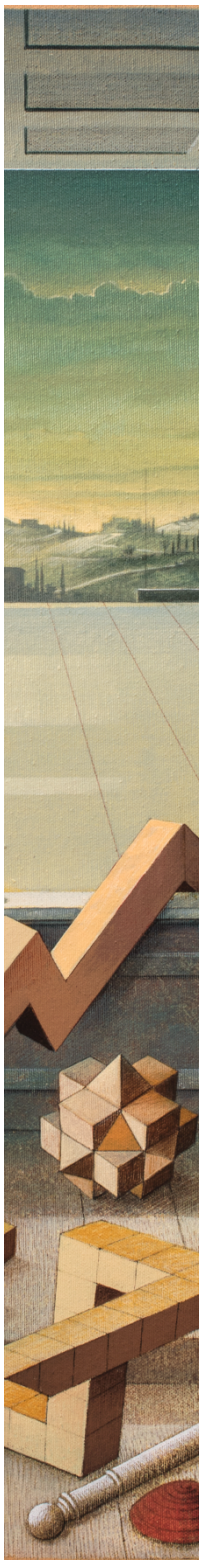
Cultura giuridica e diritto vivente
Rivista on line del Dipartimento di Giurisprudenza
Università di Urbino Carlo Bo
Note e Commenti



SPUNTI PROBLEMATICI SUL TRATTAMENTO DEI DATI PERSONALI RACCOLTI TRAMITE DRONI

Licia Califano

Abstract
[Problems about the processing of personal data collected by drones] The article examines the impact of the utilisation of drones on the right to the protection of personal data of the subjects captured during the flight operations. It analyses this particular processing used mostly for purposes of research and kind of administrative. The new regulation introduced by the GDPR (Regulation (EU) 2016/679) provides for a new perspective that the controller must take into account, starting from the right consideration of the lawfulness of processing, the data minimisation and measures to ensure privacy by design and by default.

Key Words:
Drones, Lawfulness of processing, Purpose of processing, Data minimisation, Privacy by design e by default

Vol. 7 (2020)

Spunti problematici sul trattamento dei dati personali raccolti tramite droni

Licia Califano*

1. Le riflessioni che seguono sono principalmente finalizzate a valutare l'impatto dell'utilizzo dei droni (o SAPR, cioè gli aeromobili privi di equipaggio a pilotaggio remoto) sul diritto alla protezione dei dati personali delle persone ritratte, che ha natura di diritto fondamentale alla luce dell'evoluzione normativa e giurisprudenziale intercorsa negli anni, soprattutto a seguito dell'entrata in vigore del Regolamento Ue 2016/679 (c.d. GDPR).

I droni rappresentano una realtà che probabilmente sarà oggetto di sempre più ampia diffusione, per la loro maggiore capacità, rispetto ai sistemi tradizionali, di captare informazioni dal luogo che sorvolano.

Tramite SAPR è possibile acquisire una serie piuttosto variegata di informazioni. Ben note sono le funzionalità di videoripresa, attraverso le quali è possibile raccogliere le immagini del territorio sottostante. Sono tuttavia di sempre maggiore utilizzo aeromobili dotati di sensori in grado di captare altre tipologie di informazioni, quali suoni, sorgenti di calore, ecc.

Tutte le volte che le informazioni raccolte sono riconducibili a persone fisiche, in grado di rendere queste ultime identificabili, allora tali informazioni si qualificano come dati personali. E l'identificazione può anche avvenire in via indiretta, attraverso l'interconnessione con altre informazioni raccolte in altro modo o detenute in archivi separati – a questo proposito, si tenga a mente la definizione di dato personale contenuta nell'art. 4, n. 1, del GDPR[1].

