

DRONI E TUTELA DEI DATI PERSONALI

Emilia Vermiglio *

SOMMARIO: 1. I principi della *data protection* nel reg. UE n. 679/2016 – 2. La qualificazione giuridica di un drone al fine di garantire la *data protection* – 3. I dati personali nella normativa di settore: la *data protection* come interesse pubblicistico – 3.1. La registrazione dell'operatore e l'autorizzazione operativa ai fini della *data protection* – 4. Conclusioni.

1. – È noto che i dati personali costituiscono beni in senso giuridico.

Essi rientrano nella categoria concettuale dei beni immateriali e rappresentano un possibile oggetto di diritti di godimento ed essendo negoziabili, circolano, favorendo anche lo sviluppo del mercato ¹.

È ormai consolidato, a livello normativo e giurisprudenziale, che la protezione dei dati personali ha assunto il rango di diritto fondamentale dell'uomo ².

* Titolare di assegno di ricerca dal titolo "Impiego dei droni nella urban air mobility: profili di responsabilità civile", rientrante nel progetto PRIN 2022 "ATM, Drones and D.A.N.T.E. (Digitalization, Artificial Intelligence and New Technologies for Environment)", Università degli studi di Messina. Il presente contributo è frutto di attività di ricerca finanziata dal Prin sopracitato.

Autore corrispondente: prof.ssa Maria Piera Rizzo, *Principal Investigator* del Prin.

¹ A. Morace Pinelli, *La circolazione dei dati personali tra tutela della persona, contratto e mercato*, in *Nuova Giurisprudenza Civile Commentata*, 6/2022, 1322 e ss.

² Sul punto, cfr. F. Rossi Dal Pozzo, *La tutela dei dati personali nella giurisprudenza della Corte di giustizia*, in *Eurojus*, che menziona una "progressiva costituzionalizzazione del diritto alla protezione dei dati personali", grazie al ruolo della Corte di giustizia. L'A., in particolare, afferma "L'acquis communautaire in materia di protezione dei dati personali ha, infatti, visto quale fondamentale attore la Corte di giustizia la quale, ancora prima dell'entrata in vigore della direttiva 95/46/CE10 che il regolamento (UE) n. 2016/679 sostituisce, ha permesso di edificare in via pretoria un diritto alla protezione dei dati personali tale da garantire una tutela elevata e il più possibile adeguata all'evoluzione tecnologica, anche quando la stessa direttiva 95/46/CE si è rivelata inadatta o incompleta. Grazie a questa giurisprudenza evolutiva in materia di protezione dei dati personali, anche a livello di Unione europea, la tutela della privacy ha assunto nel tempo connotazioni diverse, passando dall'essere considerata quale me-



L'art. 8 della Carta Europea dei Diritti fondamentali, rubricato "Protezione dei dati di carattere personale", sancisce infatti che "Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano".

All'interno di tale norma di rango primario, sono enucleati i principi secondo cui deve avvenire il trattamento di tali dati, affinché quest'ultimo possa considerarsi legittimo: la lealtà, la finalità predeterminata, l'esistenza di un base normativa o negoziale, ovvero del consenso della persona interessata ³.

Specularmente, nella Cedu, il diritto alla protezione dei dati personali, seppur non espressamente menzionato nella Convenzione, viene ricondotto al concetto di vita privata di cui all'art. 8, secondo costante giurisprudenza della Corte di Strasburgo ⁴.

Il quadro normativo di riferimento, che si propone di tutelare tale diritto fondamentale, è complesso e di abbastanza recente emanazione ⁵.

A livello europeo spicca il noto reg. UE n. 2016/679, anche detto "regolamento generale" o "regolamento GDPR" ⁶, che si inserisce all'interno di un insieme di riforme più vasto ⁷, la cui *ratio* di intervento si rinviene nell'esi-

na eccezione alle libertà economiche sancite dai Trattati, per giungere oggi, ben prima dell'applicazione del regolamento generale, a una configurazione orientata sui diritti fondamentali".

³ L'art 8 della CdFue, a completamento di quanto sancito nei primi commi, riconosce altresì il diritto di accesso per ogni persona ai dati raccolti che la riguardano e di ottenerne la rettifica. Infine, si specifica che il rispetto di tali regole è rimesso al controllo di un'Autorità indipendente.

⁴ Corte europea dei diritti dell'Uomo, in *giuricivile.it*, *Marper* c. Regno Unito (2008); *Delfi AS* c. Estonia (2015); *Bărbulescu* c. Romania (Grande Camera - 2017); *Jehovah's Witnesses* c. Finlandia (2023); *Drelon* c. Francia (2022); *Uzun* c. Germania (2010); *Godelli* c. Italia (2012); *Big Brother Watch e a. c.* Regno Unito (2021), secondo cui il trattamento deve ruotare attorno ad almeno tre principi cardine: legalità, rilevanza e necessità.

⁵ E anche il reg. UE n. 2018/1725, e le direttive nn. 2016/680 e 2002/58.

⁶ Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

⁷ F. Rossi dal Pozzo, *op. cit.*, "Infatti, si ricorda che, insieme al regolamento generale, sono entrate in vigore due direttive: la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati che abroga la decisione quadro 2008/977/GAI del Consiglio e la direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, il cui termine di recepimento negli ordinamenti nazionali era, rispettivamente, il 6 e il 25 maggio di quest'anno. La Commissione ha previsto anche l'adozione di un regolamento in materia di e-privacy che andrà a sostituire l'attuale direttiva 2002/58/CE (in GUUE L 201 del 31 luglio 2002, p. 37) con l'obiettivo di estendere,

genza avvertita in seno all'Unione di regolamentare con specifiche disposizioni il nuovo sviluppo economico tecnologico e digitale, la cui evoluzione coinvolge necessariamente i dati personali ⁸.

Base giuridica di tale intervento normativo è rappresentato dall'art. 16 dell'TUE, che attribuisce oggi una competenza specifica all'Unione in tema di dati personali ⁹.

A seguito dell'introduzione del regolamento GDPR, deve specificarsi che la tutela dei dati personali non coincide più con il diritto alla riservatezza, in-

in quanto lex specialis, l'ambito di applicazione della disciplina sulla tutela dei dati personali anche ai trattamenti legati allo scambio di e-mail e di messaggi, comunicazioni via social network e a tutto quanto rientri nella definizione di comunicazione elettronica. Infine, non va dimenticato che il diritto alla protezione dei dati personali si applica anche al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione. La disciplina è oggi contenuta nel regolamento (UE) n. 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (in GUUE L 295 del 21 novembre 2018, p. 39). Il regolamento (UE) n. 2018/1725 abroga e sostituisce il Regolamento (CE) n. 45/2001 – pietra angolare nell'impianto della vigente normativa dell'UE in materia di protezione dei dati personali – che è stato adottato nel 2001 con due obiettivi: salvaguardare il diritto fondamentale alla protezione dei dati e garantire la libera circolazione dei dati personali in tutta l'Unione. Il nuovo regolamento ha lo scopo di adeguare le disposizioni contenute nel regolamento (CE) n. 45/2001 ai principi e alle norme stabiliti nel regolamento (UE) n. 2016/679, così da fornire un quadro di protezione dei dati solido e coerente nell'Unione e consentire di applicare contemporaneamente entrambi gli strumenti giuridici. L'allineamento, per quanto possibile, delle norme sulla protezione dei dati per le istituzioni, gli organi, gli uffici e le agenzie dell'Unione a quelle adottate per il settore pubblico degli Stati membri è, insomma, necessario al fine di garantire un approccio coerente in materia di protezione dei dati personali in tutta l'Unione.”

