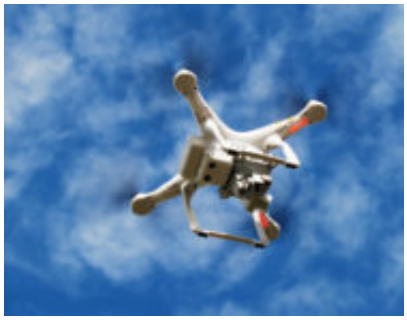
Sotto l’occhio dei droni. Profili giuridici connessi alla videosorveglianza tramite gli aerei a pilotaggio remoto

Author : Orsolina Fortini

Date : 18 Gennaio 2019



Introduzione

L’evoluzione tecnologica è in continuo sviluppo e ogni giorno vengono messi a disposizione nuovi strumenti e soluzioni sempre più sofisticate che consentono di soddisfare le più svariate esigenze. In tale quadro, l’utilizzo dei droni originariamente manifestatosi e ormai consolidatosi in ambito militare, è sempre più diffuso anche in ambito civile da parte di imprese e altri soggetti privati con finalità diverse, ad esempio in relazione ad operazioni di sicurezza territoriale, ad operazioni di telerilevamento, ad operazioni di aerofotogrammetria e rilievo dell’architettura, al monitoraggio dell’ambiente e della fauna selvatica, ad operazioni di ricerca e soccorso nonché, in generale, alle attività di videoriprese e fotografie, effettuate a fini economici ovvero ricreativi.

Scopo del presente contributo è quello di riflettere sui rischi legati alla *privacy* derivanti dall’utilizzo dei droni. In particolare, l’utilizzo dei droni solleva problemi legati al trattamento dei dati personali dei soggetti che sono resi oggetto di videosorveglianza per il tramite di tali mezzi.

Che cosa sono i droni?

Con il termine “droni” si designano i mezzi aerei a pilotaggio remoto (APR) che operano autonomamente o vengono pilotati a distanza. La definizione di drone è ricavabile dal glossario dell’Organizzazione internazionale dell'aviazione civile (CIR328, 2011), dalla normativa europea (art. 30, n. 30, Reg. UE 2018/1139 del Parlamento europeo e del Consiglio del 4 luglio 2018, entrato in vigore l’11 settembre 2018, recante norme comuni nel settore dell'aviazione civile, il “Reg. UE 2018/1139”) oltre che dalla normativa nazionale (artt. 1 e 5, Regolamento ENAC - Ente Nazionale per l'Aviazione Civile, il “Reg. ENAC”). Esistono più categorie di droni con caratteristiche e capacità anche molto diverse tra loro.

Perché l’utilizzo dei droni solleva problemi in ambito *privacy*?

Sebbene i droni offrano indubbi vantaggi rispetto ai mezzi aerei tradizionali a livello di elusione

di rischi di vario genere (legati innanzitutto alla sicurezza – si pensi al monitoraggio tramite droni delle c.d. *no go zone*) nonché di costi economici, essi presentano al tempo stesso considerevoli criticità sul piano giuridico.

Se in un primo momento l'uso dei droni ha destato preoccupazioni esclusivamente in merito ai profili legati alla sicurezza, successivamente, in virtù dell'espansione dell'impiego dei droni in ambito civile sono state sollevate numerose criticità relative all'interferenza dell'uso dei droni con il diritto alla riservatezza e, più specificamente, alla protezione dei dati personali. I droni, infatti, impattano sulla protezione dei dati personali di soggetti terzi in relazione ai sistemi di videosorveglianza in essi incorporati, i quali comportano potenziali trattamenti di dati personali (quali immagini e dati relativi all'ubicazione) relativi a persone identificate o identificabili, che possono esservi soggette senza nemmeno rendersene conto.

Qual è la normativa di riferimento?

Attualmente la normativa in materia di droni è disorganica e frammentaria. All'utilizzo di droni, infatti, risulta applicabile un insieme di discipline settoriali, nazionali ed europee. Il Regolamento UE 2018/1139 e il Reg. ENAC costituiscono i due principali testi normativi di riferimento. Essi, tuttavia, non prevedono alcuna tutela specifica rispetto alla protezione dei dati personali.

