Ghionzoli S., 'Sistemi di ia in ambiente di lavoro: traiettorie giuridiche tra privacy e strategia dei droni 2.0' (2025) EJPLT.
DOI: https://doi.org/10.57230/EJPLT25SIBGS

EJPLT
ISSN 2704-8012



Sistemi di ia in ambiente di lavoro: traiettorie giuridiche tra privacy e strategia dei droni 2.0.

Ia systems in the workplace: legal trajectories between privacy and strategy 2.0

SIMONA GHIONZOLI
Avv., Ph.D (c)
Università degli Studi L'Orientale di Napoli

Abstract

Verranno esaminate le norme internazionali, comunitarie e nazionali speciali, per tentare di comprendere se la normativa vigente, in punto di allocazione della responsabilità e non solo, derivante dall'impiego civile dei droni, sia coerente con le disposizioni di cui al Regolamento UE/2016/679 del 27 Aprile 2016 cd. GDPR, nonché con le esigenze del mercato che, prima dell'immissione in circolazione del prodotto, richiedono la conformità ad alcuni standard tecnici, di cui al Regolamento UE/2018/1139, uniformante la materia. I droni risultano, inoltre, interessati, ma solo in parte, dall'applicazione del Regolamento UE/2024/1689, che stabilisce regole armonizzate sull'intelligenza artificiale. E' stata persa un'occasione di tutela dei diritti fondamentali oppure gli strumenti di tutela giuridica, ivi inclusa la tutela dell'integrità psico-fisica del lavoratore, restano garantiti dagli istituti di tutela contenuti nel GDPR e nel Regolamento UE/2018/1139, che

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract:

The international, EU and special national regulations will be examined in an attempt to understand whether the current legislation, in terms of allocation of liability and more, arising from the civil use of drones, is consistent with the provisions set out in Regulation EU/2016/679 of 27 April 2016 cd. GDPR, as well as with the needs of the market that, before the product is put into circulation, require compliance with certain technical standards, referred to in Regulation EU/2018/1139, standardising the matter. Drones are also affected, but only partially, by the application of Regulation EU/2024/1689, which establishes harmonised rules on artificial intelligence.

Has an opportunity for the protection of fundamental rights been missed, or do the instruments of legal protection, including the protection of the psycho-physical integrity of the worker, remain guaranteed by the protective institutions contained in the GDPR and Regulation EU/2018/1139, which share relevant institutions including privacy and security by design?

Keywords: Intelligenza artificiale, sorveglianza, droni, lavoro, privacy by design, security by design, responsabilità, tecno regolazione, dati personali, consenso.

Summary: Introduzione. – 1. Definizioni e categorie nella legislazione nazionale, internazionale e dell'Unione Europea. - 2. Stato dell'arte. La marcia dei droni nella normativa nazionale, internazionale e dell'UE. Intersezioni giuridiche con Ai Act - 3. Droni e contesti operativi. Scenari attuali e futuri. – 4. Droni e potere di controllo del datore di lavoro tra Gdpr e Statuto dei Diritti dei Lavoratori, come modificato dal D.lgs 151/2015, del 23 settembre 2015, attuativo del cd. *Jobs Act.* - 5. Droni e protezione dei lavoratori nel Gdpr e nell'Ai Act. - 6. Droni e responsabilità: limiti dell'attuale regolamentazione o mancanza di regolamentazione? - 7. Dalla responsabilità all'*accountability.* Il GDPR e gli istituti a sostegno della contrattazione e della consultazione con le parti sociali. - 8. I codici di condotta. (Rinvio). - 9. Le vulnerabilità nel Gdpr e nell'Ai Act. – 10. Rilevanza della tecno-regolazione e della *privacy by design* per la privacy e la sicurezza dei dati nel Regolamento 2018/1139/UE e nell'art. 25 Gdpr. Intersezioni giuridiche con Ai Act. - 11. Droni e sandbox. Art. 57 Ai Act. - 12. Allocazione della responsabilità tra sviluppo della normativa e raccomandazioni. Nuove regole o nuovi modelli organizzativi? - 13. I Codici di condotta e la contrattazione collettiva come strumenti funzionali alla costruzione del consenso, all'implementazione della trasparenza e alla mitigazione dei rischi del trattamento. - 14. Conclusioni.

Introduzione[1].

[1] Il presente contributo è la traduzione in lingua italiana di un articolo, pubblicato sulla Rivista Scientifica di Diritto Mercato e Innovazione, *JLMI,* Vol. *3, 2024/3.* 375-415. L'autrice è Ph.D in Studi Internazionali presso l'Università degli Studi L'Orientale di Napoli e Ricercatrice presso Re.CEPL, Research Centre of European Private Law, Unisob (NA).

Nel 1970, con l'approvazione dello Statuto dei Lavoratori[2], più precisamente con l'art. 4[3], il legislatore ha introdotto e riconosciuto nell'ordinamento giuridico italiano disposizioni a tutela della privacy dei lavoratori, che fino ad allora erano state riconosciute indirettamente e limitatamente ad alcuni aspetti, come quelli di cui agli articoli 14, 15, 21 e 2 della Carta costituzionale italiana[4]

Quest'ultima disposizione, in particolare, assorbe la privacy tra i diritti fondamentali dell'individuo, analogamente a quanto affermato, invece, espressamente, negli articoli 7 e 8 della Carta dei diritti dell'Unione Europea, firmata a Nizza il 7 dicembre 2000.

Nei contesti produttivi, la tutela dei diritti fondamentali, primo fra tutti il diritto alla privacy, è oggi un tema centrale, a causa della diffusione e dello sviluppo di tecnologie sempre più innovative e pervasive, che configurano scenari di videosorveglianza inediti.

La videosorveglianza esercitata tramite UAS ovvero Unmanned Aircraft System (i cosiddetti droni), viene utilizzata in diversi contesti operativi per garantire innanzitutto la sicurezza e la sorveglianza dei luoghi di lavoro, soprattutto quando l'impiego di dispositivi fissi non risulta sufficiente.

I settori produttivi che hanno iniziato ad utilizzare queste tecnologie sono quelli industriali, portuali, dell'e-commerce per le funzioni di logistica e magazzino.

Da segnalare anche le esperienze di videosorveglianza urbana in alcuni Comuni, realizzate dalla polizia municipale con l'ausilio di droni (sicurezza stradale, flussi pedonali, orari di sosta, accesso alle aree chiuse al traffico, ecc.) e la sorveglianza di pozzi petroliferi, oleodotti, centrali termoelettriche oltre che impianti industriali e porti.

In questi contesti operativi, le soluzioni di intelligenza artificiale accompagnano i sistemi di videosorveglianza, in quanto sono in grado di monitorare e controllare punti difficilmente raggiungibili e di farlo in sicurezza e in tempo reale, riconoscendo, attraverso l'elaborazione delle immagini e i meccanismi di edge computing e deep learning, le situazioni di pericolo[5].

Avvalendosi di speciali sensori (termocamere, telecamere multispettrali, ecc.) indicano e mantengono la loro traiettoria di volo, rilevano e raccolgono

---

[2] Lo Statuto dei Lavoratori è riferito alla L. n. 300 del 20 maggio 1970 <<Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento>>.

[3] L'art. 4 della L. 20 maggio 1970, n. 300, è stato in seguito modificato dall'art. 23 del D.Lgs. n. 151 del 14 settembre 2015 ed è uno dei Decreti attuativi del Jobs Act, contenuto nella Legge Delega n. 183 del 10 dicembre 2014.

[4] D. FAUCEGLIA, *Cybersecurity, concorrenza, contratti e cyber-rischio*, in *Ejplt,* 2020, 1, 1, 1.

[5] Agenzia europea per la sicurezza e la salute sul lavoro, *Unmanned aerial vehicles: implications for occupational safety and health*, 2023. Disponibile all'indirizzo https://www.osha.europa.eu, consultato il 05 settembre 2023.

informazioni, effettuano sorveglianza e ricognizione in modo autonomo. Sono dotati di radar, telecamere, scanner IR.

Se combinati con altre tecnologie elaborano dati personali e sono in grado di interagire con la tecnologia di localizzazione, basata sui satelliti GPS. Le tecnologie integrate sono in grado di tracciare i dispositivi dotati di chip RFID e le persone che li indossano. Se utilizzati con dispositivi di geo-localizzazione, possono intercettare le comunicazioni e i dispositivi elettronici profilando le persone[6].

Risultano dotati, infatti, di una tecnologia di <<apparecchiatura di registrazione visiva>> con capacità di riconoscimento facciale a bordo o da terra, che consente il tracciamento e l'identificazione delle persone e dei dati sensibili e personali[7].

La maggior parte di essi raccoglie informazioni sulla vita quotidiana degli utenti, sulle abitudini e sulle caratteristiche sensibili, compresi gli stati fisici e mentali, per mezzo dell'enorme quantità di sensori, che sono in grado di trasportare.

In questo quadro, in ambito lavorativo, non è trascurabile l'importanza dei dati di "ubicazione", la cui definizione è riscontrabile nella normativa[8], perché sono considerati un identificativo, che consente di individuare la propria posizione e di tracciare i propri spostamenti e quindi in grado di rendere identificabile qualsiasi soggetto ad esso associato[9]. Questo spiega l'inesistenza di dati di ubicazione anonimi o non personali, perché ogni volta che si identifica la presenza di una persona fisica in un punto dello spazio, qualsiasi informazione o dato costituirà di per sé un trattamento di dati personali[10].

L'articolo 4, 1° co), del GDPR definisce, a questo proposito, gli <<identificativi>> accompagnati dall'avverbio <<qualsiasi>>, gli elementi in grado di collegare le informazioni alla persona fisica per identificarla[11].

---

[6] Direzione Generale per le Politiche Interne, Dipartimento di Politica dei Diritti dei Cittadini e Affari Costituzionali, *Privacy and Data Protection implications of the civil use of drones* (2015). Disponibile all'indirizzo www.europarl.europa.eu/studies, consultato il 4 novembre 2024.

[7] Artt. 4.1 e 9, 1° co), Reg. 2016/679/UE.

[8] L'art. 2, lett. c), della Direttiva 2002/58/CE, come modificata dalla Direttiva 2009/136/CE, definisce tale tipologia di dati come <<qualsiasi dato trattato in una rete di comunicazione elettronica o in un servizio di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente in un servizio di comunicazione accessibile al pubblico>>.

[9] G.M. RICCIO, G. SCORZA, E. BELISARIO, *GDPR e normativa privacy. Commentario.* Vicenza, 2020, 790.

[10] G.C. MALGIERI, *La titolarità dei dati trattati per mezzo dei droni tra privacy e proprietà intellettuale* in *Diritto dei droni: regole, questioni e prassi,* a cura di E. PALMERINI, M.A. BIASIOTTI, G. F. AIELLO, Lavis (TN), 2018, 194. *Contra* F. QUADRI, *Dati relativi all'ubicazione (commento all'art. 126)*, in Aa.Vv., *La protezione dei dati personali. Commentario al D. lgs. 30 giugno 2003, 196 («Codice della Privacy»)*, a cura di C.M. BIANCA, F.D. BUSNELLI, Tomo II, Padova, 2007, 1550-1555 (..).

[11] Per una discussione approfondita sull'efficacia dell'anonimizzazione e della pseudo-anonimizzazione dei dati personali si veda il Provv. GPDP n. 5, dell'11 gennaio 2024, disponibile all'indirizzo <https://www.garanteprivacy.it/home/docweb/-/docweb- display/docweb/9977020> consultato l'8 marzo 2024.

1. Definizioni e categorie nella legislazione internazionale, nazionale e dell'Unione Europea.

I droni sono giuridicamente equiparati agli aeromobili.

La Convenzione di Chicago sull'Aviazione Civile Internazionale del 1944 all'articolo 8, già faceva riferimento a <<*aircraft capable of being flown without a pilot*>>.[12] La Dichiarazione di Riga sui droni del 06/03/2015 aggiungeva che <<*Drones need to be treated as a new type of aircraft with proportionate rules based on the risk of each operation*>>.

Il Regolamento 2018/1139/UE, all'art. 3, comma 30), parla di <<aeromobili senza equipaggio>> ovvero <<*Unmanned aircraft means any aircraft operating or designed to operate autonomously or to be piloted remotely without a pilot on board*>>.

Ai fini di una corretta definizione e classificazione dei velivoli occorre fare riferimento all'articolo 2 del Regolamento 2019/947/UE, che contiene la definizione *Unmanned Aircraft System* (UAS) riferito a aeromobile senza pilota e i suoi dispositivi di controllo remoto, <<*an unmanned aircraft and the equipment to control it*>>.

Questa definizione è quella preferita dall'ICAO (International Civil Aviation Organization). Comprende il velivolo, ma anche le attrezzature di rete e il personale necessario per controllare il velivolo. Si differenzia dall'acronimo UAV o *Unmanned Aircraft Vehicle* (veicolo aereo senza pilota), genericamente inteso come un velivolo progettato per operare senza pilota a bordo, che non trasporta passeggeri, pilotabile da remoto, in grado di volare autonomamente, senza fare alcun riferimento alle attrezzature.

Il quadro normativo sui droni è composto da una pluralità di atti, che si coordinano in modo gerarchico, articolati su tre livelli ovvero internazionale, comunitario, nazionale:

Convenzione sull'aviazione civile internazionale firmata a Chicago il 07/12/1944;

Regolamento 2018/1139/UE del 04/07/2018;

Regolamento Delegato 2019/945/UE del 12/03/2019;

Regolamento di Esecuzione 2019/947/UE(UE)del 24/05/2019;

Codice della Navigazione (Regio Decreto n. 327 del 30/03/1942);

Reg. ENAC UAS IT del 04/01/2021 (per gli aspetti che rientrano nelle disposizioni dell'art. 2, par. 3 del Reg. (UE) n. 1139/2018 e per gli aspetti di competenza degli Stati membri).

Regolamento del Parlamento Europeo e del Consiglio che stabilisce

regole armonizzate sull'intelligenza artificiale, 2024/1689/UE del 12 luglio 2024 (da ora in avanti Ai Act).

Nel Regolamento di Esecuzione 2019/947/UE del 24 maggio 2019 relativo a norme e procedure operative per l'impiego di aeromobili senza pilota, in vigore dal 31.12.2020, all'art. 3 le operazioni sono suddivise in tre categorie, in base al rischio. Questa classificazione deriva dal precedente Regolamento 2018/1139/UE del 04 luglio 2018. Questo articolo definisce e suddivide le operazioni in tre categorie, ovvero <<*open*>>, <<*specific*>> e <<*certified*>>.

In categoria *Open* è possibile trovare i seguenti UAS:

- Da C0 a C4 contrassegnati dall'etichetta di identificazione della classe;
- senza etichetta o commercializzato prima del 31/12/2023;
- autocostruiti (per uso personale);
- Con un peso massimo al decollo non superiore a 25 kg;
- Conformi ai requisiti tecnici stabiliti dal Regolamento 2019/945/UE.