⁸ Si legge infatti nei considerando 6 e 7 del regolamento 679 che “La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali. Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche”.

teso come diritto alla privacy quale pretesa *ad excludendum* ¹⁰.

Il regolamento GDPR n. 679/2016 segna, infatti, il passaggio dal *right to be let alone* al nuovo assetto digitale della *data protection*, inteso quale diritto dell'individuo al controllo dei flussi di informazioni che lo riguardano ¹¹.

Volendo tentare, in estrema sintesi, una ricostruzione del quadro normativo di riferimento, il regolamento GDPR definisce i dati personali come qualsiasi informazione utile all'identificazione di un determinato soggetto ¹².

Alla stregua di quanto riportato all'interno della Carta di Nizza, il trattamento dei dati personali è consentito, così come stabilito nel regolamento, solo se rispettoso di determinati principi.

In particolare, principio cardine cui il trattamento deve essere orientato è rappresentato dal principio di legalità.

A norma degli artt. 5, par. 1, lett. a), e 6 del GDPR la liceità del trattamento è garantita in presenza di determinate condizioni, enunciate, in alternativa tra loro, nel corpo dell'art. 6, quali: la necessità del consenso dell'interessato; l'adempimento di un obbligo contrattuale o legale che grava sul titolare del trattamento; la necessaria salvaguardia di interessi primari dell'interessato o di altri soggetti; l'adempimento un interesse pubblico ovvero l'esercizio di pubblico potere; e, infine il perseguimento di un legittimo interesse del titolare, a condizione non ci siano altri diritti o libertà personali che

⁹ L'art. 16 TFUE (ex art. 286 TCE) attribuisce al legislatore europeo la facoltà di adottare, mediante procedura legislativa ordinaria, una normativa relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e alla loro libera circolazione da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, affidando il rispetto di tali norme ad autorità indipendenti. Cfr. F. Pizzetti, *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, Torino, 2016, e il commento di B. Cortese, Art. 16, in (a cura di) A. Tizzano, *Trattati dell'Unione Europea*, Milano, 2014, 444.

¹⁰ Si rammenta che nella giurisprudenza nazionale, ciò aveva trovato fondamento negli articoli 2, 3, 14, 15, 22, della Costituzione, quale diritto fondamentale della persona alla riservatezza.

¹¹ E. Alonzo, *Le interferenze tra liability e accountability nel Regolamento sulla protezione dei dati personali*, in *Resp. civ. prev.*, 2024, 4, 1133-1146; C. Angiolini, *Trattamento dei dati personali tra legittimo interesse e regole sulla fornitura di contenuti e servizi digitali*, in *Giurisprudenza italiana*, 2023, 10, 2222-2236; G. Remotti, *Evento e danno nella responsabilità per trattamento di dati personali*, in *Persona e Mercato*, 2023, 4, 726-736.

¹² In particolare, stando alla definizione contenuta nel GDPR, si considera "identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

prevalgano e che richiedano, invece, la protezione dei dati coinvolti (specie nel caso dei minori) ¹³.

Il principio di trasparenza, intimamente connesso con la liceità del trattamento, è contenuto agli artt. 5 par. 1 lett. a), 12, 13 e 14 del GDPR, e arricchisce il quadro dei principi della materia; le condizioni che garantiscono un trattamento lecito, prima richiamate, infatti, presuppongono tutte la trasparenza dell'operato del titolare del trattamento, del suo interesse e delle finalità che lo spingono alla raccolta dati.

La trasparenza non incide solo *ex ante* (richiedendo la norma in forma preventiva il consenso dell'interessato o il riscontro della base giuridica a presupposto del trattamento), ma anche *ex post*, dovendo essere garantita la conservazione dei dati e l'accesso ad essi da parte dell'interessato, tanto quanto risulta utile allo scopo per cui è stato posto il trattamento.

A conferma di tale ultimo assunto, il principio di trasparenza è, altresì, richiamato nel capo II del regolamento, dedicato ai diritti dell'interessato.

A norma dell'art. 12, infatti, il titolare del trattamento è tenuto ad adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 ¹⁴, e ulteriori comunicazioni richieste dalla legge relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

¹³ Ai sensi del medesimo articolo, ciò, tuttavia, non si applica in caso di trattamento effettuato da pubbliche Autorità nell'esecuzione dei pubblici poteri.

¹⁴ A norma dell'art. 13, invece, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni: "a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) il diritto di proporre reclamo a un'autorità di controllo; e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. Ulteriori informazioni sono poi garantite a norma dell'art 14 qualora i dati non siano stati ottenuti presso l'interessato".

Infine, il principio finalistico, che riguarda appunto la finalità di trattamento, richiamata agli artt. 5, par. 1, lett. b), e 6 del GDPR, obbliga il titolare, per tutta la durata del trattamento, che i dati siano raccolti esclusivamente per finalità predeterminate, esplicite e legittime.

La finalità del trattamento rappresenta la base giuridica in grado di legittimare il trattamento stesso¹⁵. Tuttavia, il regolamento prevede anche ipotesi in cui quest'ultimo sia posto in essere per una finalità diversa da quella originaria. Pertanto, nel caso in cui non vi sia il consenso dell'interessato o altra base giuridica idonea a giustificare il trattamento, come misura necessaria e proporzionata, il titolare è tenuto a verificarne la compatibilità del trattamento dati rispetto, alternativamente: al contesto, alla natura dei dati, alle possibili conseguenze sugli interessati derivanti dal trattamento, nonché all'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione¹⁶.

Strettamente connesso con la finalità del trattamento, il principio della minimizzazione dei dati consiste nel garantire che questi siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Ne costituisce attuazione l'art. 25 che dispone che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali strettamente necessari per ogni specifica finalità. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone senza l'intervento della persona coinvolta¹⁷.

¹⁵ Per un approfondimento sul tema, S. Orlando, *Consenso al trattamento e liceità*, in *Persona e mercato*, 2024, 2, 333-364; S. Trozzi, *Il principio della finalità del trattamento dei dati personali alla prova dei recenti sviluppi in tema di intelligenza artificiale: il caso chatgpt e la "neuroprivacy"*, in *federalismi.it*, 2024, 1, 197-231; A. Ricci, *Il trattamento dei dati personali dei passeggeri dei vettori aerei per finalità di sicurezza: riflessioni a margine di una recente pronuncia della corte di giustizia*, in *Rivista italiana di diritto del turismo*, 2023, 40, 56-90; N. D. Latrofa, *Il gdpr sulla "privacy" e i "trustee" italiani*, in *trusts e attività fiduciarie in rete*, 2023, 3, 542-547; G. Resta, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, 2022, 4, 971-995.