In altre parole, l'immagine di una persona ritratta sull'uscio di casa, ancorché abbia il volto criptato, rende tale persona identificabile allorché il titolare del trattamento (cioè

*Licia Califano è Professoressa ordinaria di Diritto costituzionale presso il Dipartimento di Giurisprudenza dell'Università di Urbino.
Indirizzo mail: licia.califano@uniurb.it

Il presente articolo ripropone il testo della relazione dal titolo "*La gestione dei dati sensibili raccolti nel corso delle operazioni*" presentata alla Giornata Formativa "*SAPR – CNR 2020*" sul tema "*Organizzazione, risk assessment, gestione dati: inquadramento e linee di indirizzo*", tenutasi presso la sede del CNR, a Roma, il 15 gennaio 2020.

[1] In particolare, tale disposizione qualifica il dato personale come "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); 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".

il responsabile della captazione) sia a conoscenza del luogo in cui è avvenuta la raccolta (perché conosce l'indirizzo) oppure possa risalirvi in maniera agevole (ad esempio, accedendo ad una qualche banca dati pubblica).

Per quanto riguarda esclusivamente la funzionalità della raccolta di immagini, spesso i SAPR vengono assimilati agli impianti di videosorveglianza tradizionali.

Anche le Linee guida sulla videosorveglianza del Comitato europeo della protezione dati, nella bozza messa in consultazione pubblica nel luglio 2019, 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.

Da questo punto di vista, per quanto riguarda la videosorveglianza tradizionale, le garanzie sono state da tempo individuate e consolidate, anche grazie alle tante pronunce del Garante (a partire dalle Linee guida sulla videosorveglianza, aggiornate al 2010[2]).

Tali garanzie riguardano, esemplificativamente: l'obbligo di informativa; l'esigenza di raccogliere i dati effettivamente necessari e pertinenti, escludendo quelli eccedenti; la regolamentazione degli accessi alle immagini; i tempi di conservazione delle stesse; il rispetto della disciplina sul controllo a distanza dell'attività lavorativa.

Tuttavia, il fatto che la videosorveglianza mediante droni abbia la caratteristica particolare di essere effettuata ricorrendo ad un punto di osservazione mobile anziché fisso, rende necessario rivedere le misure di garanzia finora conosciute e aggiornarle alla luce delle peculiari problematiche proprie del fenomeno qui in discussione.

Si pone, dunque, la necessità di contemperare e bilanciare le esigenze connesse alla captazione tramite i SAPR – consistenti nella raccolta di informazioni che, come vedremo, sono preordinate a finalità di ricerca, ma anche statistiche, di protezione civile, di pronto soccorso, o eventualmente pure amministrative – con la necessità di tutelare i diritti fondamentali delle persone, a partire dal diritto alla riservatezza e dal diritto alla protezione dei dati personali.

Esulano da queste riflessioni sia i profili penalistici connessi a fattispecie di reato quale, ad es., quello di interferenze illecite nella vita privata (art. 615-*bis* c.p.), così come gli aspetti connessi all'utilizzo dei droni per finalità connesse all'accertamento e alla repressione dei reati, in cui gli aspetti di protezione dati devono essere contemperati con il regime speciale connesso alle attività svolte da magistratura e forze dell'ordine.

Mi soffermerò, piuttosto, sull'utilizzo dei droni a fini "civili" (e quindi, di ricerca, amministrativi, statistici, di soccorso, ecc.) e sull'impatto che questi hanno sulla privacy degli individui oggetto di osservazione, ancorché occasionale (perché si trovano nei luoghi di captazione).

Va peraltro ricordato che i SAPR potrebbero venire utilizzati anche per finalità esclusivamente personali nel tempo libero. In questi casi opererebbe l'eccezione circa la non applicazione della disciplina privacy (art. 2, par. 2, lett. c), del GDPR), anche se di tale deroga dovrebbe essere data un'interpretazione restrittiva, e quindi ritenendola non opponibile qualora oggetto di ripresa siano luoghi o strade pubblici. Si è attestato su questa linea il Garante europeo (parere del 26 novembre 2014 rivolto alla Commissione), ma anche la giurisprudenza della Corte di giustizia (sent. Frantisek Rynes del 11 dicembre 2014, C-212/13).

