

Bilanciamento tra utilizzo droni e tutela della privacy

Autore: Federica Masini

In: Diritto civile e commerciale

Dal punto di vista dell'utilizzo dei droni, in ambito civile, è importante evidenziare le problematiche che possono sorgere con riferimento alla **tutela privacy**[1].

Infatti, la natura di tali mezzi li rende intrinsecamente idonei ad acquisire dati grazie alle tecnologie avanzate di cui sono dotati, quali sistemi di registrazione visiva, sensori, microfoni, riconoscimenti facciali, scanner a raggi infrarossi, sensori ottici, antenne: tutti sistemi in grado di registrare la posizione e captare informazioni, invadendo la sfera personale dell'individuo e interferendo con i dati sensibili dei privati.

Non è, quindi, il drone in sé considerato, ma tutto quello che può essere impiantato al suo interno che è **suscettibile di acquisire informazioni personali**, ossia l'equipaggiamento comprendente tutte quelle tecnologie sopra menzionate tali da ingenerare agli operatori diverse problematiche sotto l'aspetto della privacy nell'espletamento delle operazioni SAPR.

Entrano, quindi, in gioco due differenti questioni: quella della tutela della privacy e quella della protezione dei dati personali, involgendo quindi sia l'aspetto dell'acquisizione che dell'uso dei dati personali eventualmente ottenuti[2].

I droni hanno una capacità di captare informazioni e potenzialmente potrebbero sorvegliare una vastità di aree e una moltitudine di persone e quindi è importante cercare di adattare l'utilizzo dei droni alle esigenze di tutela della privacy, in quanto entrano in gioco diritti fondamentali della persona come il diritto alla vita privata e familiare incluso lo stesso diritto alla protezione dei dati personali[3].

Si legga anche:" Breve evoluzione normativa in materia di droni"

Droni e normative di riferimento

Sul punto è importante citare la Dichiarazione di Riga del 6 marzo 2015, che ha come oggetto: "on remotely piloted aircraft (drones) "framing the future of aviation" in cui si evidenzia la necessità di armonizzare la disciplina dei droni in Europa al fine di garantire la protezione dei diritti fondamentali dei cittadini quali il diritto alla privacy e alla protezione dei dati personali; attraverso la cooperazione delle autorità nazionale e sovranazionali (par. 4).

Nel 2016 il Regolamento EU 2016/679[4] “relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)” ha riformato la materia della tutela dei dati personali, disciplinandone altresì la circolazione avendo però riguardo all’esigenza di protezione delle libertà e dei diritti fondamentali con specifico riferimento al diritto alla protezione dei dati personali[5].

Utilizzo dei droni e tutela dei dati personali

Ebbene, con riferimento alla materia che forma oggetto del presente lavoro, occorre innanzitutto precisare che, al fine di garantire il rispetto dei diritti e la tutela dei dati personali è necessario che **il drone abbia fin dall’inizio della sua progettazione** e - quindi si potrebbe dire “**di default**” i requisiti e le misure necessarie per garantire sicurezza dei dati acquisiti durante le operazioni[6].

Nell’ambito di tali operazioni dei SAPR è possibile vedere come ci sia un **bilanciamento tra diritti economici, di proprietà intellettuale e il diritto alla riservatezza, alla tutela dei dati personali e dell’immagine**[7].

Per quanto riguarda le informazioni raccolte per mezzo dei droni è importante precisare quali siano i dati[8] che vengono raccolti, dagli stessi; infatti, questi sistemi aerei a pilotaggio remoto hanno capacità di **raccogliere infiniti dati**[9] grazie alle loro potenzialità di muoversi nello spazio anche in poco tempo e catturando allo stesso tempo immagini e informazioni e dati[10].

Già con il decreto legislativo 196/200[11] all'articolo, 5 comma 3, si prevedeva che le informazioni di carattere personale acquisite potevano essere utilizzate in ambito domestico o personale.

Allo stato attuale l’articolo 2, comma 2, lettera c, del regolamento (UE) n. 2016/679 dispone che non si applica la disciplina relativa alla protezione dei dati personali e il suddetto regolamento quando le informazioni private siano state raccolte da una persona fisica per l’esercizio di attività a carattere esclusivamente personale o domestico.