Per tali dispositivi è richiesta la registrazione dell'operatore su D-flight, l'attestato di pilota, con esclusione dei mezzi di peso inferiore a 25 kg e l'obbligo di copertura assicurativa. L'altezza massima di volo è di 120 metri e sono tenuti a volare in linea visiva (VLOS), ovvero devono mantenere una linea visiva tra il drone e il pilota remoto, con divieto assoluto di volo su assembramenti di persone, trasporto di merci pericolose e rilascio di materiali e sostanze. Si suddividono in ulteriori sottocategorie: A1, A2, A3. Per la classe A1 è richiesta la registrazione dell'operatore quando il drone è in grado di acquisire dati personali.

La categoria <<*specific*>> si riferisce invece a:

- operazioni con droni che non rientrano nella precedente categoria *Open*;
- operazioni che si svolgono su scenari standard nazionali o definiti dall'Easa, con decorrenza dal 01/01/2024.

Per questa categoria è richiesta la registrazione su D. Flight degli operatori e l'autorizzazione operativa (ENAC) se sorvolano su scenari non standard.

Le categorie sono suddivise in sottocategorie, rilevanti soprattutto ai fini dell'addestramento dei piloti e della registrazione degli operatori, obblighi sempre presenti, ad eccezione della sottocategoria A1 *open*, che è suggerita nel primo caso, obbligatoria nel secondo, quando il drone è in grado di raccogliere dati personali.

Dal 1° gennaio 2024, per immettere un UAS sul mercato europeo, è obbligatoria la dichiarazione di rispondenza al Reg. 2019/945/UE.

Qualsiasi drone immesso sul mercato prima del 1° gennaio 2024 privo di etichetta di classe è considerato un cosiddetto drone <<*legacy*>>, ovvero può continuare a operare nella sottocategoria *Open* A1 se ha una massa massima al decollo inferiore a 250 grammi, incluso il carico utile, o nella

sottocategoria A3 a condizione che abbia una massa massima al decollo inferiore a 25 kg, inclusi carburante e carico utile. Ai droni non classificati e immessi sul mercato dopo il 1° gennaio 2024 è vietato l'uso in categoria *Open* se non soddisfano i requisiti di cui sopra e possono volare solo in categoria *Specific*.

La categoria <<*certified*>> presenta il rischio più elevato e pertanto necessita di requisiti e condizioni di sicurezza più stringenti, per garantire elevati livelli di sicurezza. Il loro impiego richiede la certificazione del drone e dell'operatore e l'autorizzazione del pilota remoto quando l'operazione avviene su assembramenti di persone e comporta il trasporto di persone, merci pericolose o quando le dimensioni del drone sono superiori a tre metri. Questa tipologia di droni interessa i futuri modelli di sviluppo della mobilità e del trasporto, denominati Mobilità Aerea Innovativa (IAM) e Mobilità Aerea Internazionale, Regionale e Urbana (UAM).

2. Stato dell'arte. La marcia dei droni nella normativa nazionale, internazionale e dell'UE. Intersezioni giuridiche con Ai Act.

Gli UAS, chiamati profanamente droni, sono di diversi tipi in termini di forma, dimensioni e peso[12].

Dall'esame della dottrina emerge che, anche se i veicoli senza pilota hanno una tecnologia separata da altre classi di robot[13], essi fanno comunque parte del più ampio genere della robotica[14], che consiste genericamente in robot a braccio articolato, robot umanoidi e robot sociali, veicoli senza pilota, che si

[12] G. LA CAVA, A. MAROTTA, F. MARTINELLI, A. SARACINO, A. LA MARRA, *Cybersecurity issues in robotics*, in *Journal of wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (Jowua)*, 2021, 12, 3, 1-28. Consultabile in https://jowua.com/article/jowua-v12n3-1/70941/

[13] *Unmanned aerial vehicles:implications for occupational safety and health*, in Https://osha.europa.eu·

[14] L. MERLA, *Droni privacy, e tutela dei dati personali,* in *Inf. e Dir.*, 2016, 1, 29. Sul punto vedi anche Https://osha.europa.eu, *Unmanned aerial vehicles: implications for occupational safety and health*, per cui <<UAVS are a class of devices including multirotor drones, as well as single-rotor and fixed-wing devices, hybrid versions, and, potentially, alternative propulsion systems. The common characteristic of these devices is that they are all able to move, with or without a load of some type, in the same (work)space inhabited by humans. In a simplistic view, UAVS are robots that can "fly" and "From all UAV types, drones are, unquestionably, the fastest growing class (both in sheer numbers and capabilities). Therefore, the term is often used for the full class of UAVS. As of May 2022, the FAA acknowledged 865,000 registered drones in the United States, including commercial and recreational, with an estimated annual increase of approximately 6.4%. In Europe, the annual increase is estimated between 5.3% and 6.3%, with an acceleration trend (from data available in Molina & Oña, 2017). In both markets, military applications represent the biggest value>>; in dottrina G.N. LA DIEGA, *Machine rules of drones. Robots, and the info-capitalist Society,* in *ILJ, 2016*, 2, 367, secondo cui (…) <<indeed, most considerations apply equally to robots and drones, moving from the unrefined, albeit practical, observation that the latter are robots equipped with wings>>.

suddividono in veicoli terrestri, UGV e altri robot terrestri, veicoli subacquei (UUVS) e aerei (UAS)[15].

Ciò che è importante, tuttavia, è la differenza tra velivoli autonomi e velivoli a pilotaggio remoto, vale a dire <<*autonomous aircraft*>> (SAPR) in cui non c'è la presenza umana e in cui il volo è totalmente guidato dal software, e velivoli a pilotaggio remoto (APR), in cui c'è un pilota ma opera da una stazione remota, cd. <<*unmanned aircraft*>>.

Il Regolamento ENAC del 16 luglio 2015 ha unito queste due tipologie, ovvero il SAPR in cui non c'è un pilota, ma un software, che è assorbente dell'APR, in cui invece c'è un pilota, seppure da remoto[16].

Entrambe le tipologie sono state considerate, ad ogni modo, aeromobili ai sensi della Convenzione di Chicago sull'Aviazione Civile Internazionale del 1944, a cui fa riferimento l'articolo 743 del Codice della Navigazione italiano, che fonda la qualificazione di aeromobile su un vincolo di destinazione conferito dall'uomo o da disposizioni di legge e di regolamento[17].

In base a questa definizione, ne consegue che a tutti i droni, ad eccezione dei droni giocattolo, cioè dei droni conformi alla Direttiva Giocattoli 2009/48/CE[18], si applica la Convenzione di Chicago del 1944 sul trasporto aereo internazionale.

L'assimilazione è intervenuta, sulla base del Regolamento 2018/1139/UE del 04 luglio 2018, recante norme comuni per l'aviazione civile e la sicurezza dell'aviazione, seguito dagli atti di esecuzione 945 - Nuovo Quadro Normativo Europeo - e 947, che ha recepito la qualifica di UAS[19], che sostituisce quella di SAPR, fino ad allora in uso nella legislazione.

Il Regolamento 2018/1139/UE, che stabilisce norme comuni nel settore dell'aviazione civile, certamente applicabili anche ai droni senza equipaggio (C. n. 26), è partito dal presupposto che anche i droni di peso inferiore ai 25 kg siano potenzialmente in grado di arrecare danni a persone e cose in superficie e, soprattutto, costituiscano un pericolo quando acquisiscono e trattano dati personali.

Esso si propone, pertanto, di stabilire i principi fondamentali per garantire la sicurezza, la privacy e la protezione dei dati personali, introducendo alcuni

---

[15] C. SEVERONI, *Il regime di responsabilità per l'esercizio dei mezzi a pilotaggio remoto*, in *Diritto dei droni: regole, questioni e prassi, op. cit.*, 81.

[16] Regolamento ENAC sui velivoli a pilotaggio remoto del 17 luglio 2015, disponibile all'indirizzo <www.enac.gov.it>, consultato il 10 settembre 2023.

[17] << Il vincolo di destinazione>> è quello previsto dall'articolo 743 del Codice della Navigazione, che al primo comma dispone: <<Per aeromobile si intende qualsiasi macchina destinata al trasporto aereo di persone o cose>> al 2° co) aggiunge che sono altresì considerati aeromobili i mezzi aerei a pilotaggio remoto, definiti tali da leggi speciali, da Regolamenti ENAC e, per quelli militari, dai Decreti del Ministero della Difesa>>.

[18] Art. 1, 4° co)) del Regolamento Enac.

[19] L'art. 2 del Reg. 2019/947/UE, applica le definizioni del Reg. 2018/1139/Ue, tra le quali, al 1° co), punto 1), <<i sistemi di aeromobili senza equipaggio (UAS): un aeromobile senza equipaggio e i suoi dispositivi di controllo remoto>>.

requisiti di base (artt. 55 ss) e un iter burocratico preciso, fondato su un sistema comune di certificazione.

Tutti i tipi di droni risultano in tal modo integrati, indipendentemente dal peso e dalle dimensioni, nel quadro della sicurezza aerea comune dell'Easa.

Viene, in tal modo, attuata la Convenzione di Riga del 6 marzo 2015, secondo cui i droni devono essere trattati come un nuovo tipo di aeromobile, <<*Drones need to be treated as a new type of aircraft*>>. Tale importante atto, seppure di *soft law*, detta i punti chiave per la futura regolamentazione dei droni per uso civile, compresa la tutela della privacy, equipara i droni con equipaggio a quelli senza equipaggio, stabilisce che le norme di sicurezza devono essere commisurate al rischio "concreto" di ogni singola operazione[20].

Con il pretesto della privacy, viene superato il criterio del peso ed emergono ulteriori elementi, ai fini della configurazione della responsabilità, quali ad es. i rischi connessi all'attività, come quella relativa al trattamento dei dati personali.

Il recente Regolamento 2024/1689/UE, del Parlamento Europeo e del Consiglio, che stabilisce regole armonizzate sull'intelligenza artificiale, non cambia molto il quadro regolatorio e si limita a modificare e integrare il Reg. 2018/1139/UE.

Il Regolamento del Parlamento Europeo e del Consiglio, che istituisce un quadro comune di regole sull'ia, all'art. 2, nella prima versione, recitava <<*For ai systems classified as high-risk AI systems in accordance with Articles 6, para 1 and 6, para 2, related to products covered by Union harmonisation legislation listed in annex II, section B only article 84 of this Regulation shall apply. Article 53 shall apply only insofar as the requirements for high-risk AI systems under this Regulation have been integrated under that Union harmonisation legislation*>>.

L'attuale versione del Regolamento, approvata il 13 giugno 2024, classifica i droni come sistemi di intelligenza artificiale ad alto rischio. Conferma che ad essi si applicano solo alcune disposizioni, tra cui l'art. 57, che disciplina gli spazi di sperimentazione normativa (cd. sandbox), limitatamente ai casi in cui i requisiti per i sistemi di intelligenza artificiale ad alto rischio, ai sensi del Regolamento, risultano incorporati nella legislazione di armonizzazione dell'Unione[21].

Ai sensi dell'art. 6, 1° co), un sistema di ia viene considerato ad alto rischio se sono soddisfatti due requisiti, ossia se è destinato a essere utilizzato come

[20] T. PAPADEMETRIO, *Regulation of Drones: European Union* (Report April 2016 USA, the Law Library of Congress, Global Legal Research Directorate), disponibile all'indirizzo < http://www.law.gov> consultato il 30 settembre 2022.

[21] Cfr. l'art. 108 Ai Act, che invita a tenere conto dei requisiti di cui al capo III, sezione 2, dello stesso Regolamento.

componente di sicurezza di un prodotto o è esso stesso un prodotto disciplinato dalla normativa di armonizzazione dell'Unione elencata nell''allegato I, e al contempo il prodotto, il cui componente di sicurezza ai sensi della lettera a) è il sistema di ia o il sistema di ia stesso in quanto prodotto, è soggetto a una valutazione di conformità da parte di terzi ai fini dell'immissione dello stesso sul mercato o della sua messa in servizio, ai sensi della normativa di cui all'allegato I, riconducibile al Regolamento 2018/1139/UE(UE).

Dall'analisi sistematica delle disposizioni emerge che l'Ai Act ha un approccio evidentemente orientato al prodotto[22]. In tale prospettiva oltre a richiedere specifici requisiti certificati, ai fini dell'immissione sul mercato, esso condivide con il GDPR e con il Regolamento 2018/1139/UE, che unifica la materia, i principi della *privacy e sicurezza by design*, l'importanza della certificazione, la valutazione e misurazione del rischio nonché l'adozione degli strumenti di mitigazione.

La mancanza di sicurezza, dovuta all'assenza di idonei meccanismi di protezione contro gli attacchi informatici, potrebbe per es. integrare un'ipotesi di responsabilità per omissione nella progettazione di determinati elementi a presidio della cybersicurezza, classificabili come difetto del prodotto[23].

Le statistiche evidenziano, a tale proposito, incidenti a persone e atti di pirateria informatica, che coinvolgono, principalmente, droni che volano su distanze elevate (BVLOS)[24].

I droni raccolgono informazioni, le trasmettono e possono essere connessi a Internet, introducendo il tema dell'Internet of Drones (IOD); sono prodotti che consistono anche in una componente software che spesso è collegata o coinvolge il cloud, in grado di costituire un pericolo non solo per la privacy, ma anche per la protezione dei dati[25].

L'adozione di comportamenti proattivi, riconducibili al concetto di *privacy e security by design* e, soprattutto, la capacità di prevedere le potenziali minacce, sono aspetti importanti nella progettazione del software[26], che consentono di evitare (seppure il rischio 0 non esista) possibili attacchi o incidenti interni all'impresa, con la configurazione di profili di

---

[22] Questa caratteristica dell'AI Act è emersa anche in un convegno, organizzato dalla Fondazione Cesifin, *Persona, dati personali, algoritmi, tra GDPR e AI Act* (17 giugno 2024 Firenze). Si veda l'intervento del Prof. S. Orlando *Decisioni algoritmiche, diritto di spiegazione e tutela dei consumatori.*

[23] G. CAPILLI, *I criteri di interpretazione delle responsabilità* in *Diritto e Intelligenza artificiale,* a cura di G. ALPA, Pisa, *2020,* 485.

[24] Agenzia europea per la sicurezza e la salute sul lavoro, *Unmanned aerial vehicles: implications for occupational safety and health,* 2023, disponibile all'indirizzo https://osha.europa.eu>, consultato il 05 novembre 2023.

[25] D. RAGUSEO, R. GALIANDRO, G. MARULLO e A. DE CHIRICO, *Cybersecurity for Drones.* disponibile all'indirizzo www.ict security magazine.com, consultato il 10 novembre 2023.