¹⁶ D. Foresta, *Pseudonimizzazione e anonimizzazione dei dati personali contenuti nelle decisioni giudiziarie*, in *Persona e Mercato*, 2024, 1, 129-156; G. Gentili, *Principio di minimizzazione e soglia di risarcibilità del danno ex art. 15 cod. Privacy*, in *Giurisprudenza italiana*, 2022, 1, 47-57; G. Fonderico, *La regolazione amministrativa del trattamento dei dati personali*, in *Giornale di diritto amministrativo*, 2018, 4, 415-422.

¹⁷ Su tale aspetto, v. L. Califano, *Spunti problematici sul trattamento dei Dati personali raccolti tramite droni*, in *Cultura giuridica e diritto vivente*, 2020, vol. 7.

Espressione di tale principio è anche la cd. pseudonimizzazione, contenuta nel medesimo articolo, che l'art. 4 n. 5 del regolamento qualifica come una modalità di trattamento dei dati personali senza l'utilizzo di informazioni aggiuntive, ovvero un meccanismo di raccolta di dati, mediante il quale non si rende identificabile un determinato individuo.

Risvolti applicativi di tali principi sono i corollari della cd. *privacy by design* e *privacy by default*: sistemi sofisticati di software che automaticamente sono in grado di oscurare determinate informazioni identificative riguardanti un individuo: si tratta di meccanismi che, secondo la dottrina, consentono di spostare eventuali profili di responsabilità sul produttore¹⁸.

2. – In questo quadro normativo articolato e complesso, l'utilizzo di dispositivi aerei a pilotaggio remoto¹⁹ può compromettere o persino vanificare il legittimo controllo del flusso dei dati personali, stante le caratteristiche tecniche e strutturali dei mezzi che, potenzialmente, consentono di incidere e compromettere un numero elevato di dati personali²⁰.

¹⁸ Così L. Califano, *op. cit.*, che afferma "ciò significa che, a monte, il titolare del trattamento dovrà acquistare e dotarsi di soluzioni tecnologiche in linea con le esigenze di protezione dei dati personali, affidandosi a quei produttori che consentano un'ampia gamma di possibilità e un elevato grado di sicurezza. Per cui, l'obbligo che da GDPR grava sul titolare, si trasferisce indirettamente sul produttore, il quale, se vuole rimanere sul mercato, dovrà offrire soluzioni sempre più privacy oriented. (...) In ogni caso, misure di privacy by design e by default sono ormai una realtà anche nel settore degli aeromobili a pilotaggio remoto. Ad esempio, il meccanismo di geofencing rappresenta un'adeguata garanzia per evitare la raccolta di dati ultronei: l'aprioristica circoscrizione dell'area di osservazione, nonché la preimpostazione delle informazioni da non memorizzare, costituiscono misure di minimizzazione dei dati sicuramente da considerare e attuare prima di avviare un'indagine. Allo stesso modo concorre la predefinita di tempi certi di conservazione delle immagini, di cancellazione o anonimizzazione automatica al termine del trattamento, come anche la cifratura dei dati, per impedire che accessi indebiti possano comprometterne la riservatezza, l'integrità e la disponibilità".

¹⁹ R. Schnitker, D. Van Het Kaar, *Drone Law and policy. Integration into the legal order of civil aviation*, LAia, 2021, 1 ss.; D. Hodgkinson, R. Johnston, *Aviation Law and Drones. Unmanned Aircraft and the future of Aviation*, London, 2020, 5 ss. A. Masutti, N. Tomasello, *International Regulation of Non-Military Drones*, Cheltenham (UK), 2018, 44 s.; G. Aiello, M. Biasotti, E. Palmerini, *Diritto dei droni*, Milano, 2018; R. Ungaro, P. Sartori, *I velivoli a pilotaggio remoto e la sicurezza europea. Sfide tecnologiche ed operative*, in *Quaderni IAI*, Roma, 2016, 40 ss; A.M.L. Sia, *Profili attuali della disciplina giuridica dei mezzi aerei a pilotaggio remoto ed il regolamento dell'Ente nazionale dell'aviazione civile italiana (ENAC)*, in *Dir. trasp.*, 2014, 751 ss.; Ar. Abeyratne, *Unmanned Aircraft Systems. The Civil Aviation (Revised) Perspective*, in *European Transport Law*, 2011, 239; B. Gogarty, M. Hagger, *The Laws of Man over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air*, in *J. Law Inf. Sc.*, n. 19/2008, 73 ss.

²⁰ Sul punto si v. C. Della Giustina, *L'utilizzo dei droni nell'attività di prevenzione degli illeciti. Tra riservatezza e tutela dell'ordine pubblico: caos e cosmo nell'universo degli 'unmanned aerial vehicles'*, in *Amministrativ@mente*, 2024, 2, 687-707; M. Dei, O. Koban, L. Kravchenko, A. Lyseiuk, A. Va-

I rischi connessi all'utilizzo di un drone, in relazione alla tutela dei dati personali, si rinvengono proprio nella funzione di videoripresa e di acquisizione, in movimento, non solo di immagini, ma altresì di diverse tipologie di informazioni che possono essere in grado, anche indirettamente, di identificare un determinato soggetto (come fonti di calore o suoni).

Le tradizionali tutele applicabili alla videosorveglianza, seppur tecnicamente estendibili ai droni, appaiono in concreto limitate, o comunque, di difficile applicazione, specie avendo riguardo alla parte degli obblighi informativi in favore degli interessati, che, ove ripresi, devono essere informati attraverso segnalazioni chiare e visibili (come ad es. cartelli con simboli e testo)²¹.

È, dunque, necessario individuare il punto di incontro tra la disciplina generale della protezione dei dati personali e quella specifica dei mezzi aerei a pilotaggio remoto, per bilanciare le esigenze contrapposte nell'uso dei droni, che possono raccogliere informazioni per svariate finalità, come quelle di protezione del territorio o dell'ambiente, di tutela della salute, di soccorso²².

tral, *Legal Regulation of the Use of Drones: Challenges to Human Rights and Privacy*, in *Rivista del Diritto della Navigazione*, 2023, 285-301; L. Ancis, F. Morandi, C. Severoni, F. Toneatto, S. Vernizzi, *Il panorama normativo in materia di mezzi aerei a pilotaggio remoto e lo stato della sua implementazione in Italia - I parte*, in *Resp. civ. prev.*, 2022, 4, 1087-1116; E. Damiani, *Privacy e utilizzo dei droni in ambito civile*, in *European Journal of Privacy Law & Technologies*, 2021, 1, 157-179; L. Califano, *Spunti problematici cit.*, in *Cultura giuridica e diritto vivente*, 2020 fasc. 7; G. Mastrodonato, *Profili di diritto amministrativo nella disciplina giuridica dei droni*, in *ambientediritto.it*, 2020, 4, 436-476; L. Merla, *Droni, privacy e tutela dei dati personali*, in *Informatica e diritto*, 2016, 1, 29-45.

