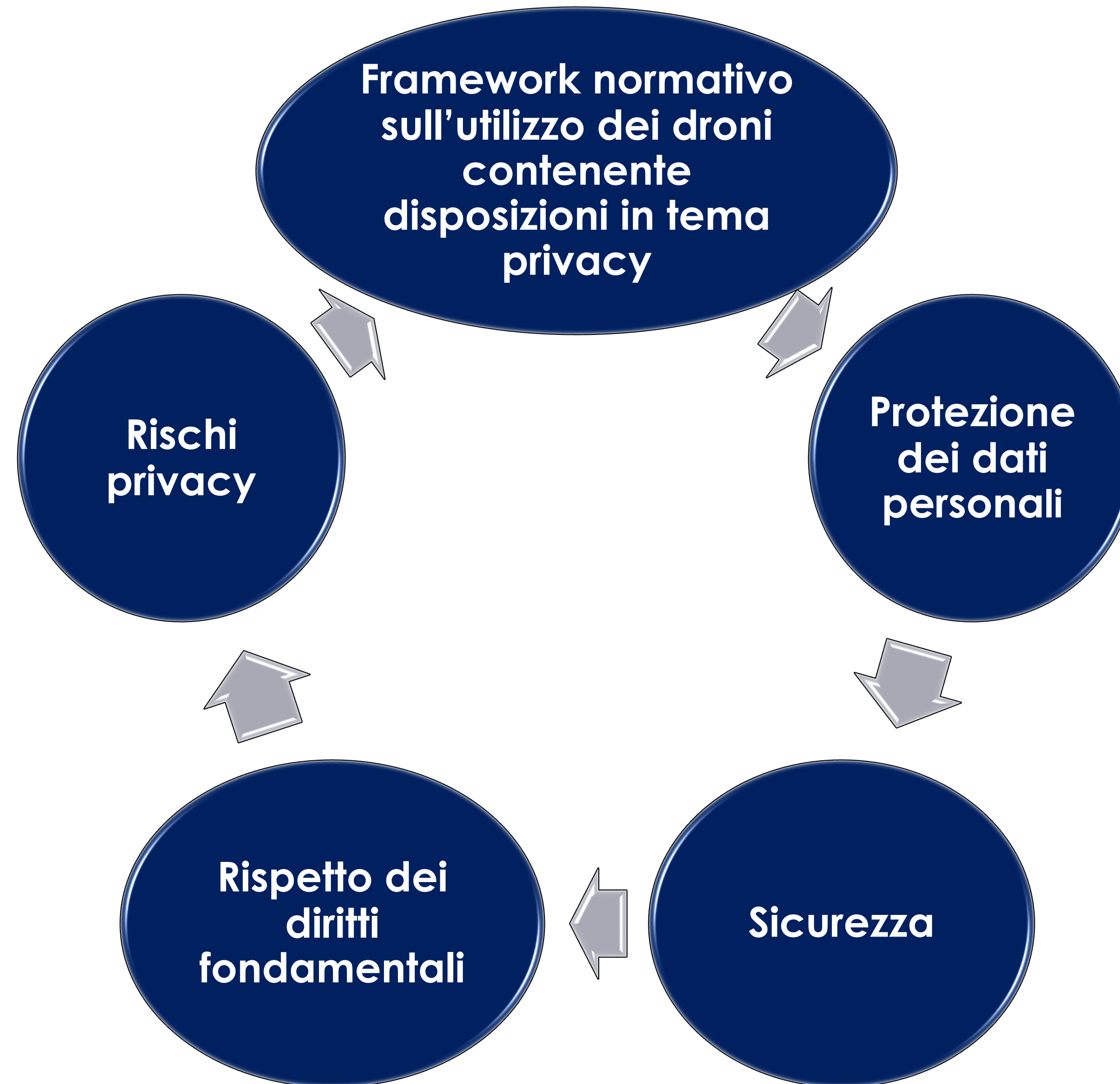


Droni: controversie sui diritti Le questioni rilevanti in tema privacy

14 giugno 2023- Fondazione dell'Avvocatura torinese Fulvio Croce