[26] G. SIMEONE, *Machine learning e tutela della privacy alla luce del GDPR*, in *Diritto e intelligenza artificiale*, a cura di G. ALPA, Pisa, 2020, 288 ss.

responsabilità[27], originati dall'omessa valutazione di tali situazioni, oltre che di scongiurare impatti psicosociali rilevanti[28].

3. Droni e contesti operativi. Scenari attuali e futuri.

L'Agenzia Europea per la Sicurezza e la Salute sul Lavoro ha condotto uno studio, denominato <<*Drones inspecting worksites of gas infrastructure operators (ID 16)*>>, dal quale emerge che un numero crescente di aziende sta utilizzando l'intelligenza artificiale o la robotica avanzata nei contesti di lavoro, per ragioni connesse all'efficientamento dell'organizzazione e della produzione e per garantire, altresì, una maggiore sicurezza dei lavoratori, riducendo le mansioni noiose, ripetitive e pericolose[29].

Questi obiettivi, tuttavia, devono conciliarsi con la tutela dei diritti fondamentali, primo fra tutti quello della privacy e della protezione dei dati.

I *case study* esaminati di seguito riguardano l'impiego di droni per ispezionare in sicurezza i cantieri e le infrastrutture del gas, i droni per l'efficientamento della logistica di magazzino, i droni per la sorveglianza delle aree urbane.

Droni per la sorveglianza dei gasdotti: In Norvegia ci sono interessanti esperienze di impiego di droni per la manutenzione e la sorveglianza delle infrastrutture del gas, situate in superficie ed esposte ad agenti atmosferici. L'impiego dei droni, supportato da sistemi di intelligenza artificiale, è utile per ridurre al minimo i rischi per i lavoratori, costretti a spostarsi su diverse altezze e su più cantieri. I droni sorvolano aree molto vaste per sorvegliare i siti, semplificando la supervisione e la manutenzione; sono supportati da telecamere e algoritmi, alla ricerca di ostacoli e pericoli specifici.

Il sistema di ispezione visiva si basa su un software di back-end alimentata da intelligenza artificiale, che svolge un compito cognitivo e informativo per gli addetti alla raccolta, che si limitano a eseguire ciò che emerge dall'analisi del drone (recupero e rimozione di oggetti caduti, interventi di riparazione).

L'impiego di questi dispositivi contribuisce in modo significativo al miglioramento della sicurezza sul lavoro e assume rilievo anche sul piano psicosociale, perché favorisce l'accettazione dell'innovazione digitale in impresa, connessa alla percezione dell'utilità di questi strumenti e all'interazione instaurabile con gli stessi se supportata da adeguati piani

[27] G. ALPA, *Manuale di diritto privato, Vicenza,* 2020, 916.
[28] Agenzia Europea per la Sicurezza e la Salute sul Lavoro, *Unmanned aerial vehicles: implications for occupational safety and health*, 2023, disponibile all'indirizzo https://osha.europa.eu, consultato il 05 novembre 2023.
[29] Agenzia Europea per la Sicurezza e la Salute sul Lavoro, *Drones inspecting worksites of gas infrastructure (ID 16)*, 2023, disponibile all'indirizzo http://osha.europa.eu, consultato il 15 settembre 2023.

formativi[30].

Ciò contribuisce all'incremento delle competenze, al rafforzamento dell'autostima e della fiducia nei confronti dell'impresa, dovute al miglioramento complessivo del clima aziendale.

La dimensione spaziale e temporale del lavoro andrà incontro ad un progressivo sviluppo e risulterà efficientata, soprattutto se tale processo sarà accompagnato da una riconsiderazione del tempo, inteso come orario di lavoro[31].

Droni Verity: Ikea è il primo rivenditore a utilizzare i droni Verity per i controlli notturni delle scorte, garantendo la disponibilità dei prodotti online e in negozio.

L'impiego dei droni migliora l'accuratezza e i livelli di conformità dell'inventario perché implementano la produttività e riducono i costi di manodopera per la gestione del magazzino. Sono in grado di rilevare un errore prima che possa trasformarsi in un vizio di sistema. Con i droni si introducono sistemi di automazione del lavoro che, pur essendo ripetitivi, presentano elementi di dinamicità, quali la possibilità di esaminare in modo critico i processi di lavoro.

Gli operatori di magazzino sono in grado di rilevare gli errori in anticipo, utilizzando le immagini catturate dai droni. Il responsabile dell'inventario esamina il report, presente nel verity cloud, in una fase antecedente all'inizio del primo turno di lavoro, individuando gli errori da correggere insieme al resto del personale. I compiti ripetitivi e noiosi, come i frequenti conteggi dei cicli, sono notevolmente ridotti. I droni vengono rilasciati di notte e sono integrati da sensori di visione notturna a raggi infrarossi. Esaminano i pallet movimentati nelle ultime 24 ore e i dati raccolti vengono utilizzati per fornire un feedback ai lavoratori e migliorare processi produttivi.

L'implementazione di processi di automazione in azienda, attraverso sistemi di sorveglianza e ia, in questo caso, aumenta la motivazione dei dipendenti e velocizza i processi produttivi, contribuisce a un maggiore coinvolgimento di tutti nell'organizzazione del lavoro e responsabilizza i supervisori[32].

Droni per la sorveglianza delle aree urbane: sono utilizzati per le attività di indagine, compiti di polizia ambientale e edilizia, sorveglianza di edifici pubblici o di interesse pubblico, rilievo di incidenti stradali e monitoraggio del traffico, operazioni di *safety e security* in occasione di eventi pubblici, attività di protezione civile, prevenzione e contrasto dei reati in materia di

[30] T. TREU, *La digitalizzazione del lavoro: proposte europee e piste di ricerca*, 2022, in *Diritto delle Relazioni Industriali,* 1, 32, 17.
[31] A.M. PONZELLINI, *Tecnologie, fine della presenza e dilemmi del controllo nei nuovi pattern spazio-temporali del lavoro*, in *Economia & Lavoro*, 2020, 1, 89 ss.
[32] Verity, *Maximizing value. Client success stories in harnessing Verity's benefits*, *2023,* disponibile su http://www.verity.net.

stupefacenti, soccorso e ricerca di persone scomparse in aree difficilmente raggiungibili.

Durante queste operazioni, è molto facile violare la *privacy* sia degli operatori che utilizzano il dispositivo sia delle persone che vengono riprese.

Molti comuni italiani hanno previsto, nel Regolamento di Polizia Municipale, l'impiego dei droni e per farlo sono state necessarie alcune attività propedeutiche, inerenti all'attuazione del principio di *accountability*[33].

Su tale presupposto il titolare del trattamento mette in atto tutte le misure tecniche e organizzative fin dalle prime fasi di progettazione[34].

Una delle misure più importanti è quella relativa all'espletamento della DPIA, la cui predisposizione avviene già prima del capitolato per l'acquisto di strumenti hardware e software[35].

La DPIA è una delle declinazioni più importanti del principio di *accountability,* perché anticipa la tutela dei diritti e delle libertà degli interessati e riguarda anche il tipo di strumenti che verranno utilizzati[36].

In tutte le casistiche considerate, la DPIA è necessaria, per via dell'uso innovativo o dell'applicazione di nuove soluzioni tecnologiche o organizzative[37], nonché per via della presenza di almeno due dei prerequisiti indicati nell'elenco di cui al WP 29, consistenti nel monitoraggio sistematico su larga scala di aree accessibili al pubblico e nel trattamento dei dati personali dell'operatore e/o dei dipendenti (es. file di log o dati di navigazione tracciati per motivi di sicurezza) che usano i dispositivi per lo svolgimento delle proprie mansioni, in grado di produrre output predittivi e valutativi, trattamenti automatizzati, compresa la profilazione[38].

---

[33] D.L. 20 febbraio 2017, n. 14, art. 5, 2° co), lett. a. Per un approfondimento si veda, inoltre, GPDP, Provv. n. 234, dell'11 aprile 2024, disponibile su https://www.garanteprivacy.it, consultato nel maggio 2024. In dottrina M. BARBAROSSA, C. BENVENUTO, V. CEROCCHI, *La responsabilità civile e danno da trattamento illecito dei dati alla luce del Regolamento UE 2016/679*, in *Il processo di adeguamento al GDPR*, a cura di G. CASSANO, V. COLAROCCO, G.B. GALLUS, F.P. MICOZZI, Milano, 2018, 370 ss.

[34] L. BOLOGNINI e E. PELINO, *Codice della disciplina privacy,* Vicenza, 2019, 201. A. BERNES, *Dalla responsabilità civile alla responsabilità sociale d'impresa nella protezione dei dati personali: alla ricerca del rimedio effettivo*, in *Actualidad Juridica Iberoamericana*, 2023, 18, 666.

[35] Cfr. C. 75 e 78, nonché art. 35 3° co) GDPR e Linee guida WP 248 rev. 01, GDPD, Provv. n. 467, dell'11 ottobre 2018, disponibile in https://www.garanteprivacy.it, consultato in data 10 gennaio 2019 e in https://www.ec.europa.eu, consultato l'11 gennaio 2024.

[36] I rischi si riferiscono ai diritti e alle libertà degli interessati (cfr. art. 35, comma 7, lett. c)); il C. 90 riguarda le fonti di rischio; il C. 84 specifica la valutazione e la gestione dei rischi del trattamento sia in ambito informatico che organizzativo. La DPIA deve essere effettuata in relazione a ciascuno degli elementi descritti nell'articolo 35, comma 7), in relazione a ciascun trattamento/strumento impiegato. Tra questi, la protezione dei dati (anche dei dipendenti) è molto importante. Cfr. G. SIMEONE, *Machine learning e tutela della privacy alla luce del GDPR*, in *Diritto e intelligenza artificiale*, *op. cit.*, 288.

[37] Cfr. art. 35, 1° co), Reg. 2016/679/UE.

[38] Si veda anche il Provv. GPDP n. 5, dell'11 gennaio 2024, disponibile all'indirizzo https://www.garanteprivacy.it, consultato il 10 marzo 2024.

4. Droni e potere di controllo del datore di lavoro tra Gdpr e Statuto dei Diritti dei Lavoratori, come modificato dal D.lgs 151/2015 del 23 settembre 2015, attuativo del cd. Jobs Act.

L'art. 23 del D.lgs 151/2015, ha modificato, *a contrario,* la disciplina in materia di controlli a distanza dei lavoratori, originariamente regolata dallo Statuto dei Lavoratori ossia è venuto meno il divieto generale di impiego di impianti per finalità di controllo a distanza, sostituito da una disciplina, che consente l'impiego di tali strumenti, in determinate circostanze, quali quelle dovute a esigenze organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale e sempre che siano accompagnati dalla stipulazione di accordi sindacali.

Il legislatore, inoltre, ha introdotto un'eccezione, ammettendo l'uso di strumenti necessari per rilevare la presenza in servizio e consentire la prestazione lavorativa. Riconoscendo, inoltre, come certi dispositivi siano ormai imprescindibili per lo svolgimento della prestazione lavorativa, ha previsto per essi una disciplina specifica, esonerandoli dagli obblighi di cui all'art. 4, 1° co)[39].

In tale ambito, l'attenzione del legislatore non si è rivolta al divieto di utilizzo, bensì alla definizione dei limiti inerenti all'impiego dei dati raccolti.

La vaghezza dell'espressione <<strumenti di lavoro>>, che non trova una precisa corrispondenza sul piano semantico e normativo, lascia spazio all'interprete e apre alla configurazione di diversi orientamenti.

Il primo che riconduce alla nozione di strumenti di lavoro i dispositivi assegnati al lavoratore per esigenze organizzative e direttamente utilizzati da quest'ultimo non solo per lo svolgimento della prestazione lavorativa, ma anche per efficientare la stessa[40], ritenendo, al contrario, doversi escludere tutti gli altri, quali il dispositivo o il programma software, quando non risultano funzionali a tutto questo e hanno invece esclusive finalità di controllo.

Il secondo orientamento, invece, è quello secondo cui il software consente il funzionamento dei dispositivi e la conservazione massiva dei dati in

---

[39] A. PRETEROTI, *Divieto di controllo a distanza e telelavoro (commento all'art. 114)*, in Aa.Vv., *La protezione dei dati personali. Commentario al D. lgs. 30 giugno 2003, 196 («Codice della Privacy»)*, a cura di C.M. BIANCA, F.D. BUSNELLI, Tomo II, Padova, 2007, 1478 (..).

[40] Cfr. C. PISANI, *Gli strumenti utilizzati per rendere la prestazione lavorativa e quelli di registrazione degli accessi e delle presenze*, in AA.VV., *Privacy e lavoro la circolazione dei dati personali e i controlli nel rapporto di lavoro,* a cura di C. PISANI, G. PROIA e A. TOPO, Milano, 2022, 445 ss; in giurisprudenza si veda la recente decisione di Cass. Civ., 03 giugno 2024, n. 15391, disponibile su <https://www.dirittoegiustizia.it>, accesso 8 giugno 2024, per cui se installato sulle vetture aziendali destinate all'esecuzione di specifici servizi, il telepass deve essere considerato uno strumento direttamente funzionale all'efficienza della prestazione individuale, oltre che ormai fortemente compenetrato con essa nell'odierna prassi lavorativa.

transito dei lavoratori ed è in grado di trasformare quest'ultimi in strumenti di controllo a distanza. Conseguentemente, i dispositivi possono essere considerati strumenti di lavoro e rientrare nel regime agevolato di cui al comma 2), solo a condizione che siano coessenziali e indispensabili per rendere la prestazione lavorativa, ritenendo, al contrario, doversi escludere il regime di eccezione nel caso in cui la prestazione possa, comunque, essere resa anche senza l'uso di tali strumenti[41].

Quest'ultimo orientamento è confermato dall'art. 15 della Raccomandazione CM/Rec (2015) 5 del 1° aprile 2015 del Comitato dei Ministri agli Stati membri sul trattamento dei dati personali nel contesto occupazionale, che ribadisce la necessaria partecipazione delle organizzazioni sindacali alle scelte datoriali in merito all'installazione e all'utilizzo di dispositivi elettronici di controllo e sorveglianza (in qualsiasi forma questo avvenga), che restano ipotesi ultima da prendere in considerazione, per il raggiungimento degli obiettivi di natura organizzativa[42].

In generale, ogni strumentazione tecnica, inclusi, ma non solo, i sistemi di videosorveglianza, che comporti o possa comportare il trattamento di dati personali o che sia potenzialmente in grado di farlo, raccogliendo e utilizzando informazioni sui dipendenti tali da identificarli o renderli identificabili[43], è idoneo a trasformarsi in un controllo diretto e indiretto[44].

I droni, quando sono dotati di telecamere o sensori, consentono, in linea teorica, di registrare i movimenti e sono in grado di catturare immagini a terra con un alto livello di precisione, grazie alla loro discrezione e versatilità. Lo zoom facilita il tracciamento delle persone fisiche. Questo significa che da strumenti di lavoro[45] utilizzabili, tra l'altro, in un'ottica difensiva del patrimonio aziendale, ma anche della salute e dell'integrità psico-fisica dei dipendenti, possono trasformarsi in strumenti di controllo diretto e indiretto

---

[41] Si veda G.M. RICCIO, G. SCORZA e E. BELISARIO, *op. cit.*, 914.