A ciò si aggiungano i rischi di riutilizzo improprio delle immagini catturate. Con la diffusione dell'utilizzo dei social network, potrebbero essere pubblicate

[2] Provv. 8 aprile 2010, pubblicato sul sito del Garante, all'indirizzo www.garanteprivacy.it, doc. web n. 1712680.

indiscriminatamente immagini che ritraggono persone, o autovetture o edifici privati riconoscibili (anche grazie a strumenti di ingrandimento e di messa a fuoco di comunissima fruizione), magari unendovi funzionalità di geolocalizzazione; il che sostanzialmente annulla le finalità esclusivamente personali di cui si parlava poc'anzi, rendendo quindi applicabile l'intera disciplina in materia di privacy.

2. Questo premesso, si osserva che oggi la disciplina giuridica del fenomeno trova come imprescindibile punto di riferimento il Regolamento Ue 2016/679 (cd. GDPR), che conferma e rafforza i principi contenuti nella Direttiva 95/46/Ce coniugandoli, per altro verso, con nuove regole ed una tendenziale uniformità della disciplina in tutto il territorio dell'Unione europea.

Il GDPR rappresenta, infatti, la cornice normativa che non può essere trascurata dagli enti pubblici e soggetti privati che si avvalgono di questa tecnologia.

Una cornice che interviene, innovandolo, in un quadro per certi versi ampiamente regolamentato, sia sul piano della cornice europea (si pensi ai regolamenti dell'Ue 1139/2018, 945/2019 e 947/2019) che della disciplina nazionale (il regolamento dell'Enac, nella versione da ultimo dell'11 novembre 2019).

Peraltro, l'importanza della disciplina in materia di protezione dei dati personali, oggi costituita appunto dal GDPR, viene corroborata da una serie di elementi contenuti nelle citate norme di settore, che quindi rafforzano l'effetto di sistema che il GDPR ha su tutti i trattamenti di dati personali, anche quelli effettuati tramite SAPR.

In particolare, i sopra citati regolamenti europei di settore richiamano ampiamente le esigenze di protezione della riservatezza e dei dati personali, affiancando tale diritto fondamentale ad altre esigenze di rilevante interesse pubblico quali quelle concernenti la sicurezza o la tutela ambientale.

In particolare il regolamento dell'Enac comprende una disposizione specificamente dedicata al tema della protezione dati (art. 34) la quale, ancorché necessiti di un aggiornamento rispetto al mutato quadro normativo in materia di privacy – infatti, cita l'art. 3 del Codice, oggi abrogato, e non indica in alcun modo il GDPR – ha certamente il merito di rinviare alla disciplina in materia di protezione dati, nonché agli interventi del Garante per la protezione dei dati personali.

Le principali questioni poste dall'utilizzo dei droni, dal punto di vista dei principi e delle regole affermati dal GDPR si possono chiarire e sintetizzare nei punti che di seguito vengono specificamente, se pur brevemente, annotati.

3. Presupposto di liceità del trattamento (artt. 5, par. 1, lett. a), e 6 del GDPR

In proposito, la prima domanda che occorre porsi è: quando possiamo effettuare un trattamento di dati personali tramite la captazione di immagini (ma eventualmente anche altre tipologie di informazioni) effettuata da drone? Qual è il presupposto di liceità?

Il GDPR individua una serie di condizioni, il primo dei quali è il consenso degli interessati (art. 6, par. 1, lett. a), che trova una specifica disciplina nei successivi art. 7 e 8)[3]. Partendo però dal raffronto con la videosorveglianza, potremmo anche considerare

[3] L'affermazione del consenso quale presupposto giustificativo del trattamento risiedeva già nella direttiva 95/46/Ce (artt. 2 e 7), e successivamente ha trovato un riconoscimento solenne nella Carta dei diritti

questo presupposto come difficilmente applicabile al caso di specie. Infatti, la raccolta di immagini tramite sistemi che siano fissi (come le telecamere tradizionali) o, a maggior ragione, mobili (come i droni), rende molto difficile, se non impossibile, acquisire preventivamente il consenso al trattamento da parte delle persone che verranno ritratte: spesso non è neanche possibile sapere a priori chi saranno gli interessati prima ancora che questi raggiungano il punto di osservazione (si pensi ai passanti che percorrono una strada o attraversano un parco pubblico).