²¹ Anche le Linee guida sulla videosorveglianza del Comitato europeo della protezione dati, nella versione 2.0, adottate nel gennaio 2020, vi ricomprendono altresì le registrazioni effettuate da un'altezza elevata, purché la persona sia identificabile: facendo in questo modo pensare alle raccolte effettuate tramite droni. Di interesse appare la casistica che negli ultimi anni ha visto l'intervento dell'Autorità Garante della Privacy, specie per quelle attività di controllo del territorio e prevenzione degli illeciti portati avanti dagli Enti locali durante la pandemia, e non solo. Da ultimo, più di recente la fattispecie che ha interessato il Comune di Trento nell'utilizzare i droni per l'attuazione di progetti che implicherebbero la raccolta di informazioni in luoghi pubblici attraverso microfoni e telecamere di videosorveglianza, al fine di rilevare potenziali situazioni di pericolo per la pubblica sicurezza. Nella specie, il Garante nel comminare una sanzione pecuniaria al Comune, ha rilevato che quest'ultimo "non annovera la ricerca scientifica tra le proprie finalità istituzionali, non ha comprovato la sussistenza di alcun quadro giuridico idoneo a giustificare i trattamenti dei dati personali – relativi anche a reati e a categorie particolari – e la conseguente ingerenza nei diritti e nelle libertà fondamentali delle persone. Tenuto conto che i dati venivano condivisi anche con soggetti terzi, tra cui i partner di progetto, i trattamenti effettuati sono stati quindi ritenuti illeciti". Fonte: *garanteprivacy.it*, provvedimento del 11 gennaio 2024.

²² L. Califano, *op. cit.*, individua i possibili impieghi di un drone nei diversi settori dell'economia. Tra cui: in Agricoltura per il Monitoraggio delle colture, mappatura dei campi, irrorazione delle colture e gestione del bestiame, ispezione, costruzione e rilevamento delle infrastrutture, map-

Il Considerando 4 del reg. GDPR specifica che il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va temperato con altri diritti fondamentali, in ossequio al principio di proporzionalità.

Anche gli UAS possono perseguire una funzione sociale, come garantire la mobilità, la sostenibilità, e la rapidità dei trasporti grazie all'avanzamento delle nuove tecnologie: il trattamento dei dati personali deve essere, quindi, proporzionato e strettamente connesso all'utilizzo dei droni: in ciò consiste il contemperamento con i diritti fondamentali coinvolti e il bilanciamento con la finalità dell'utilizzo del mezzo.

Occorre rilevare, tuttavia, che i droni potrebbero perseguire anche finalità personali di svago, in ciò comportando un (apparente) *vacuum* normativo in relazione alla tutela dei dati personali, atteso che, ai sensi del considerando 18 e dell'art. 2, par. 2, lett. C) del GDPR, il regolamento non si applica a trattamenti di dati personali nell'ambito di attività che non siano professionali o commerciali.

Sul punto, si specifica che il vuoto normativo può dirsi ormai solo apparente, atteso che la Corte di Giustizia ha nel tempo fornito un'interpretazione sempre più restrittiva di tale disposizione, considerando la disciplina del regolamento GDPR applicabile sempre, specie qualora l'oggetto della ripresa siano luoghi o strade pubbliche²³.

Pertanto, le immagini o le riprese catturate per fini esclusivamente ludici o personali potrebbero comunque essere resi noti successivamente (ad esempio attraverso la pubblicazione dei dati sui social network).

È per tale ragione che appare necessario analizzare la normativa di settore in materia di mezzi aerei a pilotaggio remoto, con particolare riferimento al

patura del sito, monitoraggio dei progressi e modellazione 3D. In ambito della cd. Mobilità aerea innovativa (IAM): Trasporto di passeggeri o merci per scopi commerciali o di altro tipo, come i servizi medici di emergenza (EMS). Nella Ricerca e salvataggio (SAR): I droni dotati di telecamere e sensori termici vengono impiegati nelle operazioni SAR per localizzare le persone scomparse, rilevare i sopravvissuti nelle zone disastrose e consegnare rifornimenti in caso di emergenza. Nel Monitoraggio ambientale: Attività di monitoraggio ambientale come il monitoraggio della fauna selvatica, valutazione dell'habitat e il rilevamento dell'inquinamento. Per le forze dell'ordine, per la consapevolezza situazionale, la gestione degli incidenti e la valutazione dei danni durante le emergenze e i disastri naturali. Nell'ambito dei Media e intrattenimento: Per le riprese aeree in film, programmi televisivi, spot pubblicitari ed eventi dal vivo. Infine, per finalità di Istruzione e ricerca: Se incorporato nei programmi educativi e nei progetti di ricerca in campi come l'ingegneria, la geografia, le scienze ambientali e la biologia della fauna selvatica. Per un ragguglio si v.: esa.europa.eu.

²³ Corte di Giustizia dell'U.E., sent. *Frantisek Rynes* del 11 dicembre 2014, C-212/13, e Garante europeo della privacy parere del 26 novembre 2014 rivolto alla Commissione europea.

regolamento basico n. 1139/2018²⁴, il regolamento esecutivo della Commissione n. 947/2019²⁵, e il nuovo reg. UAS -IT dell'ENAC²⁶, specie nella parte in cui – in tale assetto normativo – si fa espresso riferimento alla tutela dei dati personali nell'uso dei SAPR.

Ciò ci aiuterà a comprendere come le due discipline (generale sui dati personali e speciale sui droni) si intersecano tra loro, e nello specifico se vi sono eventualmente delle lacune normative che possono comportare una scopertura nella tutela del singolo.

Occorre, innanzitutto, premettere che la ricostruzione della nozione giuridica²⁷ di drone quale aeromobile, in quanto mezzo destinato al trasporto, non rileva ai fini del presente studio.

La configurazione del drone, quale aeromobile, ai fini della questione che ci occupa è rilevante in quanto, come peraltro definito dal “regolamento basico”, esso è un “apparecchio dal cui utilizzo può derivare sostentamento nell'atmosfera da reazioni dell'aria, diverse da quelle contro la superficie terrestre”²⁸.

Ciò è conforme, del resto, alla nozione adottata a livello internazionale di cui all'Annesso ICAO n. 7 alla Convenzione di Chicago del 1944²⁹.

Tali norme segnano una prevalenza del profilo cd. tecnico-statico nella definizione di drone in termini di aeromobile, dovendosi quindi tralasciare la

²⁴ Regolamento (UE) n. 2018/1139 del Parlamento europeo e del Consiglio del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio, in GUUE L 212/1 del 22.8.2018.

²⁵ Regolamento di esecuzione (UE) 2019/947 della Commissione, del 24 maggio 2019, relativo a norme e procedure per l'esercizio di aeromobili senza equipaggio C/2019/3824.

²⁶ Regolamento UAS-IT – Edizione 1 Adottato dall'ENAC il 4 gennaio 2021. Attualmente è in corso l'adozione di una nuova edizione del regolamento cui tuttora circola una bozza aggiornata al febbraio 2025.

²⁷ Sul punto, per una ricostruzione del dibattito dottrinale si v. M. Lamon, *L'impiego dei droni militari*, in questa *Rivista*, Vol. XXII/2024.