[42] Cfr. CM/Rec (2015) 5, del 01 aprile 2015, disponibile all'indirizzo https://www.garanteprivacy.it, consultato il 5 novembre 2024.

[43] Art. 4, 1° co), e art. 2 del Gdpr.

[44] Cass. Civ., sent. 06/03/1986, n. 1490, in Arch. Civ., 1986, 155 per cui ciò che rileva è l'installazione dell'impianto, da cui può derivare un controllo a distanza dei lavoratori, pur in assenza di attivazione dello stesso, tale da richiedere il consenso del sindacato o dell'ispettorato del lavoro, gli unici in grado di valutare l'idoneità degli strumenti a ledere la dignità dei lavoratori e l'effettiva rispondenza degli stessi alle esigenze tecnico produttive anche con riferimento ad uno strumento diverso dalla videosorveglianza; si veda anche Cass. Pen., 15/07/2019, n. 50919, in https://Foroplus.it, accesso del 5 maggio 2024, per la quale la violazione della procedura di garanzia di cui all'art. 4, a tutela di interessi di natura collettiva e superindividuale, è utilizzata per valutare l'idoneità dello strumento a ledere la dignità dei lavoratori e l'effettiva rispondenza dello stesso alle esigenze tecniche di produzione e sicurezza. Nello stesso senso si veda Cass. Pen., 30/01/2014, n. 4331, per la quale <<c'è violazione dell'art. 4.1 n. 300/1970 anche se l'impianto non è messo in funzione: poiché il bene giuridico protetto è la riservatezza dei lavoratori e il reato in questione si configura come un reato di pericolo, la norma sanziona a priori l'installazione, prescindendo dal suo utilizzo o meno*>>*, citata in L. BOLOGNINI e E. PELINO, *op. cit.,* 1385.

[45] G. DONZELLI, *L'interazione uomo macchina tra tecnologie digitali e successo industriale*, in *Diritto e Intelligenza artificiale, op. cit.*, 98.

della prestazione. Diretto per via dell'uso di tecnologie di sorveglianza (zoom, videocamere, sensori, ecc.), indiretto per via della raccolta, del rilevamento, dell'archiviazione, dell'elaborazione e dell'esame dei dati utilizzabili a fini di analisi predittive, valutative, di profilazione di abitudini e comportamenti.

Il loro impiego, nei casi sopra citati, potrebbe comportare il passaggio da mero rilevatore di presenza a strumento di controllo[46], per via della raccolta e del trattamento, che avviene in un lasso di tempo prolungato e continuo, che resta disciplinato dalla contrattazione con i rappresentanti dei lavoratori[47].

L'accesso al regime agevolato, è stato recentemente oggetto di un Provvedimento dell'Autorità Garante della Protezione dei Dati Personali, che ha risolto un caso analogo sulla base del criterio del tempo di conservazione dei log di posta elettronica, che non può superare i 21 giorni; in caso contrario essi potrebbero comportare un controllo indiretto a distanza dei lavoratori e quindi essere inquadrati ai sensi del 1° co) dell'art. 4 dello Statuto, in quanto potenzialmente idonei a raccogliere anche informazioni attinenti alla sfera personale o alle opinioni dell'interessato e quindi irrilevanti ai fini dello svolgimento dell'attività lavorativa.

Il trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro, se necessario ai fini della gestione del rapporto stesso[48] deve, inoltre, svolgersi nell'osservanza dei principi di cui all'art. 5 del GDPR e in particolare del principio di liceità, secondo cui il trattamento è lecito solo se conforme alle discipline di settore applicabili[49].

I requisiti di liceità previsti dalla normativa di settore sono quelli stabiliti dall'art. 4 L. 20 maggio 1970, n. 300, richiamato dagli artt. 113 e 114 del Codice Privacy[50]. Tali disposizioni recano tutele più specifiche rispetto all'art. 88 GDPR[51].

Infine, l'art. 4, 3° co), introduce ulteriori profili di illiceità in caso di ulteriore utilizzo dei dati personali raccolti[52].

---

[46] Sul punto si veda anche la Raccomandazione del Consiglio d'Europa del 1° aprile 2015 CM/Rec (2015) 5 che vieta i controlli prolungati, costanti e indiscriminati, disponibile su https://www.garanteprivacy.it, consultato il 20 maggio 2020.

[47] Art. 4, 1° co), Statuto dei Diritti dei Lavoratori.

[48] Art. 6, 1° co), lett. b) e c) e art. 9, 2° co), lett. b).

[49] Art. 5, 1° co), lett.a).

[50] A. PRETEROTI, ***Divieto di controllo a distanza e telelavoro*** *(commento all'art. 114)*, in Aa.Vv., *La protezione dei dati personali. Commentario al D. lgs. 30 giugno 2003, 196 («Codice della Privacy»)*, a cura di C.M. BIANCA, F.D. BUSNELLI, Tomo II, Padova, 2007, 1476 (..).

[51] Cfr. GPDP, Provv. n. 364 del 06 giugno 2024, disponibile su https://www.garanteprivacy.it, accesso 10 giugno 2024.

[52] Ai sensi del dell'art. 4, 3° co), dello Statuto come modificato dall'art. 23 del D.Lgs. 151/2015, <<le informazioni raccolte ai sensi dei commi 1 e 2 possono essere utilizzate per tutte le finalità connesse al rapporto di lavoro a condizione che al lavoratore sia data adeguata informazione sulle modalità di utilizzo degli strumenti e di svolgimento dei controlli e nel rispetto delle disposizioni di cui al Decreto Legislativo 30 giugno 2003, n. 196>>.

Il trattamento dei dati in questi casi deve essere accompagnato da un adeguato livello di correttezza e trasparenza nei confronti dei dipendenti, che devono essere stati adeguatamente informati[53].

Nel caso di sistemi di videosorveglianza, l'informativa di primo livello (finalità, titolare del trattamento, diritti dell'interessato, tempi di conservazione dei dati, modalità di trattamento dei dati, ecc.), deve essere, inoltre, accompagnata da un'informativa di secondo livello, a cui la prima farà esplicito riferimento, in modo da fornire agli interessati i mezzi per consultare l'informativa nella sua interezza e deve contenere, inoltre, tutti gli altri elementi indicati nell'art. 13 del Regolamento[54].

Il riferimento è rivolto, quindi non solo al GDPR, ma anche alle normative di settore applicabili[55], in modo da garantire un equo bilanciamento tra gli interessi economico-organizzativi del datore di lavoro e il diritto alla privacy dell'interessato lavoratore.

L'art. 88 del GDPR da un lato, ha fatto salve le norme nazionali di maggior tutela (le norme specifiche) volte a garantire la tutela dei diritti e delle libertà in materia di trattamento dei dati personali dei lavoratori, come l'art. 23 del D.lgs. n. 151/2015 (già art. 4 della legge n. 300 del 1970), dall'altro, però, ha aperto la possibilità di demandare ai contratti collettivi (anche integrativi, Cfr. C. 155), la disciplina, in modo da superare la distinzione di cui ai commi 1 e 2, purché più specifica e più tutelante per i lavoratori[56].

Nell'ordinamento interno, inoltre, la specifica disposizione di cui all'art. 114 del D.lgs n. 196/2003 del 30 giugno 2003, Codice della Privacy, tra le condizioni di liceità del trattamento, ha stabilito il rispetto di quanto previsto dall'art. 4 della Legge n. 300 del 1970, in base al quale se dai sistemi di videosorveglianza può derivare anche solo la possibilità di controllo a distanza dei dipendenti, gli stessi possono essere utilizzati solo per scopi legati alla produzione e all'organizzazione, per la sicurezza del lavoro e dei beni dell'azienda. La relativa installazione deve avvenire previo accordo collettivo con le rappresentanze sindacali unitarie o aziendali o con l'autorizzazione dell'ispettorato del lavoro, costituendo una condizione senza l'osservanza della quale non è possibile l'installazione di sistemi di videosorveglianza[57].

---

[53] Art. 5, 1° co), lett. a) e artt. 12, 13, 14 GDPR.
[54] Provv. GPDP 08 aprile 2010, n. 1712680, che richiama le Linee Guida n. 3/2019 EDPB sul trattamento dei dati personali mediante dispositivi video.
[55] Art. 5, 1° co), lett. a)).
[56] S. CIUCCIOVINO, *Art. 88 commento*, in AA.VV., *Codice della privacy e data protection,* a cura di R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO e F. RESTA, Milano, 2021, 948 ss.
[57] Cfr. in tal senso l'ampio esame in GPDP, Provv. N. 58, del 02 marzo 2023, disponibile all'indirizzo https://www.garanteprivacy.it, consultato il 5 novembre 2024; in dottrina cfr. A. PRETEROTI, *Divieto di controllo a distanza e telelavoro (commento all'art. 114)*, in Aa.Vv., *La protezione dei dati personali. Commentario al D. lgs. 30 giugno 2003, 196 («Codice della Privacy»)*, a cura di C.M. BIANCA, F.D. BUSNELLI, Tomo II, Padova, 2007, 1479 (..).

Esistono, quindi, diversi e autonomi livelli di garanzia, costituiti in primis dal Codice della Privacy nonché dall'art. 4 della L. 300/1970 a cui l'art. 88 rinvia, in combinato disposto con gli artt. 5 e 6 GDPR. Il GDPR estende, la contrattazione con le parti sociali con specifico riferimento al trattamento ulteriore dei dati personali, in ragione dell'evoluzione software e tecnologica, insita negli strumenti di sorveglianza e nel trasferimento dei dati tra imprese (art. 88, 2° co).

Tale ultima disposizione costituisce una norma garantista, che rafforza l'art. 23, 3° co), del D.lgs 151/2015 (già art. 4 dello Statuto), basato sul mero diritto all'informazione dei lavoratori e può aprire ulteriori e interessanti opportunità di tutela e generare strumenti negoziali, sia nelle fasi patologiche che in quelle fisiologiche del rapporto di lavoro, laddove non vengano rispettate le procedure di garanzia[58].

5. Droni e protezione dei lavoratori nel GDPR e nell'AI Act.

L'adozione di comportamenti proattivi, riconducibili ai principi di diligenza[59] e di *accountability*[60], quale gestione preventiva del rischio del trattamento[61], contribuiscono all'accettazione sociale di questi dispositivi tecnologici da parte dei lavoratori.

L' Accordo Quadro delle Parti Sociali Europee sulla Digitalizzazione del giugno 2020, tra la Confederazione Europea dei Sindacati (CES), Business Europe, SGI Europe e SME United, ribadisce, non a caso, la centralità della persona alla guida dei processi produttivi e sottolinea che i sistemi digitali devono essere conformi alla normativa vigente, ma anche al GDPR, in modo da utilizzare tutti gli strumenti messi a disposizione da quest'ultimo per rispettare la dignità umana, limitando il monitoraggio e la sorveglianza[62].

Ai sistemi di intelligenza artificiale classificati ad alto rischio, viene garantito anche il principio "*Human oversight*", che prevede la supervisione umana fin dalla fase di progettazione e sviluppo[63].

---

[58] S. CIUCCIOVINO, *op. cit.*, 950.
[59] Cfr. artt. 1218, 1176, 2087 c.c..
[60] G. FINOCCHIARO, Il principio di accountability, in *Giur. it.*, 2019, 2778 ss.
[61] G.M. RICCIO, G. SCORZA, E. BELISARIO, *op. cit.*, 300.
[62] Disponibile all'indirizzo https://www.etuc.org/system/files/document/file2020-06/Final%2022%2006%20_Agreement%20on%20Digitalisation%2020.pdf, consultato il 5 novembre 2024.
[63] Art. 14 Ai Act.

Se il principio della supervisione umana si applica ai droni, lo stesso non può dirsi per la valutazione d'impatto sui diritti fondamentali, ai sensi dell'articolo 27 dell'Ai Act[64].

Questa apparente esclusione in realtà è spiegabile alla luce della classificazione operata dall'art. 6, 1° co), che considera e per questo assoggetta i prodotti ad alto rischio, quali quelli disciplinati dalla normativa di armonizzazione dell'Unione, a valutazione di conformità da parte di soggetti terzi e dunque imparziali, già prima dell'immissione sul mercato o per il loro utilizzo.

Gli UAS restano, invece, assoggettati ad una serie di requisiti da soddisfare (art. 8), in particolare per quanto riguarda la gestione del rischio (art. 9), i dati e la governance dei dati (art. 10), la documentazione tecnica (art. 11), la trasparenza (art. 13), la supervisione umana (art. 14) e la sicurezza informatica (art. 15).

Resta centrale, quindi, quale limite all'esercizio dei poteri datoriali, il sistema di tutele contenuto nel GDPR.

Il riferimento è all'articolo 35 (DPIA), che prevede la possibilità di consultare gli interessati e i loro rappresentanti, al fine di valutare l'impatto del trattamento in scenari critici (art. 35, 3° co)[65], in grado di aprire un'importante opportunità dialettica con i dipendenti, non riscontrabile in altre discipline[66].

L'attenzione che il GDPR presta alla tutela dei diritti è ravvisabile anche nelle norme sulla sicurezza del trattamento (art. 32), in combinato disposto con l'art. 40 sui codici di condotta volontari, nelle norme sulla protezione dei dati per progettazione e protezione dei dati per impostazione predefinita (art. 25), e certamente nei principi che regolano la contrattazione con le parti sociali (art. 88), in caso di impiego di strumenti tecnologici[67].

---

[64] L'art. 2, 2° co), Ai Act, prevede, infatti, che ai sistemi di IA classificati ad alto rischio, ai sensi dell'art. 6, 1° co), relativo ai <<prodotti>> disciplinati dalla normativa di armonizzazione dell'Unione, elencati nell'allegato I, sez. B, si applichino esclusivamente l'art. 6, 1° co), gli articoli da 102 a 109, l'art. 57 e l'art. 112. Nell'allegato I, sez. B, punto 20, troviamo alcuni ambiti di riferimento, tra cui viene espressamente citato il Reg. 2018/1139/UE (art. 108 Ai Act), che si riferisce agli UAS, da modificare negli artt. 17, 19, 43, 47, 57, 58, al fine di allineare i prodotti alle disposizioni del capitolo III sez. 2, Ai Act, che richiede determinati requisiti di conformità per l'immissione sul mercato o per il loro utilizzo, riconducibili, in particolare, ad aspetti correlati alla gestione del rischio (art. 9), dati e governance dei dati (art. 10), la documentazione tecnica (art. 11), la trasparenza (art. 13), la supervisione umana (art. 14) e la sicurezza informatica (art. 15).