Avv. Giulia Escurole

Introduzione



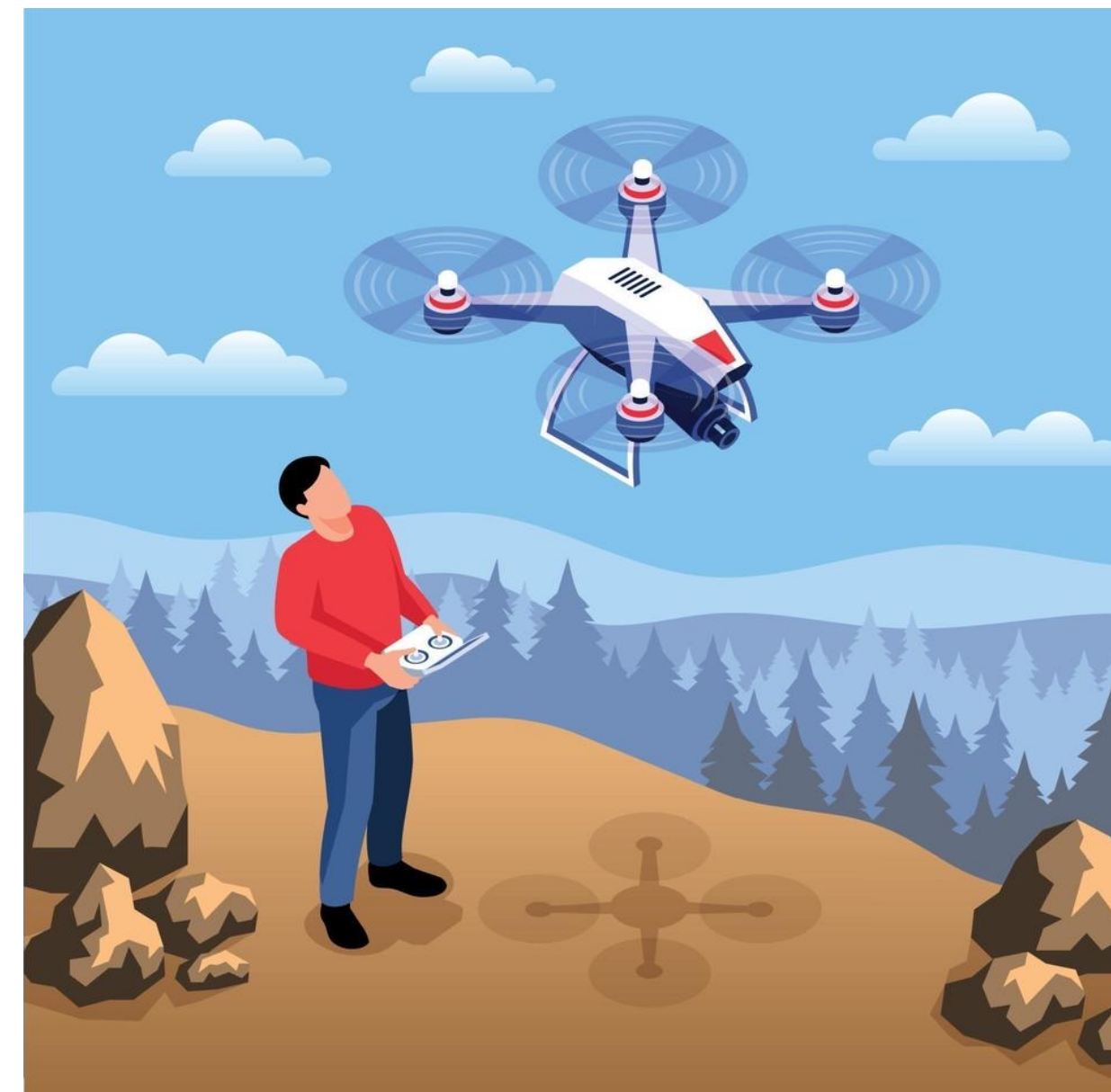
La protezione dei dati personali nella normativa europea sui droni