Nelle Linee guida sulla videosorveglianza, pertanto, il Garante aveva effettuato un bilanciamento di interessi tra il diritto alla riservatezza degli interessati e le esigenze perseguite dal titolare, consentendo il ricorso alle telecamere di sorveglianza "*qualora, con le modalità stabilite in questo stesso provvedimento, sia effettuata nell'intento di perseguire un legittimo interesse del titolare o di un terzo attraverso la raccolta di mezzi di prova o perseguendo fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, o finalità di prevenzione di incendi o di sicurezza del lavoro*".

Oggi il bilanciamento di interessi non viene più effettuato direttamente dal Garante ma, in base a quanto stabilito dal GDPR, è il titolare stesso del trattamento a valutare autonomamente, nell'ambito del principio di *accountability*, la sussistenza di un legittimo interesse suo, o di terzi, a condizione che non prevalgano gli interessi o i diritti degli interessati (art. 6, par. 1, lett. f)). In altre parole, è il titolare che deve decidere se il suo legittimo interesse ad acquisire i dati sia prevalente, assumendosene quindi la responsabilità in caso di lamentela da parte dell'interessato o di controllo da parte dell'Autorità.

Il legittimo interesse è un presupposto di liceità valido quando il trattamento viene effettuato da soggetti privati per finalità anch'esse private.

Quando però il trattamento, e quindi l'uso di droni che raccolgano dati personali, viene effettuato in ambito pubblico, allora ricorre un altro presupposto: si tratta della necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6, par. 1, lett. e)).

In questa ipotesi, non è però sufficiente la sola sussistenza di questo compito di interesse pubblico, in quanto occorre altresì una base giuridica costituita dal diritto europeo o nazionale (art. 6, par. 3). Per quanto riguarda specificamente l'Italia, tale base giuridica deve consistere in una norma di legge o, se prevista dalla legge, di regolamento, la quale fornisca un quadro un po' più definito sulle caratteristiche del trattamento e sulle garanzie a tutela degli interessati (art. 2-*ter* del Codice, come novellato dal d.lgs. 101/2018).

In sintesi, in ambito pubblico, per poter utilizzare SAPR che, anche incidentalmente, acquisiscano dati personali occorre una normativa che lo consenta. I regolamenti europei che ho citato prima, nonché il regolamento dell'Enac sui mezzi aerei a pilotaggio remoto, costituiscono, da questo punto di vista, una base giuridica, su cui occorre però svolgere alcune considerazioni per quanto concerne le finalità perseguibili.

4. Finalità del trattamento (artt. 5, par. 1, lett. b), e 6 del GDPR

Il regolamento Enac individua le seguenti finalità per le quali è possibile ricorrere all'utilizzo di droni (art. 7): anzitutto ci sono attività di ricerca e sviluppo, cui si aggiungono operazioni specializzate in scenari sia critici che non critici, che attività non specializzate

---

fondamentali dell'Unione europea del 2000, il cui art. 8, par. 2, sancisce che i dati di carattere personale "devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge".

in scenari non critici (quindi, con esclusione di aree congestionate, agglomerati urbani e infrastrutture sensibili).

L'attività di ricerca rappresenta una delle finalità per le quali il GDPR ha riconosciuto un ampio (o forse addirittura il maggior) livello di deroghe rispetto agli impegni stabiliti in via generale. Ricordiamo, per esempio, che si giustifica la ricerca (come la statistica) anche su dati raccolti per altre finalità e per tempi ulteriori rispetto a quelli originariamente previsti per tali altre finalità (art. 5, par. 1, lett. b) ed e)).