[65] Art. 35, 3° co): Una valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nel caso di: (a) una valutazione sistematica ed estesa di aspetti personali relativi a persone fisiche che si basa su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che producono effetti giuridici sulla persona fisica o che incidono in modo analogo significativamente sulla persona fisica; (b) il trattamento su larga scala di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati personali relativi a condanne penali e reati di cui all'articolo 10; (c) un monitoraggio sistematico su larga scala di un'area accessibile al pubblico.

[66] La Fria, ex art. 27 Ai Act, per es., è un onere a carico dei *deployer*, che viene adottata in modo unilaterale.

[67] A. BERNES, *op. cit.*, 672.

Il GDPR si conferma quindi uno strumento di regolazione atto a garantire che anche i sistemi di IA rispettino i diritti digitali e i diritti dei lavoratori.

Introduce regole specifiche per disciplinare il trattamento dei dati personali, con l'onere della prova a carico del datore di lavoro in merito al rispetto delle stesse e rappresenta, per questa ragione, un baluardo di democrazia, in grado di controllare e limitare il potere datoriale, colmare i vuoti normativi, superare i contrasti dottrinali e giurisprudenziali degli ordinamenti nazionali, come quello relativo all'interpretazione e all'applicazione dell'art. 4 dello Statuto dei diritti dei lavoratori, riportando a unità e rafforzando il sistema delle tutele[68].

Nella dialettica tra tutela della privacy e innovazione, lo stesso Regolamento sull'Intelligenza Artificiale (art. 2, 7° co)) riconosce espressamente la forza attribuita al GDPR, considerato sovraordinato al primo.

Tale ultima disposizione lascia inalterato il Regolamento 2016/679/UE, ad eccezione dell'art. 10, 5° co) e dell'art. 59 del medesimo Regolamento, con l'intento di introdurre maggiori misure di protezione dei dati attraverso correttivi e di evitare effetti distorsivi nonché al fine di sviluppare spazi di sperimentazione normativa (art. 57), all'interno dei quali la privacy e i dati sono sacrificabili per ragioni di interesse pubblico.

Tutto ciò, unitamente al rispetto del principio di *accountability*, prima di adottare strumenti di controllo a distanza, nonché al rispetto dei principi generali del trattamento[69], in modo da rappresentare in modo completo ed esaustivo lo stesso e prima che questo abbia inizio[70], significa rafforzare la base giuridica, quando vengono utilizzati strumenti tecnologici e significa aspirare a un risultato di sistemi di ia affidabili, a misura di persona e socialmente accettati.

6. Droni e responsabilità: limiti dell'attuale regolamentazione o mancanza di regolamentazione?

La questione della responsabilità è ancora irrisolta e, sebbene l'intenzione del legislatore comunitario sia quella di sviluppare una normativa con regole proporzionate al rischio di ogni operazione, le norme speciali del Codice della Navigazione prevedono una responsabilità oggettiva, che resta principalmente a carico dell'operatore o meglio dell'esercente.

[68] A. BERNES, *op. cit.*, 666.
[69] Artt. 5, 24 e 25 GDPR.
[70] Cfr. GPDP, Provv. n. 364 del 06 giugno 2024, disponibile all'indirizzo www.garanteprivacy.it, consultato il 10 giugno 2024; si veda anche in L. BOLOGNINI e E. PELINO, *op. cit.*, 490

L'art. 874 del Codice della Navigazione, identifica la figura dell'operatore in colui che assume l'esercizio dell'aeromobile o nel responsabile degli eventi derivanti dall'esercizio stesso.

I Regolamenti internazionali menzionano la figura dell'operatore.

Nella Dichiarazione di Riga del 06 marzo 2015 <<*Framing the future aviation*>> viene ribadito che il proprietario o l'operatore deve essere sempre individuabile.

A prescindere dalle definizioni, l'operatore di cui alla normativa internazionale o l'esercente di estrazione codicistica, sono figure entrambe chiamate a gestire le attività di volo e di sistema. Secondo la normativa Easa, essi sono responsabili di ogni aspetto relativo alla sicurezza dell'organizzazione, quindi anche della privacy, della raccolta dei dati, dei requisiti di sicurezza per le operazioni[71], della tutela dell'ambiente, nonché all'osservanza degli obblighi assicurativi[72].

Ciò comporta una responsabilità molto pesante per l'operatore, anche se nei limiti della copertura assicurativa minima obbligatoria.

La posizione dell'esercente, qualora coincida con il titolare e/o responsabile del trattamento, in caso di danno materiale o immateriale per violazione e/o non esatto adempimento degli obblighi del Regolamento 2016/679/UE[73] è passibile di sanzioni onerose, che sembrerebbero introdurre un regime di responsabilità per danni (materiali o immateriali) anche a titolo di colpa o di dolo[74], con riferimento sia al trattamento illecito dei dati, ma anche e soprattutto alla omessa adozione di comportamenti proattivi.

In particolare, la norma ponte, che consente di configurare profili di responsabilità per l'intera operazione e quindi anche per i danni a persone e cose, è quella dell'art. 965 del Codice della Navigazione, che parla genericamente di aeromobile in volo e richiama lo schema tipico della responsabilità oggettiva.

L'articolo 965 stabilisce che la responsabilità dell'esercente per i danni causati dall'aeromobile a persone e cose sulla superficie è regolata dalle norme internazionali vigenti nella Repubblica, che si applicano anche in caso di danni causati sul territorio nazionale da aeromobili immatricolati in Italia.

---

[71] Si veda a tal fine il Reg. 2018/1139/UE del Parlamento Europeo e del Consiglio, del 4 luglio 2018, recante regole comuni nel settore dell'aviazione civile e che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea, Allegato IX, art. 1, 1° co), secondo cui gli Operatori e i piloti remoti di aeromobili senza pilota sono tenuti a conoscere le norme nazionali e dell'Unione in materia di privacy, tutela della riservatezza, protezione dei dati, sicurezza, al fine di garantire operazioni sicure e le distanze che separano gli aeromobili senza pilota, le persone a terra e gli altri utenti dello spazio aereo. Questa disposizione è richiamata dal Considerando 2 del successivo Regolamento Delegato 2019/945/UE del 12 marzo 2019.

[72] G. ALPA, *op. cit.*, 921.

[73] Art. 82, 2° co.

[74] Art. 83, comma 2, lett. b).

Le stesse norme si applicano anche agli aeromobili di Stato e agli aeromobili ad essi equiparati[75].

Si parla in senso generico di aeromobili e quindi anche di UAS, e l'assimilazione di quest'ultimi alla categoria degli aeromobili consente l'applicazione delle regole del Codice.

L'indennizzo in caso di danni varia in relazione al peso dell'aeromobile[76] e quindi vi è una prima limitazione della norma, che non affronta il rischio specifico dell'operazione e risulta poco in linea con altre normative, in primis con il Regolamento 2018/1139/UE e i successivi Regolamenti attuativi, ma anche con lo stesso Ai Act, che intende uniformare la materia.

Anche il nuovo Regolamento ENAC del dicembre 2021, che ha cercato di allinearsi alla normativa europea, ha introdotto, infatti, tre categorie configurate in base ai profili di rischio delle operazioni (*open, limited, certified*) e la previsione di specifici indennizzi.

Il criterio ponderale, l'assenza di rischi specifici ai fini della commisurazione del danno risarcibile e l'attribuzione della responsabilità oggettiva in capo all'operatore[77], non solo non sembra coerente con il quadro regolatorio del settore, ma risulta anche non in linea con lo sviluppo tecnologico e con la strategia dei droni 2.0, incentrata sulle esigenze di mercato e di sviluppo del prodotto.

D'altra parte, anche nelle norme di diritto comune e in modo specifico nel caso dell'art. 2054 del c.c., 2° co), in caso di difetto di manutenzione o di costruzione, il regime della responsabilità, pur ricadendo in prima battuta interamente sul conducente e in via solidale sul proprietario del veicolo, viene attenuata per mezzo dell'introduzione della responsabilità da prodotto difettoso[78].

Nel caso dei droni, tuttavia, potrebbero esserci problemi nell'introdurre la responsabilità da prodotto difettoso per mitigare gli effetti della disciplina speciale del Codice della Navigazione, non solo per l'assenza di una responsabilità concorrente, analogamente a quanto accade nell'art. 2054 c.c., ma anche perché la disciplina codicistica è un regime speciale che prevale, quanto all'applicazione, sulle fonti generali[79].

Da ciò consegue l'opportunità di concentrare maggiormente l'attenzione sulle norme codicistiche già in vigore, ipotizzando un'estensione delle

---

[75] Artt. 744 e 746 Codice della Navigazione.

[76] Art. 11 Convenzione di Roma del 7 ottobre 1952.

[77] *Ceretti c. Crescini,* Tribunale di Brescia 28 luglio 1997, secondo cui, in caso di morte di un passeggero, il proprietario, che non è il pilota dell'aeromobile, non è responsabile in solido con il pilota, perché il diritto aeronautico non prevede un principio come quello dell'art. 2054 c.c., comma 3); anche l'esercente dell'aeromobile è privo di legittimazione passiva, a meno che non sia provata la sua qualità di impresa di trasporto o di noleggio.

[78] G. ALPA, *op. cit.*, 979, che inquadra la fattispecie quale *species* del *genus* responsabilità d'impresa.

[79] G. VISINTINI, *Nozioni giuridiche fondamentali: Diritto Privato,* Torino, 2021, 21. L'autrice sottolinea come l'ambito marittimo ha conferito una posizione speciale anche alle consuetudini, che acquisiscono un'autonomia nei confronti delle leggi generali e risultano inquadrabili quale fonte *praeter legem*.

stesse, per quanto riguarda l'allocazione della responsabilità, in capo a diversi soggetti oltre all'operatore (che può essere il proprietario, il titolare/responsabile del trattamento, che non sempre coincide con il datore di lavoro), oppure ripensando al cd. *risk based approach*, con l'allocazione della responsabilità in capo a diverse figure, come il proprietario e il committente, spostando l'attenzione dal piano sostanziale a quello procedurale circa gli obblighi inerenti all'assolvimento dell'onere della prova quanto al rispetto delle misure tecniche e organizzative e della tecno-regolazione, soprattutto nella fase antecedente al trattamento[80].

In sintesi, vale la pena chiedersi chi prende in carico il rischio e la pericolosità delle operazioni, quanto alla privacy e alla sicurezza dei dati.

Solo l'operatore o anche l'impresa che lo ha prodotto? Che ruolo hanno il progettista e lo sviluppatore del software e il deployer *alias* datore di lavoro?

L'importanza di definire *ex ante* i rischi e di sfruttare al massimo quanto già stabilito dal Regolamento 2018/1139/UE in materia di privacy e sicurezza dei dati, che condivide, tra l'altro, con il GDPR, il principio della *privacy by design*, emerge con ogni evidenza.

Un altro caso di responsabilità, riconducibile sotto la voce responsabilità d'impresa, potrebbe verificarsi nel caso di impiego di droni in contesti produttivi, con violazione degli aspetti di privacy e sicurezza dei dati sia dei dipendenti che dell'operatore incaricato della missione. In tal caso, il rafforzamento della normativa dovrebbe riguardare l'attribuzione della responsabilità in capo all'operatore, ma anche in capo al proprietario e al committente, individuando, caso per caso e in concreto, chi sia realmente il soggetto in grado di incidere sul trattamento dei dati[81].

La trasparenza, la valutazione e la determinazione dei rischi nel caso di operazioni con droni potrebbero basarsi, invece che sull'adozione di nuove regole, sul riferimento a nuovi modelli, sperimentabili a partire dal contesto di lavoro.

Ai fini della trasparenza, della descrizione del contesto e dei dispositivi utilizzati, è utile il ricorso anche ai codici di condotta volontari, che consentono, grazie alla loro versatilità, di affrontare e scongiurare il cd. rischio da sviluppo tecnologico, che nel caso di un prodotto difettoso potrebbe comportare conseguenze penalizzanti per i danneggiati a causa dell'esonero di responsabilità dei produttori. Tale aspetto veniva affrontato nella pregressa Direttiva sulla responsabilità da prodotto difettoso[82] e si

---

[80] D. MULA, *Elaborazione e sfruttamento dei dati mediante algoritmi,* in *La circolazione dei dati. Titolarità, strumenti negoziali, diritti e tutele*, a cura di A.M. GAMBINO e A. STAZI, Pisa, 2020, 1443 ss. Sulla responsabilizzazione dell'impresa tenuta ad attenersi al principio di *accountability* in punto di *data protection cfr. anche P. DE PETRIS, La discriminazione algoritmica. Presupposti e rimedi,* in *Diritto del lavoro e intelligenza artificiale*, *a cura di M. BIASI, Milano, 2024, 242.*

[81] S. CIUCCIOVINO, *op. cit.*, 955.

[82] Cfr. art. 118, lett. e) del D.Lgs. 206/2005 del 06 settembre 2005.

trova confermato nel regime attuale, in cui i codici costituiscono elemento utile, sul piano dell'assolvimento dell'onere della prova liberatoria[83].

Uno strumento di questo tipo, soprattutto se condiviso con le parti sociali fin dall'inizio o prima del trattamento, consentirebbe di adattare costantemente il prodotto alle regole, mappare i rischi, compresi quelli presenti in situazioni ad alto rischio, aggirare il problema delle normative speciali da un lato, evitando, al contempo, di rompere l'unità del sistema normativo europeo, soprattutto nell'ambito della tecno-regolazione e delle norme di prodotto, e potrebbe favorire l'accettazione sociale dei sistemi di intelligenza artificiale, contribuendo a mitigare il regime della responsabilità oggettiva.

7. Dalla responsabilità all'*accountability*. Il GDPR e gli istituti a sostegno della contrattazione e della consultazione con le parti sociali.

I principi di liceità del trattamento, minimizzazione, sicurezza e protezione dei dati fin dalla progettazione, rispondono appieno all'attuale quadro regolatorio europeo, che predilige un approccio alle problematiche determinate dall'innovazione tecnologica, orientato al rischio piuttosto che al danno, in una dinamica di prevenzione piuttosto che di risarcimento e sanzione[84]. Il legislatore europeo preferisce intervenire in una fase fisiologica piuttosto che patologica, nel tentativo, piuttosto ambizioso e di difficile realizzazione, di garantire i diritti delle persone fisiche, scongiurare onerose voci di bilancio a carico delle imprese in caso di danni accertati e mantenere alta la competitività.

Il criterio della responsabilizzazione del titolare del trattamento, inteso come colui che ha la capacità di determinare in concreto le finalità e i mezzi dello stesso[85], incontra quella del datore di lavoro, chiamato in ogni caso o anche laddove non coincida con il titolare del trattamento a garantire, sulla base delle norme di diritto comune, di cui all'art. 2087 c.c. (che prevede un

---

[83] L'operatore economico in grado di assolvere tale onere probatorio, previsto dall'art. 11, 1° co), lett. d) ed e) dell'attuale Direttiva UE 2024/2853, è esonerato da profili di responsabilità in caso di prodotto difettoso (che ha causato un danno) conforme ai requisiti giuridici e nel caso in cui <<lo stato oggettivo delle conoscenze scientifiche e tecniche al momento dell'immissione del prodotto sul mercato o della sua messa in servizio oppure durante il periodo in cui il prodotto è stato sotto il controllo del fabbricante non permetteva di scoprire l'esistenza del difetto>>.