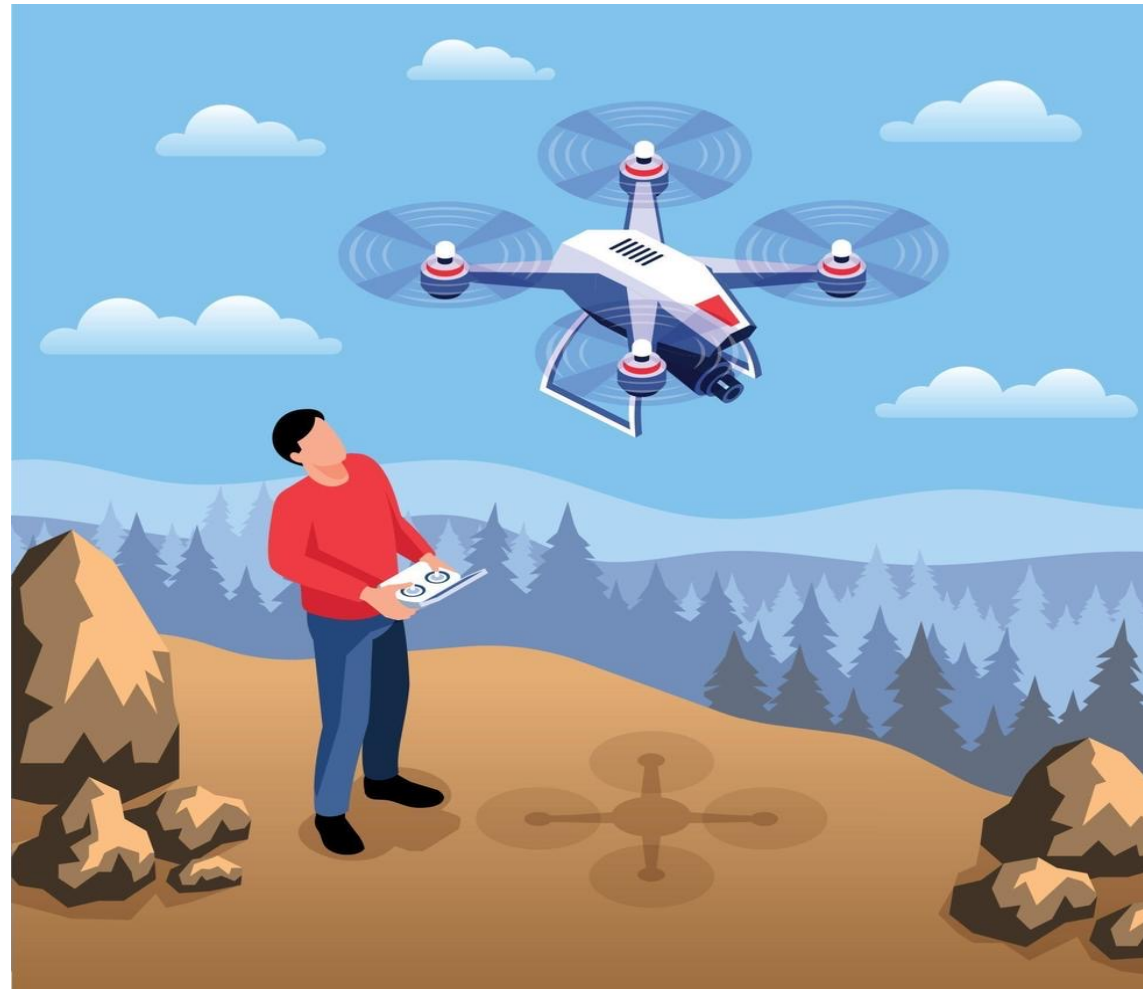
Il **Regolamento di esecuzione (UE) 2019/947** della Commissione, relativo a norme e procedure per l'esercizio di aeromobili senza equipaggio, recentemente modificato dal Regolamento di esecuzione (UE) 2020/746 della Commissione, fornisce alcuni spunti interessanti relativi al **rispetto della privacy**.

Il Regolamento di esecuzione (UE) 947/2019

Considerando 14: «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».



L'Operatore UAS



Per **operatore di sistema di aeromobili senza equipaggio** («operatore UAS, acronimo di Unmanned Aerial Sistema») si intende ogni persona fisica o giuridica che utilizzi o intenda utilizzare uno o più UAS (art. 2 Regolamento di esecuzione).

La figura dell'operatore può coincidere con quella del pilota (ad esempio un pilota remoto che opera il proprio UAS). In questo caso sul pilota remoto ricadono anche gli obblighi di legge dell'operatore.

L'operatore UAS ha la responsabilità di utilizzare o far utilizzare il drone a scopo ricreativo, professionale, ricerca, etc. nel rispetto delle leggi attuali in termini di sicurezza (manutenzione, buona conservazione, etc.), **privacy** e obblighi assicurativi.