²⁸ In questi termini, cfr. Art. 3, n. 28, del reg. “basico” n. 2018/1139.

²⁹ Nella definizione di cui all'Annesso ICAO n. 7 alla Convenzione di Chicago del 1944 per «aircraft» si intende: «Any machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the earth's surface». Gli stessi profili definitivi emergono dalla nozione di aeromobile desumibile dalla normativa tecnica eurolunitaria: v., in tal senso, l'art. 3, n. 28, reg. (UE) 2018/1139. Per un ragguaglio sulle posizioni dottrinali in merito alla definizione di aeromobile si v. S. Vernizzi, *L'aeromobile. Dato tecnico e dato funzionale. Profilo statico e dinamico*, Roma, 2020.

nozione in senso funzionale, ovvero di macchina destinata al trasporto, come quella accolta dal codice della navigazione.

Sotto quest'ultimo aspetto, si condivide la posizione della dottrina, secondo cui, il richiamo di cui all'art. 743 «rivesta un significato più di assimilazione all'aeromobile che di identificazione: si tratterebbe di una mera *fictio iuris*, tecnica utilizzata dal legislatore quando intende estendere la disciplina dettata per un fenomeno ad un altro, che è simile, ma non identico»³⁰.

La precisazione è utile ai nostri fini, posto che, l'esigenza di tutelare i dati personali non è incisa dal fatto che un drone sia adibito o meno al trasporto, rappresentando tale aspetto funzionale un elemento irrilevante per il soddisfacimento di detta esigenza; ciò che rileva ai fini della *data protection* è riscontrare, a livello strutturale del mezzo, se siano ivi installati sensori in grado di captare immagini/fonti di calore, da cui è possibile ricavare l'identificazione di un soggetto e, quindi, un insieme di dati personali di vario tipo³¹.

3. – Com'è noto, il reg. 2018/1139, cd. "regolamento básico", introduce la normativa quadro di riferimento in materia di mezzi aerei a pilotaggio remoto, istituendo altresì l'EASA, Agenzia Europea della sicurezza aerea.

Al considerando 49, tale regolamento esegue un rinvio normativo espresso al regolamento GDPR, richiamandone in toto la disciplina ivi contenuta, ritenuta direttamente applicabile all'ambito di operatività del regolamento in materia di mezzi aerei a pilotaggio remoto.

Pertanto, tale aspetto è enfatizzato nell'allegato IX del regolamento citato, il quale, nella parte in cui si dedica ai requisiti strutturali dei droni, richiede che questi ultimi abbiano caratteristiche e funzionalità specifiche che tengano conto dei principi della *data protection*, già dalla fase della progettazione

³⁰ U. La Torre, *Gli UAV: Mezzi aerei senza pilota*, in *Sicurezza, navigazione e trasporto*, a cura di R. Tranquilli Leali, E. G. Rosafio, 2008, 96 ss.; cfr. anche Id., *I nuovi veicoli volanti*, in *Riv. dir. nav.*, 2010, 557. Di diverso avviso, altra parte della dottrina che ritiene gli UAV inclusi nella nozione di aeromobile di cui all'art. 743 c. nav., comma 1, «in quanto destinati al trasporto di cose». In tal senso si esprimono: G. Mastrandrea, L. Tullio, *La revisione della parte aeronautica del codice della navigazione*, in *Dir. maritt.*, 2005, 1218. Si esprime in senso di identificazione del mezzo all'aeromobile B. Franchi, *Aeromobili senza pilota (UAV): inquadramento giuridico e profili di responsabilità – I parte*, in *Resp. civ. prev.*, 2010, 738; Id., *Aeromobili senza pilota (UAV): inquadramento giuridico e profili di responsabilità-II parte*, in *Resp. civ. prev.*, 2010, 1213 ss.

³¹ Inoltre, secondo quanto specificato sia dalla normativa di settore sia dall'EASA, il drone, oltre ad essere dotato dei predetti sensori, non deve ricadere nella disciplina di cui alla direttiva 49/2008 sulla sicurezza dei giocattoli. Si legge infatti, all'art. 14 del reg. 947/2019, per l'individuazione dei droni che necessitano del requisito dell'immatricolazione, che deve trattarsi di "aeromobili senza equipaggio dotati di un sensore in grado di rilevare dati personali, a meno che non sia conforme alla direttiva 2009/48/CE".

del mezzo e per impostazione predefinita, proprio al fine di attenuare i rischi derivanti dal loro esercizio inerenti alla sicurezza, alla tutela della riservatezza, alla protezione dei dati personali, alla security o all'ambiente.

In tale norma sono dunque riassunti tutti i principi in precedenza di cui al regolamento GDPR, applicati alla fattispecie dei droni già nella fase di progettazione: per impostazione predefinita i mezzi aerei a pilotaggio remoto devono essere dotati quindi di sistemi di pseudonimizzazione, di minimizzazione dei dati, che rappresentano espressione dei predetti modelli di privacy by design e privacy by default.

Inoltre, il richiamo al GDPR esplicita anche la possibilità che gli Stati membri nel prevedere esenzioni e restrizioni in relazione ad alcuni dei diritti e degli obblighi previsti, specie per ciò che comporta il trattamento dei dati personali dei piloti, necessario per consentire una cooperazione efficace tra gli Stati in materia di certificazione e di sorveglianza dell'idoneità psicofisica di questi.

Tale considerando è interessante specie con riguardo all'ultimo assunto, ovvero nella parte in cui espressamente si afferma che "se del caso, è opportuno integrare o chiarire nel presente regolamento i principi di cui al regolamento (UE) 2016/679".

Pertanto, non è solo previsto un rinvio generale al regolamento GDPR, ma si fa espressa menzione dei principi ivi contenuti – brevemente sopra esaminati – che sono chiariti e integrati nella disciplina di settore, dove la tutela del GDPR in relazione all'uso dei droni opera su più livelli.

Anzitutto, appare lecito affermare che la tutela dei dati personali nella disciplina di settore si pone come un interesse pubblico di rango superiore, in grado di conferire un maggiore potere restrittivo agli Stati membri, alla stregua di quanto avviene per l'ordine pubblico o la sicurezza nazionale.

Tale assunto è confermato dall'art 56 comma 8, del citato regolamento basilico, ai sensi del quale, si riconosce agli Stati la possibilità di stabilire regole nazionali finalizzate a subordinare a determinate condizioni l'esercizio di aeromobili senza equipaggio per ragioni quali la pubblica sicurezza o la protezione della riservatezza e dei dati personali, conformemente al diritto dell'Unione.

In applicazione di tale art. 56, il considerando 18 del regolamento di esecuzione n. 947 ribadisce tale potere degli Stati membri, che pone la riservatezza e la tutela dei dati personali alla stregua di interessi di portata generale.

In ciò consiste, in particolare, il potere di delimitare porzioni di spazio aereo, denominate "zone geografiche uniche dell'UAS", ai sensi dell'art. 2, n. 4, ove l'autorità stabilisce modalità e limiti delle operazioni UAS, consentite per fronteggiare "ai rischi connessi alla sicurezza, alla riservatezza, alla protezione dei dati personali, alla sicurezza o all'ambiente derivanti dalle operazioni UAS".