[84] G. FRANZA, *Il ruolo dei regolamenti aziendali e della responsabilità sociale dell'impresa: eteronomia e autonomia individuale nel diritto interno*, in *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, *op. cit.*, 641.

[85] S. CIUCCIOVINO, *op. cit.*, 955; cfr. anche Autorità Garante per la Protezione dei Dati Personali, Provv. n. 9977020 dell'11 gennaio 2024, disponibile all'indirizzo www.garanteprivacy.it. Vedi anche art. 4, comma 7, del Regolamento.

ambito soggettivo più ampio di quello del GDPR), l'integrità psicofisica e morale e quindi la tutela della dignità dei lavoratori[86].

Il datore di lavoro è chiamato a rispondere, se non ha adottato tutte le misure per tutelare l'integrità psicofisica dei lavoratori e risponde almeno a titolo di *culpa in vigilando*, essendo l'onere della prova esclusivamente a suo carico. Analogamente, la responsabilità prevista dall'art. 82 del Regolamento, così come quella prevista dalle norme del Codice della Navigazione, nel caso specifico dei droni, prevede una responsabilità oggettiva nel caso in cui siano state violate le norme del Regolamento o siano state omesse misure tecnico- organizzative proattive, a meno che il proprietario non dimostri che il danno non gli è imputabile. Tra le misure che contribuiscono a perfezionare la prova contraria, il Regolamento prevede la dimostrazione dell'adesione ai codici di condotta o ai meccanismi di certificazione[87]. Si tiene conto anche delle misure adottate per mitigare il danno[88] e in particolare delle misure tecniche e organizzative di cui agli artt. 25 e 32 GDPR[89] ai fini della graduazione della responsabilità.

L'adesione ai codici di condotta volontari e il ricorso alle certificazioni, costituiscono, dunque, misure molto importanti perché sono elementi idonei all'assolvimento dell'onere della prova, a carico del titolare, circa il rispetto degli obblighi di cui al GDPR e in particolare dell'adozione di tutte le misure proattive, riconducibili alla *privacy by design,* alla DPIA e alla contrattazione con le parti sociali[90].

8. I codici di condotta. (Rinvio).

I codici di condotta volontari, per essere realmente efficaci nei contesti produttivi, dovrebbero prendere in considerazione il parere delle parti sociali, previsto solo in via facoltativa (C. 99), diventando complementari alla contrattazione (art. 88 GDPR) e integrandosi con altri istituti del Regolamento, orientati, in modo analogo, all'adozione di misure *ex ante* di tutela dei diritti[91].

L'art. 35 GDPR, al comma 8, prevede che nella valutazione di impatto (DPIA) il titolare consideri i codici di condotta, la cui adesione dimostra l'adozione di misure adeguate. Essi favoriscono comportamenti proattivi e in

[86] G. ALPA, *op. cit.*, 260.
[87] Art. 83, 2° co), lettera j)).
[88] Art. 83, 2° co), lett. c).
[89] Art. 83, 2° co), lett. d).
[90] G. FRANZA, *Il ruolo dei regolamenti aziendali e della responsabilità sociale dell'impresa: eteronomia e autonomia individuale nel diritto interno*, in *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, *op. cit.*, 642.
[91] Agenzia europea per la sicurezza e la salute sul lavoro, *Unmanned aerial vehicles: implications for occupational, safety and health,* (2023), disponibile all'indirizzo https://osha.europa.eu, consultato il 04 novembre 2023.

grado di accompagnare le procedure di acquisizione del consenso informato da parte dei lavoratori.

Codici di condotta, accordi sindacali e valutazione d'impatto sono strumenti adeguati e fortemente raccomandati anche dai documenti dell'Agenzia Europea per la Salute e la Sicurezza sul Lavoro, al fine di certificare la correttezza delle procedure adottate per la tutela della privacy e per l'accettazione sociale di sistemi tecnologici complessi. La costruzione di un consenso realmente informato e consapevole sul prodotto utilizzato nel contesto lavorativo, caratterizzato da requisiti di conoscibilità, contribuisce a introdurre elementi di trasparenza e porta a una condivisione delle responsabilità oltre che a una distribuzione diffusa dei rischi per la salute e la sicurezza sul posto di lavoro.

La trasparenza è un elemento che contribuisce a costruire una base di fiducia con i lavoratori ed è legata al concetto di correttezza, di equità e di equità procedurale, come elemento di riequilibrio tra le diverse soggettività del rapporto di lavoro (C. 39 GDPR).

Dirigenti e lavoratori hanno diritto ad essere informati sulla raccolta e sull'utilizzo delle informazioni che li riguardano e sull'esistenza di strumenti di monitoraggio più o meno occulti, di cui devono essere delineati la natura, lo scopo e la portata.

Allo stesso tempo, è molto importante che vi sia un'adeguata informazione sull'uso di tali dispositivi, in modo da fornire agli interessati una chiara rappresentazione del trattamento effettuato, prima che esso abbia inizio e in modo che quest'ultimi ne siano consapevoli e possano formarsi un'opinione[92].

All'elevata invasività del trattamento corrisponde necessariamente la tempestività dell'informazione agli interessati, ai quali viene richiesto di esprimere il consenso, in modo da essere realmente in grado di esercitare il diritto di opposizione[93].

Trasparenza, equità e tempestività sono concetti legati tra loro.

Data la posizione di vulnerabilità e la fragilità del consenso espresso dai lavoratori, i sistemi di monitoraggio devono prevedere un confronto continuo con le parti sociali, in modo possibilmente condiviso con i lavoratori, le cui opinioni dovrebbero essere costantemente e attentamente documentate e monitorate.

I codici di condotta fungono da strumenti di sensibilizzazione tecnica in ordine al regolamento privacy, offrono un quadro conoscitivo dei prodotti

[92] Cfr. GPDP, Provv. n. 364 del 06 giugno 2024, disponibile all'indirizzo www.garanteprivacy.it> consultato il 10 giugno 2024.
[93] GC. MALGIERI, *Vulnerability and Data Protection Law* , Oxford, 2023, 38 ss, 132 ss.

tecnologici in uso, facilitando, anticipandola, la diffusione della conoscenza del prodotto.

Pur non essendo vincolanti, inoltre, una volta adottati, sono in grado di condizionare il mercato, aumentando l'affidabilità degli operatori e la fiducia dei clienti, partner e dipendenti. La violazione di tali codici espone gli organismi di controllo accreditati a sanzioni per <<non aver adottato misure adeguate>> in caso di violazione di un codice di condotta da parte del titolare o del responsabile del trattamento[94].

Rappresentano un'opportunità per attuare i principi del GDPR, in modo condiviso, rispondendo alle esigenze del mercato, degli stakeholder, dei lavoratori (C. 78).

Il contributo della tecnologia diventa fondamentale per restituire valore e dignità alla persona, attraverso il valore di scambio conferito ai dati[95]. Essi diventano centrali nei processi di consultazione e contrattazione tra parti sociali e datoriali, non solo in relazione alle politiche salariali e alle condizioni economiche, ma anche in termini di miglioramento delle condizioni di vita e di lavoro nonché ai fini della valorizzazione complessiva della disciplina che riguarda la contrattazione, da attuarsi anticipatamente ovvero in punto di "algoritmo" e in modo continuo sul "consenso", l'impiego e la "cogestione" dei dati.

9. Le vulnerabilità nel Gdpr e nell'Ai Act.

Il GDPR non prevede regole specifiche che considerano o definiscono il lavoratore come soggetto vulnerabile[96].

Tale dimensione emerge, tuttavia, nel C. 43, che esclude la validità del consenso in presenza di un evidente squilibrio (di potere) tra titolare e interessato, e nel C. 42, nel quale si sottolinea la necessità dell'elemento della "consapevolezza" affinché il consenso sia realmente libero, ascrivendo l'assolvimento dell'onere della prova, sulla formazione del (valido) consenso, a carico del titolare.

Nell'elenco allegato al provvedimento GPDP n. 467 dell'11 ottobre 2018, che in esecuzione dell'art. 35, comma 4), indica quali sono le tipologie di trattamento da sottoporre alla valutazione d'impatto sulla protezione dei

[94] Cfr. art. 83, 4° co), lett. c). In dottrina vedi L. VALLE e M.C. MARULLO, *Contract as an instrument achieving sustainability and corporate social responsibility goals*, in *International Community Law Review*, XXIV, I e II, 109.

[95] Si veda anche V. RICCIUTO, *Lo scambio dei dati con i contenuti e i servizi digitali: una nuova modalità di contrarre?* in *Ejplt,* 1, 2023, 20; S. ORLANDO, *Per un sindacato di liceità del consenso privacy*, in *Diritto Persona e Mercato, 2*022, IV, 527; I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra nuovo regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione*, in *Diritto Mercato Tecnologia,* 2017, 1, 4; F. GAZZONI, *Manuale di diritto privato,* Napoli, 2003, 183.

[96] GC. MALGIERI, *op. cit.*, 87 ss, 115 ss.

dati, vengono menzionati insieme agli altri trattamenti non occasionali di dati relativi ai soggetti "vulnerabili" anche i trattamenti effettuati nell'ambito del rapporto di lavoro, mediante sistemi tecnologici, dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti[97].

Nei contesti di lavoro c'è assenza di equilibrio nelle relazioni e la dottrina riconduce le cosiddette vulnerabilità alle relazioni tra le parti caratterizzate da asimmetria di potere, in cui il consenso è *in nuce* viziato e non "genuino"[98], in quanto non libero.

Per riportare in equilibrio tali situazioni, si rende necessaria, in primo luogo, una valutazione relativa all'eccedenza del trattamento, in grado di giustificare i limiti alle libertà del lavoratore e ai diritti fondamentali.

In secondo luogo, sarà necessario fare riferimento ad altre basi in grado di legittimare il trattamento[99] oppure rafforzare l'acquisizione del consenso con modalità tali da garantire un'informativa reale e adeguata, che lasci i lavoratori liberi di formarsi un'opinione ed eventualmente opporsi al trattamento.

L'Ai Act, analogamente al GDPR, riconosce, senza fornire una definizione, le vulnerabilità e tiene conto delle vulnerabilità di gruppo[100]. Vieta, pertanto, l'immissione sul mercato, la messa in servizio o l'uso di sistemi ia, in grado di dedurre le emozioni di una persona fisica sul posto di lavoro[101].

Per rispondere alle situazioni di vulnerabilità, oltre ai divieti, l'Ai Act rafforza la conformità dei prodotti, attraverso la previsione di adeguate certificazioni e la compliance. Il GDPR risponde, invece, alle situazioni di vulnerabilità per mezzo del principio di trasparenza[102], e la declinazione più importante sarà l'informativa fornita agli interessati e la previsione di alcuni istituti funzionali all'attuazione della trasparenza[103].

Oltre agli istituti già esaminati, particolare rilievo assume la *privacy by design*, che assicura il rispetto del principio di minimizzazione[104], in coerenza con il principio di *accountability*[105].

La *privacy by design* costituisce una misura in grado di esonerare da profili di responsabilità il titolare del trattamento ed è un istituto condiviso anche

---

[97] Cfr. in L. BOLOGNINI e E. PELINO, *op. cit.*, 1382.
[98] A. TOPO e D. TARDIVO, *Hard law e soft law nel diritto dell'Unione Europea in materia di trattamento dei dati personali e di tutela della riservatezza del lavoratore*, in *Privacy e lavoro la circolazione dei dati personali e i controlli nel rapporto di lavoro, op. cit.,* 75 ss.
[99] Cfr. artt. 6 e 9 GDPR.
[100] Art. 5 Ai Act.
[101] Art. 5, 1° co), lett. f).
[102] Cfr. artt. 12, 13, 17.
[103] GC. MALGIERI, *op. cit.*, 133.
[104] Art. 5, 1° co), lett. c).
[105] Sul principio di minimizzazione e privacy by design, si veda la decisione del GPDP, Provv. n. 1712680 del 27 aprile 2010, che raccomanda l'uso di sistemi che sono preimpostati e consentono l'anonimizzazione. Disponibile su https://www.garanteprivacy.it, consultato il 05 novembre 2024.

dal Regolamento sui droni 2018/1139/UE, che stabilisce i principi fondanti, atti a garantire la sicurezza, la privacy e la protezione dei dati personali, grazie all'introduzione di oneri burocratici nel settore dell'aviazione civile.

Da questo quadro normativo sono nati i Regolamenti 2019/945(UE e 2019/947/UE, recepiti da EASA e da ENAC a livello di ordinamento interno, che hanno dato attuazione alla Strategia dell'Aviazione per l'Europa adottata dalla Commissione nel 2015, che aveva come obiettivo lo sviluppo di operazioni sicure su droni e di una regolamentazione in grado di garantire lo sviluppo di standard industriali preordinati a questo scopo[106].

10. Rilevanza della tecno-regolazione e della *privacy by design* per la privacy e la sicurezza dei dati nel Regolamento 2018/1139/UE e nell'art. 25 GDPR. Intersezioni giuridiche con Ai Act.

L'adozione del Regolamento 2018/1139/UE ha rappresentato un importante passo in avanti nella costruzione di una politica e di un quadro comune europeo sui droni. Ha esteso l'ambito di competenza dell'UE a tutti i droni, senza fare distinzioni sulla base del peso o delle dimensioni, come avveniva nel precedente quadro normativo, includendo tra le sue disposizioni anche la progettazione e la fabbricazione nonché le apparecchiature per il controllo remoto di aeromobili senza pilota. La normativa presenta un approccio orientato al rischio per tutte le operazioni e attraverso l'implementazione e l'applicazione dei successivi Regolamenti di esecuzione e attuazione, ha cercato di affrontare la sicurezza delle operazioni, sul piano della privacy e della protezione dei dati e delle reti, attraverso il ricorso a regole tecniche, di cui la *privacy* e *security by design* costituiscono le declinazioni più importanti.

Secondo il Regolamento 2018/1139/UE il requisito fondamentale dei droni resta quello di <<possedere le caratteristiche e le funzionalità specifiche che tengano conto dei principi di tutela della privacy e della protezione dei dati "fin dalla progettazione e per impostazione predefinita" al fine di "mitigare i rischi inerenti alla sicurezza, alla tutela della privacy, alla protezione dei dati personali, alla sicurezza, all'ambiente derivanti dal loro esercizio">>. Sussiste, quindi, un espresso richiamo alla *privacy by design,* esattamente come avviene nel Regolamento 2016/679/UE (GDPR). Quest'ultimo, tuttavia, è trasversale a tutti i settori di impiego della tecnologia e quindi si riferisce al trattamento sia che avvenga sulla piattaforma che al di fuori di essa.