Il Reg. ENAC, all'art. 34, per quanto riguarda il trattamento dei dati personali rinvia espressamente alla normativa di settore in materia di *privacy*. Anche il Regolamento UE 2018/1139 non contiene disposizioni specifiche in relazione alla protezione dei dati personali ma opera un rinvio alla normativa sulla *privacy* – pur contenendo deleghe alla Commissione europea per l'adozione di norme attuative volte alla tutela della *privacy* correlata all'utilizzo dei droni (ci si riferisce all'istituzione di sistemi di immatricolazione digitale dei droni e i loro operatori nel caso in cui l'utilizzo dei droni comportino rischi per la riservatezza e la protezione dei dati personali ex art. 57 e All. IX, artt. 4.1 e 4.2) e la previsione secondo la quale, se necessario al fine di attenuare i rischi inerenti alla sicurezza, alla tutela della riservatezza, alla protezione dei dati personali, alla *security* o all'ambiente derivanti dal loro esercizio, gli aeromobili senza equipaggio devono possedere le relative caratteristiche e funzionalità specifiche che tengono conto dei principi della tutela della riservatezza e della protezione dei dati personali fin dalla progettazione e per impostazione predefinita (All. IX, art. 1.3).

Ne consegue che il quadro normativo di riferimento è costituito essenzialmente dal Regolamento UE 2016/679 ("GDPR") e dal D.lgs. 101/2018 di adeguamento del Codice *Privacy* alle disposizioni del GDPR, oltre che dalle linee guida e ai provvedimenti delle Autorità competenti in ambito *privacy* (si segnala che queste ultime fonti sono antecedenti al GDPR e occorrerà, di conseguenza, leggerle alla luce dei principi del GDPR). La normativa sulla *privacy*, peraltro, non prevede allo stato una regolamentazione specifica sulla protezione dei dati personali dei soggetti sottoposti alla videosorveglianza tramite l'utilizzo dei droni.

Da quanto sopra descritto emerge come sia necessario un quadro normativo che preveda una tutela specifica rispetto alla protezione dei dati personali dei soggetti sottoposti alla videosorveglianza tramite i droni. Come spesso accade, anche in questo settore l'intenso dinamismo della tecnologia procede molto più velocemente del legislatore.

I droni sono in sé pericolosi?

L’Opinion 01/2015 on *Privacy* and Data Protection Issues relating to the Utilisation of Drones adottata il 16 giugno 2015 dal WP29 (ora “Comitato Europeo per la protezione dei dati personali”) (“Opinion 01/2015”) chiarisce che l’utilizzo dei droni in sé non presenta particolare problematiche, le quali invece risultano collegate agli effetti invasivi derivanti dall’uso di dispositivi installati sui droni stessi, quali, ad esempio, gli impianti di videosorveglianza.

Quando il trattamento dei dati può considerarsi ***privacy compliant*****?**

Ai sensi del GDPR, tutte le attività e gli strumenti che comportano il trattamento dei dati personali – tra i quali rientrano i sistemi di videosorveglianza dei droni – devono conformarsi alle disposizioni contenute nella stessa normativa. Molte attività effettuate tramite i droni consistono proprio nella raccolta e nel trattamento di dati quali immagini, foto e video. Peraltro, si rammenta che anche la semplice raccolta dei dati, senza ulteriore registrazione o conservazione, costituisce un trattamento di dati personali ai sensi dell’art. 4, n. 2 GDPR. Non costituisce, invece, trattamento di dati personali, e non si applica la suddetta normativa, il caso di utilizzo delle immagini o dei video raccolti tramite i droni utilizzati da una persona fisica per l’esercizio di attività a carattere esclusivamente personale o domestico (art. 2, comma 2 lett. c GDPR).

Per essere conforme al GDPR, il trattamento dei dati effettuato tramite attività di videosorveglianza deve rispettare i principi in esso contenuti (liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazioni, integrità e riservatezza, responsabilizzazione – art. 5 GDPR). È evidente che la difficoltà dei soggetti sottoposti alla videosorveglianza di recepire la presenza dei droni e degli strumenti in essi incorporati può comportare la violazione dei principi richiamati in mancanza di idonee accortezze.

È sempre obbligatorio effettuare la DPIA?

In ossequio al principio di liceità, quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il titolare del trattamento è tenuto ad effettuare una valutazione d’impatto *privacy* (c.d. “DPIA”) prima dell’inizio del trattamento dei dati al fine di individuare la probabilità e la gravità dei rischi e al fine di minimizzarli (art. 35, comma 3 GDPRLinee guida del WP29 concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 adottate il 4 aprile 2017 come modificate e adottate il 4 ottobre 2017 e approvate dal Comitato Europeo per la protezione dei dati personali in data 25 maggio 2018; Provvedimento dell’Autorità Garante per la protezione dei dati personali n. 467 dell'11 ottobre 2018 recante “Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell’art. 35, comma 4, del Regolamento (UE) n. 2016/679”).