In particolare, l'art. 89 del GDPR consente un ampio rinvio alla normativa nazionale, che deroghi anche ad alcuni istituti del GDPR stesso, proprio in materia di ricerca e statistica. Grazie a queste clausole il legislatore nazionale ha potuto stabilire una specifica disciplina dedicata a questi settori e contenuta negli artt. da 97 a 110-*bis* del Codice, come novellato nel 2018. Tale disciplina, che sostanzialmente riprende quella esistente nel Codice anche prima che il GDPR diventasse applicabile, contiene una serie di misure specifiche, anche a garanzia degli interessati, perché la ricerca possa dirsi rispettosa della disciplina in materia di protezione dei dati personali. Peraltro, l'art. 106 del Codice rinvia ad apposite regole deontologiche attraverso le quali definire un perimetro in cui la ricerca può essere ampiamente condotta senza che siano arrecati pregiudizi agli interessati.

Al momento, le regole deontologiche esistono e sono costituite dal preesistente codice deontologico come adattato al nuovo quadro normativo europeo (ai sensi dell'art. 20 del d.lgs. 101/2018). Tuttavia, le categorie interessate (a partire dai ricercatori) possono promuoverne l'aggiornamento e l'integrazione, anche alla luce delle nuove esigenze che si possono porre.

Ma, come si accennava all'inizio, i droni potrebbero essere utilizzati anche per altre finalità, come ad esempio: la videosorveglianza su infrastrutture critiche; la protezione civile, la gestione delle catastrofi e dei soccorsi; la protezione dell'ambiente; la produzione agricola.

Il presupposto giuridico per l'effettuazione dei trattamenti, nei predetti casi, dovrebbe risiedere nell'esercizio di un compito di interesse pubblico, per cui, come si diceva poc'anzi, serve una norma di legge o di regolamento, nei casi previsti dalla legge, che consenta il trattamento, che ne stabilisca le caratteristiche e che stabilisca misure a tutela dei diritti degli interessati. Ovviamente questo discorso vale solo per quelle riprese che intercettano persone fisiche identificabili o comunque elementi in grado di identificarle: se le aree sottoposte ad osservazione sono deserte oppure vengono utilizzate tecniche in grado di non raccogliere con assoluta certezza dati personali, allora il tema della base giuridica non si pone.

Il tema del ricorso ai droni per fini amministrativi è comunque molto delicato. Le sue potenzialità potrebbero spingere enti pubblici ad utilizzare il SAPR per finalità di controllo, viste le caratteristiche che lo renderebbero più utile rispetto a mezzi più tradizionali di videosorveglianza (a partire dal fatto che si tratta di un punto di osservazione mobile): si pensi, ad esempio, all'ipotesi di un Comune che voglia monitorare il proprio territorio alla ricerca e all'approfondimento di potenziali abusi edilizi. Ciò fa capire come solo la legge possa eventualmente stabilire se un tipo di trattamento è consentito, in quali termini e, soprattutto, con quali garanzie per gli interessati; senza un quadro normativo certo e proporzionato questi usi non sono consentiti.

Occorre, pertanto, fare bene attenzione al perimetro di utilizzo stabilito dalla norma che vi è alla base, come anche, in caso di raccolta per finalità di ricerca, occorre attenersi rigorosamente al programma di ricerca e alle cautele ivi previste. Un utilizzo per finalità

ulteriori, che esondano da quanto prefissato in maniera trasparente, rappresenta un trattamento illecito che l'Autorità può perseguire avvalendosi dei suoi poteri correttivi.

5. Trasparenza (artt. 5, par. 1, lett. a), 12, 13 e 14 del GDPR

Trasparenza significa rendere edotti tutti i potenziali interessati del fatto che si stanno effettuando dei trattamenti, e di perché e come tali trattamenti stiano avvenendo, nonché delle modalità di esercizio dei propri diritti.

Se per gli operatori protagonisti dell'attività di ricerca sono sufficienti modalità di informativa tradizionale, ricorrendo a documenti informativi individuali, magari uniti a informative semplificate da affiggere in prossimità dei luoghi di ripresa (come avviene per la videosorveglianza tradizionale), qualche problema in più si pone per tutte le altre persone che si trovano o nelle zone limitrofe alle aree di decollo e atterraggio o addirittura nelle zone di ripresa.