[106] COM. (2015), 598, disponibile all'indirizzo https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52014DC0207&from=EN> consultato il 5 novembre 2024.

Attenersi alla tecno-regolazione significa, dunque, anche seguire le regole della *privacy by design*, in modo da garantire l'immissione dei dettami della legge nel software dell'agente robotico e prevenire atti indesiderati[107] durante l'intero ciclo di vita del prodotto[108].

Nel settore, che ci riguarda, i droni, che possono essere assimilati ai "robot", dovrebbero incorporare[109] alcuni principi, come il consenso informato, la crittografia e il controllo dell'accesso ai dati, già in fase di progettazione. Anche il principio di minimizzazione e le finalità del trattamento possono essere ivi contenuti e costantemente aggiornati[110].

Con l'entrata in vigore del Regolamento Delegato della Commissione 2019/945/UE del 12 marzo 2019 relativo ai sistemi aeromobili senza equipaggio (C. 1 e 2) si ribadisce che è dirimente per gli UAS, appartenenti alla categoria cd. *open,* definire *ex ante* i rischi derivanti dall'esercizio dei dispositivi, facendo riferimento a un quadro di regole comuni e armonizzate a livello UE invece di riferirsi alle "classiche" procedure di conformità aeronautica. Il C. 2 spiega che tali requisiti devono corrispondere a quelli previsti dall'art. 55 del Regolamento 2018/1139/UE, che dovrebbero, in particolare, tenere conto delle caratteristiche e delle funzionalità specifiche necessarie per mitigare i rischi inerenti alla sicurezza del volo, alla tutela della privacy, alla protezione dei dati personali o all'ambiente derivanti dal funzionamento degli UAS.

Il Regolamento Delegato 2019/945/UE (art. 1) approfondisce ulteriormente e dispone che esso intende stabilire i requisiti di progettazione e fabbricazione e dei componenti aggiuntivi di identificazione remota. Per i requisiti, fa riferimento alle parti 1-6 dell'allegato, che risulta assorbente dei dispositivi software di controllo remoto degli UAS, che, secondo quanto specificato nella parte 6, sarebbero quelli di identificazione remota diretta.

La tecno-regolazione di cui al Regolamento 2019/945/UE si applica anche alla progettazione, alla fabbricazione, alla manutenzione e al funzionamento degli aeromobili senza pilota, da intendersi estesa al software oltre che ai motori e alle eliche.

Da tutto quanto sopra potrebbero originarsi eventuali ulteriori profili di responsabilità, in caso di malfunzionamento del prodotto, oltre a quella oggettiva già gravante sull'operatore, e dunque configurare ipotesi di

---

[107] L. MERLA, *op. cit.*, 44.

[108] P.V. MOORE, A. CEFALIELLO e R. DONOGHUE, *Making algorithmic management safe and health for workers: addressing psychosocial risks in new legal provisions*, in *European Labour Law Journal*, 2023, 2, 117.

[109] Linee Guida della Commissione Europea in materia di Robolaw, disponibili all'indirizzo https://www.robolaw.eu>, consultato il 10 dicembre 2023.

[110] L. MERLA, *op. cit.*, 35 e ss. Vale la pena citare il pensiero dell'autore secondo cui <<Il trattamento dei dati personali ben può dipendere dal modo in cui il drone è stato disegnato o costruito, dalla negligenza del fornitore di connettività o di coloro I quali sviluppano determinati applicativi>.

responsabilità da prodotto difettoso, anche con riferimento alla violazione della normativa sulla privacy.

Valutare preventivamente e in maniera condivisa i profili di rischio e i pericoli insiti nelle attività automatizzate, come richiesto anche dall'art. 11 <<Regole per la valutazione dei rischi operativi>> del successivo Regolamento di Esecuzione 2019/947/UE, relativo alle regole e alle procedure per l'esercizio di aeromobili senza pilota, aiuta a definire i profili di responsabilità e a mitigare la connotazione fortemente oggettiva, che emerge dal regime speciale del Codice della Navigazione.

Anche le norme contenute nei Regolamenti 2016/679/UE e 2018/1139/UE condividono il concetto di *privacy by design*. Il secondo provvedimento, in particolare, opera un rinvio, per i requisiti, all'allegato IX, per la mitigazione dei rischi derivanti da sicurezza, privacy, protezione dei dati, ambiente, da tutelare attraverso finalità e caratteristiche specifiche fin dalla progettazione e per impostazione predefinita ovvero *by design e by default*.

Anche l'Ai Act (C. 69) tiene conto della *privacy by design* e della componente valoriale della progettazione, richiedendo la protezione dei dati personali durante l'intero ciclo di vita del prodotto e in modo da rispettare il principio della minimizzazione fin dalla progettazione e per impostazione predefinita, dunque *by design e by default*.

In linea con le considerazioni già svolte sulla natura e le basi giuridiche dell'Ai Act[111], considerata l'indeterminatezza e la genericità delle norme sulla responsabilità oggettiva, che necessitano di essere adattate alle esigenze del mercato e dello sviluppo tecnologico, inerenti al settore dei droni (si veda anche la Strategia droni 2.0)[112], il Regolamento 2018/1139/UE e i successivi 945 che regola l'uso dei droni nei diversi scenari di volo e 947 sui requisiti di progettazione, produzione e vendita, si confermano strumenti essenziali per garantire il rispetto dei diritti fondamentali (se integrati con le norme contenute nel GDPR) oltre che per sostenere l'innovazione tecnologica e la competitività delle imprese.

L'applicazione ai droni dell'art. 57 dell'Ai Act, relativamente alle sanbox, conferma questa idea e apre alla possibilità di regimi sperimentali, in grado di favorire il mercato.

11. Droni e sandbox. Art. 57 Ai Act.

[111] Artt. 14 e 116 TFUE.

[112] Commissione Europea, *Strategia dei droni 2.0 per un ecosistema intelligente e sostenibile di velivoli senza pilota in Europa*, COM (2022) 652 disponibile all'indirizzo <https://www.ec.europa.eu>, consultato il 10 ottobre 2024.

Il Regolamento del Parlamento Europeo e del Consiglio che stabilisce norme armonizzate in materia di intelligenza artificiale[113], classifica i droni quali sistemi di intelligenza artificiale ad alto rischio e considera applicabili ad essi solo alcune disposizioni dell'Ai Act, la più importante delle quali è l'art. 57, che disciplina le sandbox, limitatamente, tuttavia, ai casi in cui i requisiti per i sistemi di intelligenza artificiale ad alto rischio, ai sensi del regolamento, sono stati incorporati in tale legislazione di armonizzazione dell'Unione[114].

Le sandbox intendono superare le rigidità e l'assolutezza della conformità del prodotto, fattori bloccanti dello sviluppo del mercato e dell'innovazione, cercando di promuovere la ricerca di regole inedite, studiate e testate per i singoli casi, considerati in una dimensione concreta anziché astratta, per arrivare a formulare nuove soluzioni tecnologiche, in cui l'efficientamento del mercato non intende mettere in crisi i principi in materia di responsabilità. La partecipazione alle sandbox non solleva, infatti, gli operatori dai danni arrecati a terzi durante il regime di sperimentazione[115].

Uno dei punti critici delle sandbox è costituito dell'uso indiscriminato dei dati personali[116], che non dovrebbe, tuttavia, riguardare gli UAS, dato il perimetro circoscritto di applicazione del Regolamento al prodotto in questione[117].

Il rafforzamento dei profili di responsabilità oggettiva di cui il settore già soffre sono un altro dei punti critici che caratterizzano questo interessante istituto giuridico.

12. Allocazione della responsabilità tra sviluppo della normativa e raccomandazioni. Nuove regole o nuovi modelli organizzativi?

Nel 2019, la Commissione ha adottato due regolamenti di attuazione.

Il Regolamento 2019/945/UE, in particolare, stabilisce i requisiti tecnici per i velivoli senza pilota, ovvero: i requisiti di prodotto per la progettazione

[113] Art. 2, 1° co), lett. a).
[114] Per la definizione di <<spazio di sperimentazione normativa>> e <<piano dello spazio di sperimentazione>>, funzionale al primo, si vedano i commi 54) e 55) dell'art. 3 Ai Act.
[115] L'art. 57, comma 12), così afferma <<i fornitori e i partecipanti agli spazi di sperimentazione durante la stessa, restano in ogni caso e di fatto responsabili ai sensi del diritto dell'Unione e dell'ordinamento interno, per i danni causati a terzi per effetto della sperimentazione>>.
[116] Art. 54, 1° co), Ai Act.
[117] Cfr. La Dichiarazione dell'Austria, espressa in occasione dell'approvazione dell'Ai Act da parte del Consiglio il 15 Maggio 2024, che esprime preoccupazione per l'uso indiscriminate dei dati personali nelle sandbox previste dal Regolamento, in quanto la formulazione è considerate vaga e generica e non idonea a costituire una solida base giuridica per il trattamento dei dati personali ai sensi dell'art. 6, 1° co), lett. c) del Gdpr, e non sarebbe conforme al principio di minimizzazione, in quanto manca di limiti per quanto riguarda l'ambito del trattamento e le categorie di dati personali potenzialmente trattati. Disponibile su <https://www.data.consilium.europa.eu>, accesso del 23 giugno 2024.

e la fabbricazione; gli obblighi degli operatori economici importatori e distributori; il requisito della presunzione di conformità nonché il tipo di drone la cui progettazione, fabbricazione e manutenzione è soggetta a certificazione; l'implementazione di droni destinati all'impiego nella categoria cd. *open* e componenti aggiuntive di identificazione remota.

Il Regolamento 2019/947/UE, invece, stabilisce condizioni dettagliate per le operazioni con i droni, compresi i requisiti per la qualifica del pilota (remoto) e aeronavigabilità, la valutazione del rischio, le operazioni transfrontaliere, la registrazione del drone e del suo operatore, l'autorità competente.

Le autorità nazionali competenti sono tenute a istituire e mantenere sistemi di registrazione per i droni (la cui progettazione è soggetta a certificazione) e per gli operatori di droni, il cui esercizio può rappresentare un rischio per la sicurezza, la riservatezza e l'ambiente.

Anche per gli aspetti relativi alla privacy e alla protezione dei dati personali si conferma la centralità dell'operatore, che resta l'unico soggetto responsabile.

Il Reg. ENAC del 04 gennaio 2021 ha rinviato, genericamente, alle norme del GDPR, per il rispetto della privacy (cfr. art. 29).

La vaghezza e la residualità di quest'ultima disposizione normativa è dovuta principalmente all'assenza di un sistema sanzionatorio in caso di violazione, circostanza che conferma, ancora una volta, la centralità e la rilevanza del GDPR.

Per quanto riguarda gli aspetti della privacy, in particolare, gli operatori, qualora operino in una categoria specifica e certificata, saranno tenuti a registrare ed esporre il proprio numero di matricola sull'UAS. La stessa regola si applica nel caso di esercizio in categoria *open*, quando il peso supera i 25 KG o comunque se il drone è dotato di sensori in grado di rilevare dati personali.

L'immatricolazione è una procedura amministrativa a cui gli artt. 14 del Regolamento 2019/947/UE e 6 dell'Enac, collegano la qualifica di operatore di droni (cd. "esercente" secondo l'approccio aeronautico).

Il principio di *privacy by design e by security,* che troviamo disciplinato sia nel Reg. 2016/679/UE che nel Reg. 2018/1139/UE, è un onere che grava sui progettisti e sugli operatori economici, ai sensi del Reg. 2019/945/UE e che le Autorità Nazionali sono tenute a verificare prima di procedere con l'emissione delle certificazioni di conformità prevista dal Reg. 2019/947/UE[118].

[118] Si vedano a tal fine il Regolamento 2016/679/UE del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relative 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 [2016] GU L119/1, art. 25 e il reg. (UE) n. 1139/2018 del Parlamento Europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile e che istituisce un'Agenzia dell'Unione Europea

Entrambi i Regolamenti sono tenuti a rispettare le disposizioni del Capo III, Sezione 2, del Regolamento sull'intelligenza artificiale, che prevede gli oneri di uniformità a carico dei fornitori di sistemi di intelligenza artificiale ad alto rischio, tra cui i droni.

Il GDPR assorbe i principi esposti e si conferma lo strumento normativo più rilevante nell'attuale panorama legislativo dell'UE per la protezione della persona fisica. Oltre ai divieti, si occupa principalmente del trattamento dei dati, prevede diritti per gli interessati e non solo doveri a carico di specifiche categorie di soggetti, quali i responsabili e i titolari del trattamento dei dati, che sul posto di lavoro, tra l'altro, possono non coincidere con la committenza dell'operazione con drone.

Rispetto al trattamento, infatti, sono previste forme di tutela *ex ante* basate su comportamenti proattivi e modelli organizzativi ed *ex post*, per mezzo di rimedi privatistici, di natura restitutoria e risarcitoria[119], con cui l'ordinamento intende rispondere all'illiceità del trattamento, ai sensi degli artt. 82 e 83. Quest'ultima disposizione, in particolare, inserisce una responsabilità per colpa, basata anche sulla mancata adozione di misure, come la *privacy by design,* la cui presenza, in alcuni casi esclude la responsabilità (cfr. art. 82, 2° co)), in altri la limita (cfr. art. 83, 2° co), lett. d e j))[120].

13. I Codici di condotta e la contrattazione collettiva come strumenti funzionali alla costruzione del consenso, all'implementazione della trasparenza e alla mitigazione dei rischi del trattamento.

La Dichiarazione di Riga sui droni del 2015 aveva sollevato la questione dell'assicurazione, della responsabilità e dei sistemi di risarcimento per le vittime, affermando la necessità di sviluppare norme inerenti alle tecnologie e agli standard, in modo da garantire l'integrazione dei droni nello spazio aereo. I codici di condotta volontari potrebbero contribuire all'elaborazione e alla configurazione, in concreto ed *ex ante* delle situazioni di rischio. La consultazione obbligatoria delle parti sociali e degli stakeholder,

per la sicurezza aerea [2018] GU L212/1, art. 55 e allegato IX, art. 13, secondo cui il requisiti fondamentale per I droni è <<Possedere le relative caratteristiche e funzionalità specifiche che tengano conto dei principi della riservatezza e della protezione dei dati personali fin dalla progettazione e per impostazione predefinita>>.

[119] L. GATT, R. MONTANARI e I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Politica del diritto*, 2017, 2, 351.

[120] G. SMORTO, *Foro It,* 2024, parte 5^, pp. 208-220. C. SCOGNAMIGLIO, *Danno e risarcimento nel sistema del Rgdp, un primo nucleo di disciplina eurounitaria della responsabilità civile?,* in *Nuova giur. comm.*, 2023, V, 1150-1159.

attualmente prevista solo in via facoltativa, potrebbe essere la condizione per rendere questo strumento davvero efficace ai fini della tutela della privacy e dei diritti dei lavoratori[121].

