braccio robotico potrebbe tenere traccia in locale dell'interazione con i sensori della *smart suit* per il tempo strettamente necessario al compimento delle operazioni da parte del lavoratore che indossa la tuta, provvedendo poi alla cancellazione automatica dei dati ove, terminata tale attività, non si siano verificati eventi anomali (e.g. infortuni).

Un secondo scenario potrebbe concretizzarsi nel caso in cui le *smart suit* vengano invece assegnate in maniera fissa e predeterminata agli operatori in ragione della loro personalizzazione⁴⁸. In tal caso, ogni tuta corrisponderebbe ad un determinato operatore e, conseguentemente, la geolocalizzazione della tuta comporterebbe, indirettamente, l'individuazione ed identificazione dell'operatore che la indossa.

Per aggirare tale eventualità — a parte il ricorso al mero dialogo *machine-to-machine* di cui si è detto sopra — si potrebbero impiegare dati pseudoanonimi attraverso la creazione di due *database* separati, l'uno contenente i dati identificativi dell'operatore e l'altro quelli di geolocalizzazione della tuta, prevedendo che solo procedure *ad hoc* eccezionali consentano l'abbinamento delle informazioni (ad esempio in caso di infortunio o di anomalie), al di fuori delle quali non sarà possibile associare i dati di geolocalizzazione della tuta con l'identità dell'operatore che la indossa⁴⁹.

⁴⁸ È il caso in cui la tuta sia personalizzata e su misura di uno specifico lavoratore per via delle caratteristiche fisiche di quest'ultimo, delle speciali mansioni affidategli ovvero perché affetto da *handicap* fi-

sico o patologie che necessitano di un monitoraggio costante e specifico.

⁴⁹ Si vedano anche le ulteriori misure delineate nei provvedimenti GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento*

Tuttavia, possono emergere situazioni particolari che richiedono la necessaria associazione dei dati identificativi e di quelli relativi alla geolocalizzazione, ad esempio per finalità di sicurezza sul lavoro e dell'ambiente lavorativo (e.g. accesso ed operazioni in aree ad alto rischio, sistemi di sicurezza in dette aree): in tal caso, l'utilizzo di dati non sottoposti a pseudonimizzazione sarebbe legittimo purché, a seguito di un bilanciamento di interessi, il trattamento dei dati personali appaia necessario e proporzionato rispetto alle finalità e tenuto conto delle libertà e dei diritti degli operatori.

Giova ricordare che, sempre sulla base di un bilanciamento di interessi, occorrerà stabilire se la rilevazione dei dati georeferenziati possa avvenire in maniera continuativa e in tempo reale ⁵⁰ ovvero secondo una periodizzazione temporale predefinita ⁵¹ o, ancora, al verificarsi di eventi predeterminati ⁵². In ogni caso, qualora la rilevazione dei dati geo-referenziati si risolva in una forma di controllo a distanza dei lavoratori (come sovente accade), occorrerà osservare il dettato normativo dello Statuto dei Lavoratori e, come previsto ai sensi dell'art. 4, un previo accordo con le rappresentanze sindacali ovvero l'autorizzazione dell'Ispettorato del lavoro ⁵³.

Infine, anche i termini di conservazione saranno diversi a seconda delle finalità perseguite e della tipologia di dati trattati. Fatto salvo il principio generale di limitazione della conservazione, i dati di geolocalizzazione potrebbero essere conservati, su base storica, per finalità di analisi e di ottimizzazione delle prestazioni e delle attività a condizione che vengano previamente anonimizzati per aggregazione. Potranno invece essere conservati in forma non anonimizzata per un periodo più lungo qualora necessari per osservare adempimenti relativi alla gestione del rapporto contrattuale (i.e. calcolo della busta paga o tenuta del libro unico del lavoro), limitatamente alle informazioni richieste

di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi *smartphone*. Verifica preliminare richiesta da Wind Telecomunicazioni s.p.a., 9 ottobre 2014, doc. web n. 3505371 e GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi *smartphone*. Verifica preliminare richiesta da Ericsson Telecomunicazioni s.p.a.*, 11 settembre 2014, doc. web n. 3474069.

⁵⁰ La rilevazione costante e in tempo reale potrebbe risultare necessaria in caso di cooperazione continuativa con un *robot*, tale per cui occorra monitorare la posizione dell'operatore per tutta la durata dello svol-

gimento dell'attività o della mansione o, finanche, del turno di lavoro. Tuttavia, in questo caso, sarebbe preferibile adottare la già menzionata soluzione dell'archivio temporaneo dei dati in locale in maniera decentrata sul *robot*.