In questo caso vanno pertanto individuate delle modalità di informativa adeguate, che rendano realmente consapevole il pubblico della circostanza che si stanno effettuando delle riprese.

A questo proposito, si potrebbero prendere come punto di partenza le prescrizioni impartite a Google con provvedimento del Garante del 4 dicembre 2014 (doc. web n. 3633473), in riferimento al servizio Streetview e, in particolare, al momento in cui i veicoli di Google si recano nelle località italiane per raccogliere le immagini da caricare sul noto servizio di Google Maps. In quella sede, il Garante ha prescritto sia forme di informazione diretta al pubblico (pubblicazione della notizia sul sito web del titolare, dei partners nonché degli enti, strutture, soggetti privati, fondazioni, ecc. che possiedono, gestiscono o soprintendono i luoghi oggetto di ripresa; avvisi o cartelli affissi all'ingresso di siti o luoghi, pubblici o privati, recintati ovvero aperti al pubblico), sia accorgimenti volti a indicare, in modo inequivocabile, che si stanno acquisendo immagini fotografiche istantanee oggetto di pubblicazione online (ad esempio, fissando sulle attrezzatture ovvero anche sull´abbigliamento dei relativi addetti adesivi, cartelli o altri segni distintivi ben visibili).

6. Minimizzazione e privacy by design e by default (artt. 5, par. 1, lett. c), e 25 del GDPR

Quello della proporzionalità del trattamento rispetto alle finalità perseguite è forse l'aspetto centrale che la novellata disciplina privacy ha inteso rafforzare. E forse è anche quello più complesso da definire.

Infatti, la proporzionalità si lega a doppio filo con l'accountability, cioè il potere del titolare (e, specularmente, l'onere) di fare autonome valutazioni volte a minimizzare i rischi connessi al trattamento e l'impatto dello stesso sui diritti e sulle libertà fondamentali delle persone. Non ci sono regole fisse valevoli per tutti, non c'è una ricetta universale: ogni trattamento, ogni tecnologia, ogni contesto, richiedono un'attenta valutazione circa i confini oltre i quali il titolare non si può spingere e misure che garantiscano un'adeguata tutela per gli interessati.

Il principio di minimizzazione è la sintesi di questo approccio. Nel settore quest'oggi oggetto di dibattito, minimizzazione significa sicuramente raccogliere i dati personali assolutamente necessari, senza i quali l'indagine effettuata tramite SAPR sarebbe impossibile: ad esempio, limitando la captazione di persone e oggetti ricompresi all'interno dell'area di osservazione, e possibilmente a quelle persone e oggetti che fanno parte del progetto di ricerca, o quantomeno escludendo terzi estranei. Ciò dovrebbe anche

tenere conto delle limitazioni al sorvolo stabilite dal regolamento ENAC con riferimento alle operazioni critiche (ossia quelle che interessano aree congestionate, assembramenti di persone o agglomerati urbani).

Ma la minimizzazione va applicata anche ad altre fasi del trattamento, come la successiva rielaborazione delle immagini.

Occorre cioè che vengano conservati i soli dati personali assolutamente necessari, cancellando quelli eccedenti e non pertinenti, o quantomeno rendendo non più identificabili le persone cui si riferiscono.

Peraltro, in alcuni settori potrebbe anche non servire il dato grezzo, poiché oggetto dello studio successivo potrebbero essere template o codici che scaturiscono dalla rielaborazione matematica del dato grezzo: in questo caso il dato grezzo dovrebbe essere cancellato non appena cessata l'operazione di conversione, e dovrebbe essere garantita la non reidentificazione degli interessati.

Le misure possibili, però, non possono essere improvvisate, ed i problemi non possono essere affrontati solo a trattamento in corso.