Non solo la trasparenza ne uscirebbe rafforzata, ma anche l'acquisizione del consenso[122], sarebbe realmente informato, libero, responsabile e consapevole[123] trasformandosi in un vero e proprio atto di manifestazione di volontà, dal quale partire per la valutazione della liceità del trattamento[124], superando lo schema meramente autorizzativo.

I codici di condotta si confermano strumenti di autoregolamentazione utili, versatili e autorevoli in virtù della loro legittimazione a livello pubblico corrispondente all'approvazione da parte delle Autorità Pubbliche di Vigilanza[125].

Consentono di introdurre la consultazione obbligatoria delle parti sociali e si prestano a regolamentare qualsiasi situazione che preveda l'uso di tecnologie, anche ad alto rischio, come possono essere quelle relative al trattamento dei dati nei contesti produttivi. Una volta sviluppati e approvati, potranno essere funzionali ai fornitori per dimostrare il rispetto degli obblighi previsti dal GDPR, anche ai fini dell'assolvimento dell'onere della prova in caso di risarcimento danni per violazione della privacy e *data breach*[126].

Laddove occorra effettuare la valutazione d'impatto sulla protezione dei dati, come nel caso dell'utilizzo dell'intelligenza artificiale e di tecnologie particolarmente innovative e pervasive, come i droni, con un potenziale enorme, in termini di sorveglianza, analisi predittiva, profilazione e valutazione della persona[127] e dei sistemi di monitoraggio insiti nel trattamento automatizzato, l'adozione del codice di condotta (art. 35, comma 8)), contribuirà a rendere conoscibile e comprensibile il prodotto impiegato e dunque avrà un impatto positivo sulla trasparenza[128].

I codici di condotta di cui all'art. 40 del GDPR, a differenza di quelli di cui all'Ai Act (cfr. art. 95), non prevedono il limite dell'adottabilità in situazioni a

---

[121] Si veda tal proposito il Reg. (UE) n. 679/2016 del parlamento Europeo e del Consiglio, del 27 aprile 2016, relative 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 [2016] GU L119/1, Considerando 99, che impiega il verbo "dovrebbero" in relazione alla consultazione, da parte dei titolari del trattamento, degli interessati, in sede di redazione, modifica e proroga dei Codici di Condotta.

[122] Cfr. Cass. Civ. Ord. 25 maggio 2021, n. 14381, in *Tecnologie e Diritto*, 2022, II, 367.

[123] A. DAVOLA, *L'acquisizione dei dati da parte dei private nelle operazioni con sapr*, in *Diritto dei droni. Regole, questioni e prassi*, *op. cit.*, 194.

[124] S. ORLANDO, *op. cit.*, 527.

[125] Cfr. art. 55 Reg. 2016/679/UE in combinato disposto con l'art. 40 e dei considerando 55 e 122).

[126] Nuove regole per l'intelligenza artificiale – Domande e risposte. Disponibile all'indirizzo https://wwwcommissione.europa.eu. Consultato il 02 gennaio 2024.

[127] G. NOTO LA DIEGA, *Machine rules. Of Drones, Robots, and the Info-Capitalist Society*, in *The Italian Law Journal*, 2016, II, II, 401.

[128] Trib. Torino, Ord. 05 agosto 2023.

basso rischio e dunque risultano di più ampia applicazione, ovvero in situazioni connotate dall'impiego della tecnologia, in generale.

Anche la Raccomandazione CM/Rec (2015) 5 del 1° aprile 2015, del Comitato dei Ministri agli Stati membri sul trattamento dei dati personali nel contesto occupazionale, sollecita a tenere presente i principi quali la protezione dei dati e il rispetto della vita privata e a <<promuovere l'accettazione e l'applicazione dei principi enunciati nell'appendice del documento di soft law>>, attraverso strumenti integrativi, quali i codici di condotta, in modo da garantire che tali principi siano conosciuti, compresi e applicati da tutti i soggetti che operano nel settore dell'occupazione, compresi gli organismi rappresentativi dei datori di lavoro e dei lavoratori, e che se ne tenga conto nella progettazione e nell'utilizzazione di ITC in ambito occupazionale>>.

L'art. 88 GDPR, supera i codici di Condotta e prende in considerazione solo gli accordi con le parti sociali, che sono idonei a definire il quadro normativo di riferimento, a presidio della tutela dei diritti fondamentali, da effettuarsi esclusivamente per mezzo della contrattazione effettuata in punto di tutela dei valori costituzionali (antidiscriminatori) che regolano l'algoritmo e in termini di cogestione dei dati (determinazione delle finalità del trattamento, accesso, trasferimento, modifica e revoca del consenso, diritto alla rettifica e controllo dell'esattezza dei dati).

La contrattazione potrà avere un impatto significativo sulla qualità della vita dei lavoratori e delle condizioni di lavoro, modificando, ad esempio, il tempo e l'orario di lavoro (cd. *work life balance*)[129]. Questo, tra l'altro, sarà funzionale al superamento dello schema negoziale, basato sullo scambio e sul prezzo dei dati.

Il consenso non sarà riconducibile a un atto di autonomia privata, ma nemmeno a una mera presa d'atto; sarà, invece, un'autorizzazione realmente libera, perché consapevole e informata, finalizzata a ottenere il controllo sui dati, con un ritorno di benefici non strettamente legati solo alla dimensione economica. Ciò consentirà un bilanciamento di interessi, come quello (ma non solo) riconducibile alla partecipazione agli utili aziendali e alla ricchezza prodotta in azienda, da parte degli interessati[130].

L'Accordo Quadro delle Parti Sociali Europee sulla Digitalizzazione, pur affermando la validità della presenza della tecnologia in azienda, menziona espressamente, i contratti collettivi quali strumenti idonei ad attuare l'art.

---

[129] A. MACCAFERRI, Sostenibilità, al centro la qualità della vita e del Lavoro, in Il Sole 24 Ore, 25/02/2024, 20. Secondo l'autrice <<la sostenibilità è sempre più Intesa come qualità della vita e del Lavoro e l'89% delle aziende è sempre più interessato alla sostenibilità sociale, prima di tutto interna, impegnandosi a migliorare la qualità della vita e del Lavoro dei propri dipendenti>>.

[130] A. GRAMOLATI, *La contrattazione da farsi in Azienda e sul territorio*, in *Contrattare l'innovazione digitale, Una cassetta degli attrezzi 4.0*, a cura di A. GRAMOLATI e C. SATERIALE, 70 ss.

88 del GDPR, in modo da consentire ai rappresentanti dei lavoratori di affrontare le questioni relative ai dati, al consenso, alla tutela della privacy e alla sorveglianza.

A tal fine, sarà importante collegare la raccolta dei dati a uno scopo concreto e trasparente, prestato separatamente per ciascuna diversa finalità (cd. granularità del consenso), in modo che sia attuale e non genericamente determinabile in futuro.

14. Conclusioni

Esiste una legislazione uniformante la materia degli UAS a livello europeo.

La disciplina internazionale assimila e conforma sotto il regime delle disposizioni speciali, aeromobili e droni in modo onnicomprensivo; sono state esaminate le intersezioni con altre normative e grazie al contributo del Regolamento 2018/1139/UE, è emersa la necessità di ripensare ad un approccio basato sul rischio, al fine di configurare fattispecie di responsabilità estese anche alla privacy e alla sicurezza dei dati.

La vigente normativa speciale del Codice della Navigazione (e non solo) presenta una serie di limiti, tra cui un'eccessiva concentrazione della responsabilità interamente sull'operatore, l'entità del danno commisurata al peso e non ai rischi concreti connessi all'operazione, e quindi non in linea con le attuali esigenze di sviluppo del mercato; infine, la normativa è generica in termini di privacy e acquisizione del consenso, e manca di un apparato sanzionatorio per la violazione degli aspetti privacy e protezione dei dati, rispetto ai quali si rinvia al GDPR e anche all'Ai Act, limitatamente ai fornitori di sistemi ia ad alto rischio. Nei contesti produttivi, dove i droni sono per lo più strumenti di lavoro, si pongono problemi di allocazione della responsabilità per la privacy in capo a soggetti diversi e non solo sull'operatore e quindi anche sul committente, che non sempre coincide con il titolare o con il responsabile del trattamento.

Il datore di lavoro è comunque chiamato a rispondere, ai sensi dell'art. 2087 del Codice Civile, verso i lavoratori ed è quindi obbligato, già prima dell'inizio del trattamento, a seguire i principi di responsabilità e conformità, di *privacy by design*, ricorrendo alla consultazione preventiva e alla contrattazione ovvero è tenuto ad agire in modo proattivo per garantire i diritti degli interessati.

Il principio di *privacy by design* è presente in tutte le discipline esaminate e costituisce uno degli aspetti più evoluti della progettazione dei sistemi di

ia. Si suppone che sia condivisa con gli sviluppatori di software, ma anche con i fornitori, come nel caso dei sistemi di ia ad alto rischio.

Ha luogo prima del trattamento e deve per questo motivo essere promossa dai titolari e dai responsabili del trattamento, già in una fase antecedente, risultando complementare agli altri strumenti presenti nel GDPR, come la valutazione d'impatto, atti a incorporare, fin dall'inizio, non solo i valori costituzionali, ma anche quelli relativi alla *privacy*, alla protezione dei dati, non discriminazione e trasparenza, all'interno del prodotto[131].

Questa lettura è confermata dall'art. 2 del GDPR denominato <<ambito di applicazione materiale>>, che sembra introdurre un tipo di responsabilità diffusa, riconducibile a un ambito molto ampio, che caratterizza il concetto di <<trattamento>>.

Emerge, dunque, l'importanza della tecno-regolazione, presente in tutte le discipline esaminate (GDPR, Ai Act oltre che nelle norme uniformanti la materia dei droni), che conferma l'importanza della dimensione di *accountability,* in presenza di un quadro incentrato sulla responsabilità oggettiva delle norme speciali del Codice della Navigazione. Questa dimensione assoluta della responsabilità, che inibisce il mercato (aspetto criticato nella strategia dei droni 2.0), è ribadita e trova conferma anche nell'art. 57 dell'Ai Act, che con gli spazi di sperimentazione normativa tenta di dare una risposta al mercato e all'innovazione, senza risolvere, tuttavia, il problema, visto il perdurare delle norme sulla responsabilità.

È onere dell'azienda, inoltre, dimostrare di aver adottato tutte le misure previste dal GDPR, durante il trattamento dei dati dei lavoratori per mezzo delle tecnologie, e sarà quindi interesse dell'azienda dimostrare di aver adottato i comportamenti proattivi ivi previsti e le misure di mitigazione del rischio. Quest'ultime sono ravvisabili nel C. 71 (trattamento accompagnato da adeguate garanzie quali l'informativa, il diritto all'intervento umano, il divieto di trattamento automatizzato, la manifestazione della propria opinione e la garanzia del contraddittorio, il diritto alla spiegazione, il diritto di contestazione, adeguate procedure matematiche o statistiche per la profilazione, misure tecniche e organizzative per la correzione delle inesattezze dei dati, la riduzione al minimo dei rischi per la salute e la sicurezza dei dati); nel C. 78 per gli aspetti afferenti alla *privacy by design*[132]; nel C. 77 per i codici di condotta, che contribuiscono all'acquisizione del consenso, attraverso modelli procedurali adeguati al rischio.

L'art. 88 pur rispettando le norme di garanzia dell'ordinamento giuridico interno e dei contratti collettivi, come l'art. 4 dello Statuto dei Diritti dei Lavoratori, intende, con approccio lungimirante e rivolto al futuro,

[131] S. ORLANDO, *op. cit.*, 538.
[132] G. SIMEONE, *Machine learning e tutela della privacy alla luce del GDPR*, in *Diritto e intelligenza artificiale, op. cit.*, 290.

disciplinare le finalità della raccolta e l'uso che verrà fatto dei dati, attraverso sistemi tecnologici, cercando di evitare fin dall'inizio discriminazioni e violazioni della privacy[133]. Si comprende la ragione per cui sia necessario garantire la conoscenza e la conoscibilità dell'algoritmo, riconducibile all'idea di riconoscere e incorporare i valori costituzionali fin dalla fase di progettazione, cioè dal momento in cui si inseriscono gli algoritmi nel sistema e si scelgono i dati che qualitativamente rispondono a determinate caratteristiche, per far funzionare i sistemi predittivi e di sorveglianza, sia all'interno che all'esterno della piattaforma.

Quanto sopra conferma l'importanza non solo dei codici di Condotta e dell'istituto della Dpia, ma anche dei contratti collettivi, sia in punto di contrattazione degli algoritmi che di cogestione dei dati, da svolgere sia in via preventiva e difensiva sia in modo continuo, durante l'intero ciclo di vita del prodotto.

Con l'avanzare delle attrezzature e delle risorse tecnologiche, che incrementano le possibilità di controllo sul lavoratore, che può avvenire anche per via informatica, anche le normative nazionali devono essere adeguate. L'articolo 88, 1° co), risponde a questa esigenza e demanda alla contrattazione collettiva la prerogativa di introdurre una contrattazione mirata proprio sugli aspetti organizzativi, rivolta alla gestione e alla pianificazione del lavoro. Il 2° co) specifica, infatti, che tali accordi saranno adottati per garantire la trasparenza del trattamento, la tutela della dignità, in caso di trasferimenti di dati e nel caso di adozione di sistemi di monitoraggio dei luoghi di lavoro.

L'apporto della tecnologia avrà un impatto significativo sulla contrattazione futura, sempre più incentrata, sul tempo e sullo spazio del lavoro, con benefici rilevanti per la libertà dei lavoratori, la qualità del lavoro e l'equilibrio vita-lavoro.

L'adozione di nuovi modelli può servire a ristabilire l'equità e a ripristinare simmetria alle relazioni, insieme all'individuazione di interessi legittimi superiori, come quelli della tutela della salute, che da soli possono giustificare l'uso di tecnologie invasive e il trattamento dei dati, ma che possono diventare un facile pretesto per un uso improprio e strumentale nei confronti di soggetti oggettivamente più deboli e vulnerabili, come i lavoratori.

E' comprensibile, quindi, il motivo per cui anche l'Ai Act ha riproposto il principio di *privacy by design* quale elemento della compliance di prodotto ed ha previsto l'armonizzazione delle normative, che riguardano anche gli UAS, in modo da garantire l'applicazione di alcuni principi, primo fra tutti il principio di *Human oversight,* attribuendo precise responsabilità in capo ad

[133] A. SANTOSUOSSO, *op. cit.,* 346 ss.

un soggetto determinato o ad una catena identificata e identificabile, che apre nuove prospettive per l'Ai Act, avvicinandolo ad una dimensione maggiormente soggettiva.