Pertanto è da ritenersi che, in via generale, la DPIA vada effettuata in caso di trattamento dei dati derivante dall'utilizzo dei droni qualora la videosorveglianza si traduca in un monitoraggio sistematico (ossia allorquando la raccolta di dati avvenga in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà) su larga scala, comportando quindi un rischio elevato.

Qual è la base giuridica del trattamento dei dati effettuato mediante videosorveglianza tramite i droni?

Per essere considerato lecito, il trattamento dei dati personali deve essere effettuato in virtù di una determinata base giuridica, quale il rilascio del consenso informato, l'esecuzione di un contratto, la salvaguardia di interessi vitali dell'interessato o di un'altra persona fisica, l'esecuzione di un compito di interesse pubblico di cui è investito il titolare del trattamento, il perseguimento del prevalente legittimo interesse del titolare del trattamento o di terzi che risulti prevalente rispetto all'interesse dei soggetti interessati a non essere ripresi (si pensi al caso in cui l'attività di videosorveglianza venga effettuata sulla base del legittimo interesse alla tutela del patrimonio aziendale di un'impresa che effettui attività di videosorveglianza dei propri stabilimenti tramite droni) (art. 6 GDPR).

Come si può ottenere il consenso informato?

Per quanto riguarda il tema del consenso informato, le modalità con cui l'informativa può essere fornita da parte del titolare del trattamento effettuato mediante videosorveglianza tramite i droni e l'ottenimento del consenso degli interessati appaiono alquanto problematici, se si considera che il drone è un dispositivo spesso non percepibile e il pilota del drone può non avere contezza dei soggetti sottoposti a videosorveglianza.

A tale riguardo, il WP29, nell'Opinion 01/2015, suggerisce un approccio "*multilivello*": da cartelli o simboli predisposti all'ingresso di una zona sottoposta a sorveglianza tramite droni, a dispositivi che lanciano segnali o luci facilmente visibili, a informative pubblicate sui siti *web* degli operatori e/o su piattaforme uniche che raccolgano informazioni sui voli dei droni, quali ad esempio i siti *web* delle Autorità di aviazione competenti. Nei casi in cui non sia possibile l'accesso al sito internet, l'informativa può essere pubblicata su giornali, tramite poster o lettera inserita nelle cassette delle lettere.

Peraltro il consenso non risulta necessario qualora l'attività di videosorveglianza venga effettuata in virtù della diversa base giuridica consistente nel legittimo interesse del titolare.

Come si applicano i principi di *privacy by design* e di *privacy by default* ai droni?

Nella progettazione e nell'utilizzo dei droni risulta necessario tenere inconsiderazione i principi di *privacy by design* e di *privacy by default*.

In base al primo principio, i produttori di droni dovranno considerare la tutela dei dati personali

sin dalla fase di progettazione dello strumento che tratterà tali dati, in modo da realizzare un prodotto finale che riduca al minimo l'utilizzo dei dati stessi. I dispositivi di videosorveglianza incorporati nei droni dovrebbero inoltre essere progettati con tecnologie tali da consentire di prestabilire un periodo di conservazione dei dati personali raccolti e, di conseguenza, la cancellazione automatica dei dati personali non più necessari.

In base al secondo principio, invece, gli utilizzatori del drone, in qualità di titolari del trattamento, dovranno adottare misure tecniche e organizzative adeguate per garantire che siano trattati solo i dati necessari per la finalità perseguita.

Che cosa prevede il Provvedimento in materia di videosorveglianza dell'Autorità Garante per la protezione dei dati personali?

Il Provvedimento in materia di videosorveglianza emanato in data 8 aprile 2010 dall'Autorità Garante per la protezione dei dati personali non ha ad oggetto specificamente i droni ma prevede indicazioni generali relativamente all'attività di videosorveglianza.

In particolare viene previsto l'obbligo di segnalazione della presenza dei sistemi di videosorveglianza e la comunicazione del titolare del trattamento relativa alle finalità del trattamento dei dati trattati, in conformità a quanto previsto all'art. 13 GDPR.

Si ritiene che una tale previsione, volta a consentire ai soggetti che si approssimino all'area interessata dalle riprese di essere avvisato della presenza di telecamere già prima di entrare nel loro raggio di azione, debba applicarsi, *a fortiori*, in caso di utilizzo di dispositivi quali i droni, che spesso sono difficilmente percettibili.

Per quanto riguarda la conservazione dei dati raccolti, il provvedimento stabilisce un limite di tempo (pari a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve le eccezioni legate a speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso di adesione ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria).

Come rispettare la *privacy* quando si usa un drone a fini ricreativi?