⁵¹ Ad esempio, secondo intervalli di tempo prestabiliti e congrui in relazione alle finalità perseguite. Cfr. *supra* nota 49.

⁵² Come, ad esempio, in caso di anomalie, disservizi o incidenti.

⁵³ Cfr. ampiamente in tal senso, G. FINOCCHIARO, *Limiti posti dal Codice in materia di protezione dei dati personali al controllo del datore di lavoro*, in P. TULLINI (a cura di), *Web e lavoro: profili evolutivi e di tutela*, Torino, 2017.

dalla normativa di riferimento e per un periodo di tempo commisurato a quello richiesto per l'assolvimento di detti adempimenti. In tal senso, qualora le finalità del trattamento siano invece solo concernenti il corretto svolgimento dell'attività lavorativa, si potrebbe prevedere la cancellazione automatica dei dati a fine turno, al termine della giornata lavorativa o, in presenza di anomalie ovvero di particolari situazioni che necessitino di essere esaminate (e.g. ragioni di sicurezza inerenti la conservazione del patrimonio aziendale), la cancellazione dei dati potrà avvenire non appena si saranno concluse le opportune verifiche.

2.3. (segue). *Dati relativi alla voce.*

Per molto tempo si è discusso se qualificare la voce alla stregua di un dato personale. Oggi la qualificazione della voce come informazione riconducibile ad un soggetto identificabile o identificato è pacifica. In più occasioni⁵⁴, il Gruppo di lavoro Art. 29 ha poi ricondotto la voce entro la categoria dei dati biometrici.

Come è proprio dei dati biometrici, anche i sistemi basati sulle tracce vocali prevedono articolate procedure di acquisizione del dato⁵⁵. Una prima fase di campionamento consiste nel far pronunciare ripetutamente all'utente una determinata frase ovvero una serie di vocaboli differenti affinché il sistema possa acquisire informazioni sufficienti per formare il vocabolario dell'utente (fase di *enrollment*) e consentire la sua successiva univoca identificazione. Le informazioni vocali così raccolte (consistenti, ad esempio, nella cadenza, nel timbro e nel tono di voce) vengono quindi trasformate in un *template* che verrà utilizzato ogni volta per il confronto con il dato biometrico risultante dall'analisi delle parole pronunciate dall'utente. Alla procedura di acquisizione e confronto seguirà quindi il riconoscimento e l'identificazione del soggetto, salvo particolari circostanze in cui questo non sia possibile⁵⁶.

2.3.1. (segue). *Sistemi di identificazione vocale.*

Nel contesto delle *smart factories*, le tracce vocali possono

⁵⁴ Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 4/2007 sul concetto di dati personali*, adottato il 20 giugno 2007, e *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, adottato il 27 aprile 2012.

⁵⁵ Cfr. G.W. KENNEDY, *Thumbs Up for Biometric Authentication*, in *Computer L. Rev. & Tech. J.*, 2004, 8, 379 ss.; J.D. WOODWARD, *Biometric Scanning, Law & Policy: Identifying the Concerns - Drafting the*

Biometric Blueprint, in *U. Pitt. L. Rev.*, 1997, 59, 97 ss.

⁵⁶ Il sistema potrebbe non riuscire a identificare l'utente in caso di errata pronuncia di un vocabolo o di una frase ovvero qualora la voce dell'utente risulti alterata (a causa, ad esempio, di un raffreddore o di un particolare stato emotivo). Ancora, la mancata identificazione potrebbe conseguire anche nel caso di elevato rumore ambientale che disturba la ricezione delle tracce vocali.

essere impiegate ai fini di identificazione per l'accesso ad aree comuni ovvero a zone particolarmente sensibili in ragione di condizioni di rischio o di segretezza. Va in proposito rilevato come, la natura biometrica del dato, la procedura di *enrollment* e di generazione del *template*, di cui si è detto, escludano in radice la possibilità di avere a che fare con dati raccolti *ab origine* in modo anonimo⁵⁷.

Stante la natura stessa del *template* generato ed il suo successivo impiego, non pare neppure possibile addivenire ad una anonimizzazione dello stesso (ad es. peggioramento della qualità della traccia, con riduzione della frequenza di campionamento), pena la perdita di utilità del medesimo ai fini di riconoscimento vocale. Le tracce vocali potrebbero però essere oggetto di successive procedure di pseudonimizzazione.

In quest'ultima ipotesi, a seguito dell'acquisizione delle tracce vocali, i dati identificativi del lavoratore potrebbero essere separati dai *template* biometrici formati a seguito del campionamento, impiegando due *database* separati e non comunicanti tra loro. A ogni *template* potrebbe essere quindi attribuito un codice identificativo che individui l'utente come soggetto autorizzato all'accesso, senza però rivelarne l'identità.