Inoltre, a norma dell'art. 15, si specifica che per la tutela della riservatezza, gli stati membri possono vietare operazioni o richiedere particolari condizioni, ovvero autorizzazioni operative preventive (a prescindere quindi dalla categoria del drone).

Di conseguenza, come anche ravvisato nei considerando 20 e 21 del medesimo regolamento esecutivo, gli operatori e i piloti remoti UAS saranno tenuti ad essere adeguatamente informati in merito alle norme nazionali e dell'Unione applicabili alle operazioni previste, in particolare in materia di sicurezza, tutela della riservatezza, protezione dei dati, responsabilità civile, assicurazione e protezione dell'ambiente ³².

Tale aspetto è enfatizzato, anche, nell'allegato IX del regolamento, nella parte in cui si menzionano i cd. "Requisiti essenziali degli aeromobili senza equipaggio", che includono caratteristiche e funzionalità in grado di garantire il rispetto delle limitazioni, i divieti o condizioni applicabili, in particolare per quanto riguarda l'esercizio degli stessi in particolari zone geografiche.

Da tali fonti normative si rileva che la tutela dei dati personali assurge non solo a diritto fondamentale dell'individuo eventualmente coinvolto, ma rappresenta un interesse super individuale a carattere pubblicistico, che può orientare l'operato degli stati membri nello stabilire norme ulteriori, anche di carattere restrittivo, a sua tutela, alla stregua di quanto avviene nei casi di ordine pubblico o sicurezza nazionale.

3.1. – L'Allegato IX del regolamento basico dispone che il drone sia – tra l'altro – dotato di caratteristiche e funzionalità tali da garantire una facile identificazione dell'aeromobile, come pure della natura e della finalità del suo impiego.

Nel considerando 31 del regolamento esecutivo n. 947 si menzionano i dati personali in collegamento con l'esigenza di immatricolazione degli aeromobili senza equipaggio, nonché l'esigenza di istituire sistemi nazionali di immatricolazione degli aeromobili e dei relativi operatori, a loro volta rispettosi di riservatezza e trattamento di dati personali, conservati in sistemi facilmente accessibili.

³² Recita il regolamento, al medesimo considerando che "Alcune zone, quali quelle che ospitano ospedali, assembramenti di persone, impianti e strutture come istituti di pena o impianti industriali, autorità governative centrali e locali, aree naturali protette o determinati elementi delle infrastrutture di trasporto, possono essere particolarmente sensibili per alcuni o per tutti i tipi di operazioni UAS. Ciò dovrebbe lasciare impregiudicata la possibilità per gli Stati membri di stabilire regole nazionali per subordinare a determinate condizioni l'esercizio di aeromobili senza equipaggio per ragioni che non rientrano nell'ambito di applicazione del presente regolamento, quali la protezione dell'ambiente, la pubblica sicurezza o la protezione della riservatezza e dei dati personali conformemente al diritto dell'Unione".

Rilevante sotto il profilo del trattamento dati personali è l'attività d'immatricolazione/registrazione dei droni stessi e dei relativi operatori.

Il regolamento stabilisce un sistema d'immatricolazione sorvegliato e controllato da un'autorità nazionale competente che impone in via preventiva all'operatore di comunicare informazioni circa il mezzo da lui utilizzato e il piano di volo che intende eseguire, e su cui l'autorità può svolgere tale controllo orientato a individuare i principali rischi che l'attività di volo comporta.

Il sistema d'immatricolazione, pertanto, rappresenta una forma preventiva di garanzia per la gestione di determinati rischi, in relazione alla quale l'operatore si impegna a rispettare una serie di requisiti su cui, poi, l'autorità competente esercita il suo potere di controllo.

Il regolamento di esecuzione n. 947/2019 richiama la disciplina contenuta nel regolamento básico e sancisce regole più esplicite circa la necessità d'immatricolazione dell'operatore dell'aeromobile senza equipaggio.

Ci si riferisce dapprima al considerando 14, secondo cui è opportuno immatricolare gli operatori di aeromobili senza equipaggio se utilizzano aeromobili senza equipaggio che, in caso di impatto, possono trasferire all'essere umano un'energia cinetica superiore a 80 Joule o il cui esercizio presenta rischi per la riservatezza, la protezione dei dati personali, la sicurezza o l'ambiente.

Pertanto, stando alla lettera della norma, si evince che l'immatricolazione degli operatori di aeromobili senza equipaggio è necessaria se dall'esercizio del mezzo può essere compromessa sia la protezione dei dati personali sia la riservatezza.

In particolare, il considerando 16 ci fornisce un'ulteriore specificazione, ovvero, tenendo conto dell'eventuale compromissione della riservatezza o della tutela dei dati personali, è richiesta l'immatricolazione agli operatori di aeromobili senza equipaggio che utilizzano tali aeromobili, dotati di sensori in grado di raccogliere dati personali: quindi indipendentemente dal peso del mezzo e dall'energia cinetica utilizzata in caso di impatto.

Come anticipato nel corpo del paragrafo precedente, l'elemento strutturale tecnico del mezzo che rileva ai fini della protezione dei dati personali è, esclusivamente, l'esistenza di sensori in grado di captare immagini video o altre fonti, da cui è possibile anche indirettamente identificare uno o più soggetti.

Esula dall'obbligo di immatricolazione il drone che soggiace già alle tutele di cui alla direttiva 2009/48/CE del Parlamento europeo e del Consiglio sulla sicurezza dei giocattoli.

Nel nostro ordinamento, in applicazione di tale normativa, l'operatore è quindi tenuto a registrarsi come tale presso la piattaforma D-Flight; ciò non è necessario se il drone pesa meno di 250 g e non dispone di fotoca-

mera o altro sensore in grado di rilevare dati personali; tale obbligo non sussiste anche nel caso in cui il bene, anche con una fotocamera o un altro sensore, pesa meno di 250 g, ma è un giocattolo (ciò significa che la sua documentazione dimostra che è conforme alla direttiva “giocattolo” 2009/48/CE).

Se ne deduce che la marchiatura di conformità alla direttiva giocattolo, esclude *in nuce* l'applicabilità della disciplina in esame al drone, il quale, seppur dotato di sensori o fotocamera, resta qualificato come giocattolo e, pertanto, non sarà ritenuto de iure in grado di compromettere dati personali.

Tale assunto è ribadito all'art 14 rubricato immatricolazione per operazioni rischiose³³.

Con particolare riguardo al caso dei droni che operano in categoria *specific*, il regolamento prevede ulteriori prescrizioni.

A norma dell'art 12, rubricato “autorizzazione operativa categoria specifica”, è previsto un potere autorizzativo al volo in capo all'autorità competente, per garantire la sicurezza al volo in tutte le sue fasi.