L'Autorità Garante per la protezione dei dati personali ha fornito alcuni consigli per rispettare la normativa in materia di protezione dei dati personali nel caso di utilizzo di droni a fini ricreativi. Il documento in parola è stato aggiornato da ultimo lo scorso 9 novembre. I consigli dell'Autorità Garante si possono riassumere nei seguenti punti:

- Evitare di invadere gli spazi personali e l'intimità altrui in caso di utilizzo di un drone munito di fotocamera e/o videocamera in luoghi pubblici, quali ad esempio parchi, strade, spiagge, allo scopo di effettuare riprese che possano coinvolgere terze persone. Occorre inoltre evitare di riprendere (e diffondere) immagini contenenti dati personali quali targhe di automobili o indirizzi di casa. Le riprese che violano gli spazi privati altrui (quali la casa o il giardino domestico) sono sempre da evitare, anche perché la raccolta

e il trattamento di dati personali, oltre a violare la normativa *privacy*, rilevano sotto il profilo penale, essendo l'interferenza illecita nella vita privata punita dal codice penale.
- Diffusione delle riprese: la diffusione di immagini e video ripresi con il drone sul *web*, *social network* o in *chat* è consentita solo in presenza del consenso dei soggetti ripresi, ad eccezione di particolari usi connessi alla libertà di espressione, quali quelli giornalistici. Negli altri casi, se risulta eccessivamente difficoltoso raccogliere il consenso dei soggetti interessati, è possibile diffondere le immagini solo ove i soggetti ripresi non siano identificabili, o perché ripresi da lontano o perché si sono oscurati i loro volti.
- Rispetto degli altri: la presenza di un drone che effettua riprese nelle vicinanze può dare la sensazione di essere osservati, inducendo disagio e influenzando il normale comportamento delle persone. È quindi buona regola utilizzare tali strumenti senza invadere la sfera personale degli altri, magari anche comunicando preventivamente le proprie intenzioni. Un'altra buona pratica da seguire è quella di fare in modo che il pilota del drone sia sempre ben visibile, così da non suscitare sospetti o allarme negli altri.
- Non diventare un "orecchio indiscreto": non si possono usare droni per captare volontariamente conversazioni altrui. Eventuali frammenti di conversazione registrati in modo accidentale possono essere utilizzati (ad esempio pubblicati sul *web*) solo se non rendano riconoscibili il contesto, cioè il contenuto dei discorsi, e le persone coinvolte.
- *Privacy by design e by default*: ai sensi del GDPR e come ribadito anche dal Reg. UE 2018/1139, i droni devono essere progettati, configurati e utilizzati secondo misure tecniche e organizzative conformemente alle norme sulla tutela dei dati personali, raccogliendo solo i dati necessari e proporzionati rispetto alle finalità perseguite.

Considerazioni finali

L'utilizzo dei droni sta avendo un impatto molto rilevante per quanto concerne la protezione dei dati personali dei soggetti sottoposti alla loro videosorveglianza. L'analisi del quadro normativo di riferimento fa emergere l'urgenza di una normativa che offra tutele più specifiche per gli interessi dei singoli, in considerazione della sempre maggiore diffusione dell'utilizzo dei droni in diversi ambiti e dell'evoluzione tecnologica applicata a tali strumenti. Nell'attesa di un intervento del legislatore, si raccomanda alle imprese e ai soggetti che si avvalgono di tali strumenti di riferirsi ai principi e alle regole vigenti in materia di *privacy*.

Fonti:

- Regolamento ENAC edizione 2 del 16 luglio 2015, emendata in data 21 maggio 2018
- Regolamento UE 2018/1139 recante norme comuni nel settore dell'aviazione civile
- Regolamento UE 2016/679 (c.d. GDPR)
- Linee guida del WP29 concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 adottate il 4 aprile 2017 come modificate e adottate il 4 ottobre 2017, 17/IT – WP 248 rev.01
- Opinion 01/2015 on *Privacy* and Data Protection Issues relating to the Utilization of Drones, 16 giugno 2015, 01673/15/EN – WP 231

- Garante per la protezione dei dati personali, Provvedimento in materia di videosorveglianza del 8 aprile 2010
- Garante per la protezione dei dati personali, Consigli per rispettare la *privacy* se si usa un drone a fini ricreativi, da ultimo aggiornati in data 9 novembre 2018
- Pauner e J. Viguri, A legal approach to civilian use of drones in Europe. *Privacy* and personal data protection concerns
- Caruso, Dirittodellinformatica.it, Droni ad uso ricreativo: quali I limiti per rispettare la *privacy*
- Feder*privacy*, Droni e *Privacy*: cosa cambia con il nuovo GDPR?

Articolo a cura di **Orsolina Fortini**, Avvocato in Milano