Pertanto, per quanto concerne i droni, è pacifico che nel caso di utilizzo di tali sistemi per scopi personali, quindi per uso non commerciale, professionale o economico, i cui dati non vengano quindi diffusi al pubblico, si esula dall’ambito di applicazione del GDPR escludendo quindi ogni responsabilità sotto l’aspetto della protezione dei dati personali.

L’applicazione della disciplina in tema di privacy deve comunque tener conto pur sempre di altre **esigenze contrapposte**, in primis economiche, di cui sono titolari il committente, l’operatore SAPR e pilota APR, da contemperare con quella del rispetto dei dati personali: occorre in ogni caso garantire il risultato dell’operazione, non potendo la tutela della privacy costituire un ostacolo in tal senso (ad. Es.

deve ritenersi consentita la ripresa di soggetti che si trovino ad attraversare una zona oggetto di sorveglianza attraverso il drone).

Il regolamento generale sulla protezione dei dati regolamento (UE) n. 2016/679 del Parlamento europeo del consiglio europeo del 27 Aprile 2016: all'articolo 6 rubricato "liceità del trattamento" dispone che: "a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; (C42, C43) b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; (C44) c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; (C45) d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; (C46) e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; (C45, C46) f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore".

Inoltre, il medesimo articolo fa salva la possibilità per gli Stati membri di specificare e introdurre disposizioni più adeguate rispetto a quelle sopra menzionati.

L'articolo 35 sulla valutazione d'impatto sulla protezione dei dati disciplina invece il trattamento dei dati personali nel contesto dell'utilizzo di nuove tecnologie, quindi in particolar modo anche l'utilizzo dei droni; infatti, nel paragrafo 2 si parla di "valutazione d'impatto"[12]in base ai dati personali acquisiti, facendo una valutazione e una sorveglianza sistematica dell'area[13].

Regolamento Enac: protezione dei dati personali e privacy

Partendo con l'analisi della normativa nazionale il Regolamento ENAC, all'articolo 35 "Protezione dei dati e privacy" dispone che, al fine del rilascio dell'autorizzazione, nella richiesta deve essere indicato se nell'operazione verranno acquisiti dei dati e delle informazioni personali e che però, si rispetteranno le normative presenti all'interno del codice privacy.

Sul tema il 27-29 ottobre 2010 si è tenuta la Conferenza mondiale dei Garanti della privacy avente ad oggetto la **c.d. Privacy by Design (PbD)**, con particolare riguardo al rapporto tra il trattamento dei dati personali e l'utilizzo di determinate tecnologie, quali, per quanto di interesse in questa sede, i droni. Tale conferenza ha avuto come scopo ben preciso, quello di individuare soluzioni operative tali da garantire la sicurezza del trattamento di dati personali mediante mezzi tecnologici [14].

Sul punto, uno studio della Commissione europea, in un progetto chiamato "Robolow" aveva **precisato che l'applicazione di tale formula sarebbe stata in grado di evitare problemi per quanto**

riguarda il trattamento dei dati personali[15].

Per quanto concerne i droni, nel contesto della strategia “Privacy by design” potrebbe ad esempio rilevare, al fine di agevolare la sicurezza del trattamento dei dati personali e il rispetto dei diritti dei soggetti coinvolti, **l’installazione nei mezzi in questione di software** in grado di procedere, in caso di rilevazione dei volti delle persone, al successivo oscuramento degli stessi.

già la Direttiva 95/46/CE[16] all’interno dell’articolo 17, prevedeva espressamente l’obbligo in capo agli Stati membri di introdurre nei rispettivi ordinamenti specifiche disposizioni che imponessero al responsabile del trattamento dei dati di dotarsi di misure, sia tecniche che organizzative, idonee ad assicurare la protezione dei dati acquisiti durante le operazioni[17].