In particolare, l'autorità competente effettua una valutazione dei rischi e della solidità delle misure di attenuazione proposte dall'operatore UAS, e rilascia l'autorizzazione quando all'esito di tale valutazione conclude che le misure di attenuazione dei rischi proposte dall'operatore sono adeguate e idonee al mantenimento della sicurezza dell'operazione, tenuto conto di tutti i rischi individuati sia a terra sia in volo³⁴.

A corredo della domanda di autorizzazione presentata dall'operatore, quest'ultimo deve fornire una specifica dichiarazione di conformità alle normative nazionali e dell'Unione specie con riguardo ai seguenti aspetti: la tutela della riservatezza, la protezione dei dati, la responsabilità civile, l'assicurazione, la sicurezza e la protezione dell'ambiente³⁵.

³³ A norma di tale disposizione, gli operatori UAS sono tenuti a immatricolarsi: a) quando operano nell'ambito della categoria «aperta» utilizzando aeromobili senza equipaggio, se con peso superiore a 250 gr (o che, in caso di impatto, possono trasferire al corpo umano un'energia cinetica superiore a 80 Joule), ovvero aeromobili senza equipaggio dotati di un sensore in grado di rilevare dati personali, a meno che non sia conforme alla direttiva 2009/48/CE; b) sempre, se operano nell'ambito della categoria «specifica» utilizzando aeromobili senza equipaggio aventi qualsiasi massa. Sancisce poi l'art. 18 compiti dell'autorità competente, tra cui, alla lett. m), l'“istituzione e dell'aggiornamento dei sistemi di immatricolazione per gli UAS il cui progetto è soggetto a certificazione e per gli operatori UAS le cui operazioni possono presentare un rischio per la sicurezza, anche in termini di security, la tutela della riservatezza e la protezione dei dati personali o dell'ambiente”.

³⁴ Se l'operazione non è ritenuta sufficientemente sicura, l'autorità competente ne informa il richiedente, motivando il suo rifiuto di rilasciare l'autorizzazione operativa.

³⁵ Nella parte B “punto UAS.SPEC.030”, rubricato “Domanda di autorizzazione operativa”,

Con riferimento a tale dichiarazione, sussiste una specifica responsabilità dell'operatore, come richiamato nella parte b dell'allegato al regolamento n. 947, per cui riguardo al GDPR, si richiede che l'operatore garantisca tutte le operazioni rispettino il regolamento (UE) n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ³⁶.

4. – Per i droni per i quali sussistono i requisiti tecnici sopracitati, pare chiaro quindi che l'immatricolazione (*rectius*: registrazione) dell'operatore rappresenta il sistema mediante il quale il Legislatore intende garantire la tutela dei dati personali, consentendo di identificare tale soggetto presso l'autorità competente, con tutto ciò che ne deriva in termini di individuazione del responsabile in caso di danni a terzi.

Diverso è ciò che è previsto per i droni che operano in categoria *specific*.

In tale quadro, l'immatricolazione è necessaria ma non sufficiente, essendo altresì richiesta l'autorizzazione operativa al volo a fronte di una domanda *ad hoc* da parte dell'operatore, munita di dichiarazione di conformità alla normativa sulla privacy.

In tal caso, l'operatore è tenuto preventivamente a garantire il rispetto della protezione dei dati personali; una volta fornita tale garanzia, l'operatore ottiene l'autorizzazione se rispettoso altresì di tutti gli altri requisiti indicati dalla normativa per volare in sicurezza.

L'autorizzazione operativa è rilasciata sulla stregua di un'autodichiarazione dell'operatore di conformità alla normativa nazionale ed europea su riservatezza e sui dati personali (e non solo).

Nell'allegato al regolamento si richiama una responsabilità dell'operatore al rispetto del regolamento GDPR, pertanto un'eventuale compromissione di dati personali sarebbe comunque da imputare all'operatore che sottoscrive la dichiarazione di conformità, in quanto l'autorità competente al rilascio

sono scandite le varie fasi richieste dal regolamento all'operatore per avviare un'operazione UAS nella categoria «specifica». In particolare, si legge che "l'operatore UAS deve ottenere un'autorizzazione operativa dall'autorità nazionale competente dello Stato membro di immatricolazione, a domanda di autorizzazione operativa deve basarsi sulla valutazione dei rischi di cui all'articolo 11 e includere inoltre le seguenti informazioni: a) il numero di immatricolazione dell'operatore UAS; b) il nome del dirigente responsabile o il nome dell'operatore UAS nel caso di una persona fisica; c) la valutazione dei rischi operativi; d) l'elenco delle misure di attenuazione proposte dall'operatore UAS, contenente informazioni sufficienti che consentano all'autorità competente di valutare l'adeguatezza degli strumenti di attenuazione per affrontare i rischi."

³⁶ Inoltre, a norma della medesima disposizione, è richiesto che se dall'utilizzo del suo drone si ricade nella fattispecie obbligatoria per la quale, è tenuto ad effettuare una valutazione d'impatto sulla protezione dei dati, lo farà a norma dell'articolo 35 del regolamento (UE) 2016/679.

dell'autorizzazione si limita ad esercitare il suo potere valutativo circa i rischi coinvolti nell'operazione di volo, senza espressamente considerare la compromissione di dati personali, il cui eventuale coinvolgimento e la relativa tutela restano tutti a carico dell'operatore.

Dalla lettera della norma sembrerebbe, infatti, che per il rilascio dell'autorizzazione, l'Autorità competente si limiti a riscontrare esclusivamente l'esistenza dell'auto dichiarazione di conformità alla normativa europea di tutela alla riservatezza e ai dati personali.

Pertanto, anche nella categoria *specific*, non si rinviene un potere di controllo preventivo da parte dell'autorità competente, effettivamente penetrante e valutativo dei rischi che possono compromettere i dati personali.

Sia per le operazioni *open* sia per le operazioni in categoria *specific* (seppur in quest'ultimo caso sussista l'autorizzazione operativa), non si riscontra un effettivo potere di controllo da parte dell'autorità competente circa la tutela dei dati personali coinvolti: la procedura prevista è ridotta infatti ad un'auto-dichiarazione rimessa in capo all'operatore, la cui immatricolazione, certamente utile al fine di individuare il soggetto responsabile, non appare un sistema sufficiente per evitare o comunque contenere eventuali compromissioni di dati personali.

Per ovviare a tali inconvenienti si prospetta l'applicazione di una serie di norme del GDPR di carattere preventivo.

È di sicuro interesse sul punto – già più volte richiamata – dei principi di *privacy by design* e *privacy by default* direttamente nella fase di progettazione e di impostazione predefinita del mezzo, in applicazione dell'art. 5 del GDPR che riguarda la minimizzazione, di cui è menzione anche nel regolamento dell'ENAC all'art 29 (nell'attuale bozza in aggiornamento a febbraio 2025 refluìto nel nuovo art 33): la norma dispone che drone deve assicurare la raccolta di dati strettamente necessari e adeguati al fine e prevedere sistemi automatici di offuscamento e di scrematura di elementi riconoscibili in grado di ricondurre all'identificazione di soggetti coinvolti, ovvero meccanismi di cancellazione automatica di dati ultronei.