Tutte le azioni vanno attentamente pianificate prima, in modo da predisporre fin da subito gli accorgimenti in grado di minimizzare la qualità e quantità di dati trattati, nonché di ridurre i rischi.

Questa progettazione rappresenta l'obiettivo dei concetti di privacy by design e by default che il GDPR ha finalmente positivizzato, trasformando tale processo organizzativo e valutativo in un vero e proprio obbligo in capo **ai** titolari dei trattamenti.

Ma 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*.

Peraltro, se il produttore poi fornirà anche servizi ulteriori di manutenzione e assistenza al titolare, e, in questo caso, qualora avrà accesso ai dati personali oggetto di trattamento (ancorché solo incidentalmente), dovrà assumere la qualità, gli obblighi e le responsabilità del responsabile del trattamento, ai sensi dell'art. 28 del GDPR.

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 predefinizione 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.

In proposito, il regolamento di esecuzione 2019/947 della Commissione del 24 maggio 2019 riconosce l'utilizzo, sui droni, di sensori in grado di rilevare dati personali, prevendendo che, in questo caso i piloti di SAPR procedano ad una specifica immatricolazione, salvo che tali sensori non siano già conformi a quanto stabilito dalla direttiva 2009/48/CE (art. 14 e considerando 16). Il ricorso a questi sensori dovrebbe quindi essere incoraggiato, poiché rappresenta una misura di privacy by design di grande utilità.

7. Valutazione d'impatto sulla protezione dei dati personali (artt. 35 e 36 del GDPR)

Per consentire un'adeguata ponderazione di tutti gli aspetti sopra rappresentati (ma non solo), il GDPR ha introdotto un altro strumento. Si tratta della valutazione d'impatto sulla protezione dei dati personali, che il titolare deve effettuare preliminarmente all'avvio del trattamento, e che serve proprio a definire la cornice e le caratteristiche del trattamento stesso, al fine di individuare tutte le misure volte a minimizzare i rischi.

La valutazione d'impatto non è obbligatoria in via generale per tutti i trattamenti.

Lo diventa tuttavia per il settore dell'osservazione mediante SAPR, in quanto l'art. 35 del GDPR la impone quando viene effettuata la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Peraltro, la parte B dell'allegato al citato regolamento UE di esecuzione 2019/947 obbliga il pilota di drone a stabilire procedure e limitazioni adeguate al tipo di operazione previsto e al rischio connesso, tra cui: misure volte a impedire interferenze illecite o accessi non autorizzati; procedure volte a garantire che tutte le operazioni rispettino il GDPR; orientamenti per i piloti al fine di ridurre al minimo il disturbo a persone e animali; designazione e responsabilizzazione dei piloti con l'attribuzione di specifici compiti. Tra queste procedure vi rientra, in particolare, l'espressa necessità di effettuare una valutazione d'impatto ai sensi dell'art. 35 del GDPR.

8. Sicurezza (artt. 5, par. 1, lett. f), e 32 del GDPR

Gli aspetti di sicurezza sono ovviamente tra i più nevralgici al giorno d'oggi: gli accessi abusivi o non autorizzati rappresentano uno dei rischi più concreti connessi ai trattamenti effettuati mediante dispositivi tecnologici.

Per non parlare della perdita di disponibilità dei dati che, oltre a comprometterne la riservatezza, mette a rischio l'integrità delle informazioni e la continuità delle funzioni, che invece deve essere sempre garantita. Non dimentichiamo che informazioni sbagliate, perché magari nel frattempo sono state manipolate, rappresentano un danno non solo alla dignità degli individui (se si tratta di dati personali), ma anche alla genuinità e credibilità della ricerca.

Sicuramente ci sono delle misure di sicurezza di base che riguardano le banche dati in cui confluiscono le informazioni raccolte mediante droni. Rientrano in questo ambito: l'individuazione dei soggetti autorizzati all'accesso; le forme di autenticazione; la cifratura delle informazioni; forme di *back up* e misure di *disaster recovery*.