Qualora il riconoscimento del lavoratore sia invece finalizzato all'ingresso in aree sensibili, potrebbe sussistere la specifica esigenza di conoscere in tempo reale l'identità di colui che vi accede per fini di prevenzione e sicurezza. In tal caso, valutando la sensibilità dell'area, la rischiosità dell'attività ivi svolta e le informazioni e i beni ivi custoditi, il trattamento di dati personali (i.e. tracce vocali identificative non oggetto di pseudonimizzazione) potrebbe essere considerato necessario e proporzionato.

Relativamente alla conservazione delle tracce vocali, occorre distinguere fra la conservazione di dette tracce in forma di *template* e la conservazione del comando vocale ricevuto dal dispositivo che si attiva sulla base di quest'ultimo. Mentre, infatti, con riguardo al primo caso è ragionevole prevedere un più ampio periodo di conservazione, che coincide con il perdurare dell'esigenza di far uso dei comandi vocali ad opera del dipendente, nel secondo caso la memorizzazione del comando vocale ricevuto potrebbe non avvenire o avvenire per un lasso temporale limitato.

Con riferimento alla memorizzazione del comando vocale ricevuto, occorrerà considerare la particolarità dell'area e la finalità a cui il sistema di riconoscimento è preposto. A tal proposito, in assenza di disposizioni *ad hoc*, potrebbe considerarsi in via

⁵⁷ Allo stato attuale non si rinvencono tecniche diffuse nella prassi in grado di scindere, sin dalla raccolta, il dato biome-

trico dall'identità del soggetto a cui appartiene.

analogica quanto previsto in materia di videosorveglianza e conservazione delle immagini ⁵⁸.

Qualora si tratti di aree comuni e spesso frequentate, che non presentino rischi per l'incolumità dei lavoratori né custodiscano informazioni o beni di valore, i dati relativi ai comandi vocali potrebbero invece essere cancellati immediatamente dopo l'avvenuta identificazione ovvero, per soddisfare esigenze minime di sicurezza, potrebbero essere conservati per un periodo limitato di tempo pari ad un massimo di ventiquattro ore dalla rilevazione. Decorso tale termine, andrebbero previsti meccanismi di cancellazione automatica dei dati in questione.

Potrebbe poi ritenersi ammesso un tempo più ampio di conservazione dei comandi vocali qualora emergano esigenze di tutela del patrimonio aziendale rispetto a possibili atti illeciti ovvero sia necessario assicurare l'incolumità dei lavoratori. In questi casi, la conservazione prolungata delle informazioni potrebbe agevolare le indagini finalizzate all'identificazione di eventuali responsabilità, considerando altresì che spesso l'accertamento di illeciti, anomalie o incidenti avviene solo a fronte di complesse attività di controllo o, comunque, a distanza di tempo rispetto all'accadimento ⁵⁹.

Con riferimento al *template*, questo andrà invece cancellato qualora la sua conservazione non sia più necessaria al perseguimento delle finalità, ad esempio quando l'interessato non ha più necessità di ricorrere all'identificazione vocale a causa del mutamento della mansione affidata ovvero per cessazione del rapporto lavorativo.

2.3.2. (segue). *Comandi vocali indirizzati a robot o AGV.*

Le tracce vocali possono anche essere coinvolte in un secondo scenario in cui si concretizza la cooperazione uomo-macchina: si tratta delle ipotesi in cui il lavoratore fornisca istruzioni o comandi vocali al *robot* o a sistemi AGV (*Automated Guided Vehicle*) volti alla movimentazione dei prodotti all'interno di uno stabilimento.

⁵⁸ Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Provvedimento in materia di videosorveglianza, 8 aprile 2010, doc. web n. 1712680, <<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680#3.4>>.

⁵⁹ Ad esempio, potrebbe prevedersi un termine di conservazione delle tracce vocali pari a cinque anni coincidente con il termine di prescrizione previsto dall'art. 2947, 1° comma c.c. per il diritto al risarcimento del danno derivante da fatto illecito. In

modo analogo il Garante ha ammesso la conservazione pari a due anni delle immagini registrate concernenti eventi significativi relativi a sinistri da circolazione, al fine di far valere le pretese connesse al verificarsi di danni prodotti dalla circolazione di veicoli ex art. 2947, 2° comma c.c. (cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, provvedimento del 29 novembre 2012, doc. web n. 2257616, <<http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2257616>>).