Pur essendo un utile strumento, nella pratica si potrebbe comunque giungere ad una compromissione dei dati personali, atteso che spesso anche dati "offuscati" potrebbero portare all'identificazione di un soggetto.

Pertanto può risultare utile vagliare altri due strumenti suggeriti dal GDPR che potrebbero applicarsi alla fattispecie in esame.

Prima di tutto la cd. DPIA, anche detta valutazione di impatto sui dati personali³⁷ (espressamente richiamata tra l'altro, solo nei casi in cui è obbli-

³⁷ P. Chiara, F. Galli, *Normative Considerations on Impact Assessments in EU Digital Policy - Considerazioni normative sulle valutazioni d'impatto nella politica digitale dell'UE*, in *MediaLaws*, 2024

gatoria, nell'allegato al reg. 947 citato).

A norma dell'art. 35 del GDPR tale valutazione prodromica è obbligatoria in determinate circostanze (come quella, che qui può interessare, di raccolta di dati su larga scala o su un luogo pubblico), la quale impone all'operatore di svolgere una sorta di mappatura di dati coinvolti, individuando la natura, l'ambito, il contesto e lo scopo dell'attività, identificando le fonti di eventuali rischi per la privacy e la protezione dei dati.

Utilizzando tale mappa, l'operatore sarà quindi in grado di identificare i rischi rilevanti per la privacy e la protezione dei dati che potrebbero sorgere durante o come risultato dell'operazione, nonché di decidere le misure di sicurezza appropriate per mitigarne gli impatti.

Con tale strumento l'operatore potrà anche prospettare soluzioni per ridurre al minimo i rischi per la protezione dei dati che possono includere: salvaguardie tecniche – misure di sicurezza, mezzi tecnici per ridurre al minimo i dati raccolti o conservati o proteggerli da accessi non autorizzati.

L'obiettivo finale di questa fase è fornire una panoramica completa di quanto sia proporzionata l'interferenza dell'utente con i dati personali degli individui.

Occorrerà poi che l'operatore individui la base giuridica e riferisca espressamente il rispetto della minimizzazione, trasparenza, ed espliciti appunto l'eventuale e successiva condivisione di dati con terze parti.

Il ricorso alla DPIA di cui all'art. 35 del GDPR appare così un sistema efficace, utile ad individuare preventivamente potenziali rischi per la circolazione dei dati personali e la riservatezza, nonché a stabilire le possibili soluzioni che l'operatore ritiene efficace per abbattere il rischio di compromissione di dati.

Ancora, più che il ricorso ad appositi organismi di certificazione³⁸, si ritiene particolarmente rilevante considerare l'applicazione dei cd. Codici di condotta³⁹ di cui all'art. 40 GDPR (anche in considerazione dell'art. 24 del

fasc. 1, 86-105; A. Moretti, *Algoritmi e diritti fondamentali della persona. Il contributo del Regolamento (UE) 2016/679*, in *Il Diritto dell'informazione e dell'informatica*, 2018 fasc. 4-5, 799-817.

³⁸ M. Cardì, *Ruoli soggettivi in materia di certificazione nell'ambito della normativa sulla privacy*, in *Cyberspazio e Diritto*, 2022 2, 261-279; M. Moerschini, *GDPR certifications: state of play, developments and hints at the Italian situation*, in *federalismi.it*, 2020 fasc. 8; E. Lenzoni Milli, *La responsabilità degli organismi di certificazione nel settore della navigazione da diporto*, in *Diritto dei trasporti*, 2018, 2, 515-520.

³⁹ L. Ammannati, *Regolatori e supervisori nell'era digitale: ripensare la regolazione*, in *Giurisprudenza costituzionale*, 2023, 3, 1453-1473; D. Amram, *Comparing EU initiatives on data: addressing risks and enhancing harmonisation opportunities*, in *Opinio Juris in Comparatione*, 2023, 1, 1-25; N. Maccabiani, *Co-regolamentazione, nuove tecnologie e diritti fondamentali: questioni di forma e di sostanza*, in *Osservatorio sulle fonti*, 2022, 3, 55-91; O. Pollicino, *I codici di condotta tra "self-regula-*

GDPR che prevede che l'adesione a tali codici di condotta o a un meccanismo di certificazione ex art. 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento).

Come rilevato correttamente dall'EASA ⁴⁰, i Codici di condotta hanno lo scopo di aiutare le attività degli operatori di droni e dei piloti di droni nello svolgimento di servizi professionali. Il Codice può aiutare le aziende a pianificare le proprie attività e a stabilire una serie di regole formalizzate per la condotta dei propri dipendenti in modo da ridurre al minimo il loro impatto sulla privacy delle persone e facilitare il rispetto dei requisiti stabiliti dal regolamento GDPR.

Al fine di rendere operativo un codice di condotta occorre che lo stesso sia presidiato da un Organismo di controllo all'uopo designato, per il monitoraggio e la supervisione del rispetto delle regole ivi contenute da parte delle parti firmatarie, a norma dell'articolo 41 del GDPR.

Secondo quest'ultimo approccio, l'adozione di codici di condotta rappresenterebbe un utile esercizio di co-regolamentazione della fattispecie concreta, per evitare che la norma tecnica ad alto contenuto tecnologico rimanga inattuata, ritenendo da prediligere una forma di autoregolamentazione di tipo pubblico privato.

tion e "hard law": esiste davvero una terza via per la regolazione digitale? Il caso della strategia europea contro la disinformazione "online", in *Rivista trimestrale di diritto pubblico*, 2022, 4, 1051-1068.

⁴⁰ Fonte: www.easa.europa.eu

Abstract

Il presente contributo offre riflessioni di carattere sistematico derivanti dallo studio della normativa in materia di tutela dei dati personali, applicata all'utilizzo di mezzi aerei a pilotaggio remoto.

In particolare, si vuole analizzare come i principi derivanti dal regolamento "GDPR" UE n. 1679/2016 si intersecano con la disciplina di settore in materia di droni, specie con riferimento al regolamento "basico" UE n. 1139/2018 e al regolamento di esecuzione n. 947/2019.

Dopo aver affrontato anche la nozione giuridica di drone, declinata nel senso "tecnico-statico" di aeromobile, il contributo esamina la tutela della riservatezza, letta sia in chiave pubblicistica, come interesse trasversale che orienta i poteri degli Stati membri nel delimitare porzioni di spazio aereo, ovvero in chiave privatistica, verificando come gli operatori UAS possano in via preventiva prevedere rischi e relative soluzioni per eventuali compromissioni di dati personali.

This paper offers systematic reflections arising from the study of the legislation on data protection, applied to the use of remote-piloted aircraft. In particular, we want to analyze how the principles from EU GDPR Regulation n. 1679/2016 intersect with the sector discipline on drones, especially with reference to EU "basic" Regulation n. 1139/2018 and Implementing Regulation n. 947/2019.

After having addressed the legal notion of drone, declined in the "technical-static" sense of aircraft, the contribution examines data protection, read both in a public key, as a cross-cutting interest that guides the Member States' powers to demarcate portions of airspace, or in a private way, by examining how UAS operators can pre-emptively foresee risks and related solutions for possible compromise of personal data.