Anche nel regolamento generale sulla protezione dei dati[18] all’articolo 25 “Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita” emerge la particolare importanza del concetto di “Privacy by design”, per cui **l’acquisizione dei dati personali deve essere limitata già dalla progettazione e produzione di sistemi tecnologici** (quali, nel caso che ci occupa, i droni), prevedendo a monte i costi necessari ad assicurare detto risultato. Inoltre, particolare rilievo assume il processo di pseudonimizzazione, attraverso il quale ex ante vengono stabiliti, secondo impostazioni predefinite, i dati che dovranno necessariamente essere raccolti e trattati. Il legislatore europeo ha introdotto poi un certificato, necessario per attestare l’osservanza delle norme in punto di trattamento dei dati personali, disciplinato dall’articolo 42[19] rubricato “Certificazione” - il cui quarto comma precisa, comunque che la certificazione non esenta di per sé il soggetto da responsabilità nel caso in cui si accerti una violazione del diritto alla privacy e della protezione dei dati personali.

Tali obblighi di minimizzazione, anonimato etc. **perdurano per tutto il tempo del trattamento**, e devono essere conservati in modo da non poter essere utilizzati da soggetti terzi, se non previa autorizzazione della persona interessata (c.d. impostazione predefinita).

Inoltre, con riguardo al rapporto tra i droni e l’acquisizione di dati personali e, in particolare di fotogrammi durante le operazioni viene in rilievo anche l’articolo 10 del Codice civile [20], rubricato “Abuso dell’immagine altrui”, in virtù del quale si prevede un apposito rimedio giudiziale per la tutela del diritto all’immagine, che costituisce un aspetto del più ampio diritto alla riservatezza e all’identità personale.

Inoltre, nel 2017 l’allora segretario del Garante della privacy, Giuseppe Busia, evidenziò che, nel caso di riprese divulgative a mezzo di droni in cui compaiono soggetti terzi è necessario ottenere la previa autorizzazione di tali persone. Lo stesso aggiunse che nel caso in cui tali persone non siano reperibili o comunque risultino difficili da rintracciare, ai fini

dell’autorizzazione, occorre ricorrere a quegli **strumenti informatici**, precedentemente menzionati, che consentono la **minimizzazione o la pseudonimizzazione**[21].

Volume consigliato

Note

[1] La privacy è un ambito circoscritto della vita personale e privata ed è regolato da delle leggi su tale argomento che difatti tutelano la persona e l'utilizzo dei dati personali. In Italia è possibile trovare una figura chiamata garante per la protezione dei dati personali e il codice della privacy istituito con un decreto legislativo del 30 giugno 2003 n. 196 che predispone la normativa nazionale in base all' adeguamento delle disposizioni rinvenute all'interno del regolamento dell'unione europea 2016/697. Ci sono diversi ambiti in cui opera il codice della privacy come, ad esempio, per quanto riguarda la tutela della salute, dell'incolumità fisica la sicurezza nazionale il trattamento dei dati personali in ambito pubblico (disciplinati dalla legge 7 agosto 1990 n. 241), per quanto riguarda l'utilizzo dei dati pubblici nei registri e negli albi professionali.

[2] DAVOLA. A., L'acquisizione di dati da parte dei privati nelle operazioni SAPR, in *Diritto dei droni Regole, questioni e prassi*, a cura di Erica Palmerini, Maria Angela Biasiotti, Giuseppe Francesco Aiello, Milano, Giuffrè, 2018, p.137 ss.

[3] DUCATO R., Droni per il search and rescue in aree valanghivive: profili privatistici in *Diritto dei droni*, 2018, pp. 379-421, a cura di Erika Palmerini, Maria Angela Biasiotti, Giuseppe Francesco Aiello.

[4] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[5] L'articolo 1 del regolamento (UE) 2016/679 dispone che: " Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali."

[6] Considerando n. 79 del Regolamento (UE) n. 2016/679 ("GDPR").

[7] MALGIERI G., La titolarità dei trattati per mezzo dei droni tra privacy e proprietà intellettuale, in

Diritto dei Droni, 2018, pp. 163-196, a cura di Erika Palmerini, Maria Angela Biasiotti, Giuseppe Francesco Aiello.

[8] L'articolo 4 comma 1 lettera b del D.Lgs. 196/2003 disponeva che per dato personale si intende: "qualunque informazione relativa a persona fisica, identificativa o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale."

[9] Article 29 Data Protection Working Party. Il Gruppo di lavoro "Articolo 29" (Art. 29 WP) era il gruppo di lavoro europeo indipendente che, fino al 25 maggio del 2018 (entrata in vigore del RGPD) aveva lo scopo di occuparsi di questioni relative alla protezione della vita privata e dei dati personali., sito web: https://edpb.europa.eu/our-work-tools/article-29-working-party_it.