Anche in questi casi, si potrà ricorrere a procedure di pseudonimizzazione delle tracce vocali. Dopo la fase di campionamento e trasformazione del dato in *template*, potranno essere creati due *database* separati l'uno contenente i dati identificativi del lavoratore e l'altro i dati relativi alla sua voce, prevedendo che solo procedure *ad hoc* eccezionali consentano l'abbinamento delle informazioni (ad esempio in caso di infortunio o di anomalie), al di fuori delle quali non sarà possibile associare le tracce vocali con l'identità del lavoratore a cui esse appartengono.

È possibile infine immaginare un eventuale scenario futuro in cui, specie i *robot*, vengano programmati in modo da rispondere ai comandi solo di soggetti qualificati e/o autorizzati (e.g. interazione uomo-macchina sulla postazione di lavoro). In tal caso, in alcune ipotesi l'identificazione del soggetto sarebbe connaturata al tipo di interazione (seguendo l'esempio, è nota l'identità del soggetto che occupa la postazione di lavoro) o conseguenza della necessità di restringere solo a determinati soggetti legittimati (per ruolo o funzione attribuiti) la possibilità di dare un determinato comando al *robot*. In tali casi, occorrerà comunque valutare preliminarmente se, in applicazione dei principi di minimizzazione e proporzionalità, non serva ricorrere invece a diverse soluzioni tecniche (pseudonimizzazione o attribuzione di comandi non per via vocale), al fine di operare un bilanciamento con le esigenze di proporzionalità e necessità del trattamento che legittimi l'impiego di dati personali.

Anche in questo scenario, la conservazione andrà commisurata alle finalità perseguite e, quindi, non dovrà essere superiore al tempo necessario al conseguimento delle finalità per le quali le tracce vocali sono state rilevate.

Quando tuttavia lo scopo connesso all'impiego di tracce vocali non riguardi l'identificazione, ma l'interazione con le macchine, la necessità di conservazione del comando vocale potrebbe essere minore. Così, ad esempio nel caso di attivazione o blocco di un AGV su base di comando vocale, quest'ultimo potrà essere memorizzato dall'AGV per eventuali esigenze probatorie in caso di incidente (e.g. caso in cui l'AGV non risponde al comando ed investe il lavoratore danneggiandolo), ma la durata della conservazione del dato sarà funzionale al verificarsi dell'evento dannoso (seguendo nell'esempio, se entro un breve lasso di tempo nessun incidente si è verificato non occorre conservare ulteriormente traccia del comando ricevuto).

Sono poi ravvisabili casi più complessi di interazione uomo-robot, rispetto ai quali possono essere necessari accertamenti *ex post* ai fini di sicurezza aziendale o di accertamento delle dinamiche di eventi dannosi con riferimento a lassi temporali più ampi. Da qui la necessità di una valutazione caso per caso rispetto ai tempi di conservazione dei comandi vocali.

Con riguardo, infine, alla conservazione del *template* valgono le considerazioni espresse nel paragrafo precedente.

3. CONCLUSIONI.

Il fine della presente analisi va al di là dell'applicazione del Regolamento (UE) 2016/679 ad alcune delle principali tecnologie che, nell'arco di pochi anni, connoteranno l'interazione uomo-macchina nel contesto dell'Industria 4.0. Sebbene questo sia un primo risultato operativo dell'indagine condotta, il portato principale della stessa è però di carattere metodologico.

Attraverso il caso della *smart factory* si sono infatti potute delineare le fasi operative e le logiche sottese all'applicazione dei due elementi chiave del nuovo Regolamento, ossia la valutazione dell'impatto dell'uso dei dati e l'adozione delle misure volte a mitigare tale impatto sin dalla fase iniziale della progettazione dei prodotti o servizi. Gli scenari esaminati offrono dunque una concreta applicazione di tale metodologia, aprendo ad una visione maggiormente orientata all'analisi empirica della disciplina sul trattamento dei dati personali.

Ormai a distanza di oltre quarant'anni dalla prima normativa nazionale adottata in Europa in materia di dati personali, vent'anni dopo l'adozione della Dir. 95/46/CE, forti di un'ampia elaborazione dottrinale e giurisprudenziale, pare infatti esser giunto il tempo di porre una maggior attenzione, anche nel contesto del dibattito dottrinale italiano, agli aspetti operativi e concreti di questa materia. Aspetti con riguardo ai quali anche la dottrina può apportare un contributo in termini di potenziali soluzioni, tanto più importante laddove — specie in Italia — pare ancora mancare un'adeguata cultura operativa in materia di trattamento dei dati personali e ancora incerto è il profilo del cosiddetto “esperto di privacy”.