Nel nostro specifico caso, vi è poi da considerare la peculiarità connessa alle modalità di acquisizione dei dati. Il più delle volte questi vengono raccolti su apposite schede di memoria caricate sul drone stesso: una volta terminate le operazioni, la scheda viene prelevata ed il suo contenuto immesso all'interno di un archivio.

Tuttavia, potrebbe esservi l'eventualità che le immagini captate vengano trasmesse in *streaming* dal SAPR al cruscotto del pilota oppure, addirittura, nella banca dati destinata alla loro conservazione. In questo caso occorre assicurare canali di trasmissione sicuri, per evitare che il flusso possa venire intercettato, ad esempio, tramite comuni *hot spots wi fi*, e comunque da parte di impianti ricetrasmittenti esterni.

In ogni caso, l'approccio di accountability vale anche nella predisposizione delle misure di sicurezza. Oggi non è più una questione di misure minime stabilite per legge, come prevedeva il Codice previgente; oggi deve essere garantito un livello adeguato rispetto al trattamento, i quali cambiano a seconda delle modalità di effettuazione, del contesto, della tipologia e mole di dati trattati, dei rischi connessi. Pertanto, la valutazione

di impatto deve servire proprio a cercare di prevedere tutti gli scenari probabili, e quindi di adottare le misure utili e minimizzare i rischi. Sapendo che, se non vi si riesce, occorre consultare l'Autorità.

9. Meccanismi di certificazione e codici di condotta per piloti (artt. 40 e 42 del GDPR)

Il GDPR fornisce ulteriori strumenti in grado di aiutare i titolari nell'effettuare trattamenti in un quadro di garanzie sempre più affidabile.

Uno di questi è rappresentato dai meccanismi di certificazione, su cui comunque già la normativa sui SAPR è ricca di prescrizioni rivolte sia ai produttori che agli utilizzatori.

Un altro è rappresentato dai codici di condotta, che possono invece costituire un valido strumento per la creazione di regole, autoprodotte da parte degli stessi utilizzatori, in grado di vincolare in maniera più forte i trattamenti rispetto ai principi della protezione dati.

Ad esempio, la promozione di un codice di condotta per i piloti di SAPR potrebbe costituire uno strumento utile per accrescere la consapevolezza dei rischi e una cultura della responsabilità in grado di consentire l'utilizzo dei droni in un contesto sempre più sicuro.

10. Quelle appena riportate rappresentano una prima riflessione sulle implicazioni legate alla necessità di dare piena e coerente applicazione al quadro normativo tracciato dal Regolamento europeo (GDPR) ai trattamenti di dati personali effettuati mediante aeromobili a pilotaggio remoto. Si tratta di indicazioni sull'operatività in concreto degli istituti giuridici, tutti improntati alla responsabilizzazione del titolare e alla predeterminazione delle caratteristiche e delle garanzie.

Rimane indubbia la necessità di interventi di carattere più generale, che forniscano quantomeno un quadro minimo di garanzie applicabile a tutte le molteplici possibilità di utilizzo di droni. E le Autorità di protezione dati, a livello europeo, potrebbero anche promuovere azioni in questo senso.

Così come va ribadito che, per utilizzi specifici come quelli volti a perseguire finalità di interesse pubblico, non è possibile discostarsi dal quadro normativo, poiché solo il diritto positivo di rango primario (o secondario) può stabilire circostanze ulteriori, circondandole ovviamente delle necessarie garanzie: non dimentichiamo che con i droni, più che con la videosorveglianza, è possibile entrare nelle abitazioni (o comunque nelle aree di domicilio) e monitorare i comportamenti di persone in movimento. E questa può rappresentare una forte compressione delle libertà individuali.

Cultura giuridica e diritto vivente

Cultura giuridica e diritto vivente è espressione del Dipartimento di Giurisprudenza (DiGiur) dell'Università di Urbino. Lo sviluppo e la manutenzione di questa installazione di OJS sono forniti da UniURB Open Journals, gestito dal Servizio Sistema Bibliotecario di Ateneo. **ISSN 2384-8901**