[10] È possibile classificare i dati in base ai diritti soggettivi in gioco, a) dati personali che hanno ad oggetto il nome un numero di identificazione, elementi che vanno a dare un'identificazione fisica, fisiologica, psichica (ad esempio, foto, targhe); b) dati personali sensibili, che manifestano l'origine razziale, opinioni politiche, status familiare, orientamento sessuale, o dei satì che sono inequivocabili per identificare la persona; c) opere dell'ingegno, come disciplinato ai sensi dell'articolo 2 comma 7 della legge 633/1933 sul diritto d'autore in cui si dispone che: "E' considerato autore dell'opera collettiva chi organizza e dirige la creazione dell'opera stessa. È considerato autore delle elaborazioni l'elaboratore, nei limiti del suo lavoro.", come ad esempio fotografia, dipinti, pellicole cinematografiche; d) segreti commerciali che sono qualunque informazione che ha un valore economico, che sono segrete e che sono sottoposte a misure atte a preservare la riservatezza.

[11] Codice privacy decreto legislativo 30 giugno 2003, n.196 modificato con D. Lgs. 10 agosto 2018, n. 101.

[12] L'articolo 35 del regolamento (UE) nel comma 7 dispone che: "a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione".

[13] In dottrina come anche riportato in MOEREL L. e PRINS C. in Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things e nell'articolo 29 Working Party gli elementi che bisogna valutare se effettivamente vi è una prevalenza del titolare per quanto riguarda l'acquisizione dei dati personali: " a) il modus con cui i dati vengono adoperati, b) l'an e il quomodo dell'utilizzo dei dati, c) la relazione tra il titolare del trattamento e i soggetti interessati, d) la tutela dei dati, e come minimizzare l'utilizzo di esso (es. pseudonomizzazione, minimizzazione).

[14] LOBIANCO R., Mezzi aerei a pilotaggio remoto: brevi osservazioni sul regolamento ENAC, in *Responsabilità civile e previdenza*, 6, 2017, p. 2078 e ss.

[15] ROBOLAW, Guidelines on Regulating Robotics. EU Project on Regulating Emerging Robotic Technologies in Europe: Robotics Facing Law and Ethics, 2014, p. 19.

[16] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[17] MERLA L. Droni, privacy e tutela dei dati personali in *Informatica e diritto*, XLII annata, Vol. XXV, 2016, n. 1, p. 33 ss.

[18] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, Arricchito con riferimenti ai Considerando, aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018 (Regolamento generale sulla protezione dei dati).

[19] L'articolo 42 del regolamento (UE) n. 2016/679 dispone che:” 1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.

Oltre all'adesione dei titolari del trattamento o responsabili del trattamento soggetti al presente regolamento, i meccanismi, i sigilli o i marchi approvati ai sensi del paragrafo 5 del presente articolo possono essere istituiti al fine di dimostrare la previsione di garanzie appropriate da parte dei titolari del trattamento o responsabili del trattamento non soggetti al presente regolamento ai sensi dell'articolo 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera f). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati. 3. La certificazione è volontaria e accessibile tramite una procedura trasparente. 4. La certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti a norma degli articoli 55 o 56. 5. La certificazione ai sensi del presente articolo è rilasciata dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente ai sensi dell'articolo 58, paragrafo 3, o dal comitato, ai sensi dell'articolo 63. Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati. 6. Il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al

meccanismo di certificazione fornisce all'organismo di certificazione di cui all'articolo 43 o, ove applicabile, all'autorità di controllo competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione.7. La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i criteri pertinenti. La certificazione è revocata, se del caso, dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente, a seconda dei casi, qualora non siano o non siano più soddisfatti i criteri per la certificazione. 8. Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.

[20] L'articolo 10 del Codice civile dispone che: "genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato,

Qualora l'immagine di una persona o dei può disporre che cessi l'abuso, salvo il risarcimento dei danni."

[21]PRISCO F., Droni "guardoni", Cosa si deve sapere quando ti sorvolano, in Il sole 24 ore, 28 settembre 2017.

<https://www.diritto.it/bilanciamento-tra-utilizzo-droni-e-tutela-della-privacy/>