Il Regolamento di esecuzione (UE) 947/2019

Considerando 16 «in considerazione dei rischi per la riservatezza e la protezione dei dati personali, gli operatori di aeromobili senza equipaggio dovrebbero essere immatricolati se utilizzano aeromobili senza equipaggio dotati di sensori in grado di raccogliere dati personali.

Tuttavia ciò **non dovrebbe avvenire** quando l'aeromobile senza equipaggio è **considerato un giocattolo** ai sensi della direttiva 2009/48/CE del Parlamento europeo e del Consiglio sulla sicurezza dei giocattoli».

Il Regolamento di esecuzione (UE) 947/2019

Considerando 20: «gli operatori e i piloti remoti UAS dovrebbero assicurarsi di essere adeguatamente informati in merito alle norme nazionali e dell'Unione applicabili alle operazioni previste, in particolare **in materia di sicurezza**, anche **intesa come security, tutela della riservatezza, protezione dei dati**, responsabilità civile, assicurazione e protezione dell'ambiente».



La protezione dei dati personali nella normativa italiana sui droni



L'Ente Nazionale per l'Aviazione Civile (ENAC) nel 2021 ha pubblicato il **REGOLAMENTO UAS-IT** che disciplina quanto di competenza degli Stati Membri.

Art. 29 Regolamento UAS-IT – Protezione dei dati e privacy

(1) «Laddove le operazioni svolte attraverso UAS **possano comportare un trattamento di dati personali**, tale circostanza deve essere menzionata nella documentazione sottoposta ai fini del rilascio della pertinente autorizzazione».

(2) «Il trattamento dei dati personali deve essere effettuato in ogni caso nel rispetto del **Regolamento (UE) 2016/679 e del Decreto Legislativo 30 giugno 2003, n. 196 e successive modificazioni** (“Codice in materia di protezione dei dati personali”), **con particolare riguardo al rispetto del principio di minimizzazione dei dati di cui all’articolo 5(1)(c) del predetto Regolamento**».

La normativa sui dati personali

Ad esclusione dei – rarissimi – casi in cui un drone sia sprovvisto di strumenti idonei a trattare i dati personali (es. videocamera o GPS), è necessario quindi garantirne un utilizzo del drone che rispetti:

- i. il Regolamento UE 2016/679 (c.d. **GDPR**);
- ii. il D.lgs. 30 giugno 2003, n. 196 come novellato dal D.lgs. 101/2018 (c.d. **Codice Privacy**);
- iii. la normativa sull'utilizzo dell'immagine altrui (es. Legge 633/1941).

Quali dati possono essere trattati attraverso un drone?

Ogni altra informazione
che consente di
identificare direttamente
o indirettamente
l'interessato

Immagine/
Foto

Dati biometrici
(es. sistemi di
riconoscimento
facciale)



Video

Dati personali
indiretti (dati relativi
alla posizione e agli
spostamenti, targhe
di macchine)

Suoni

Gli utilizzi dei droni: le finalità recreative (APR “aeromobile a pilotaggio remoto”)

In relazione ai droni utilizzati per finalità ricreative trova applicazione il GDPR?

L'**art 2 GDPR** (Ambito di applicazione materiale) prevede che il regolamento non si applichi ai trattamenti di dati personali effettuati da una persona fisica per l'esercizio di **attività a carattere esclusivamente personale o domestico**.

Il **Considerando 18 GDPR**, tuttavia, chiarisce che pur non applicandosi al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico, il GDPR si applica tuttavia ai titolari del trattamento o ai responsabili del trattamento **che forniscono i mezzi** per trattare dati personali nell'ambito di tali attività a carattere personale o domestico.

Gli utilizzi dei droni: le finalità ricreative

Per cui, anche se il pilota remoto del drone utilizzato per finalità ludiche non è da considerare un Titolare del trattamento, può essere individuato, per esempio, un Titolare del trattamento nel soggetto che mette a disposizione la banca dati per la conservazione delle immagini raccolte dal drone.

Per questo motivo, il **Garante per la protezione dei dati personali** ha evidenziato che tutti i droni idonei a trattare dati personali, come tutti i dispositivi elettronici, devono rispettare i principi di privacy by design e privacy by default.

La scheda informativa del Garante per la protezione dei dati personali

Consigli per rispettare la privacy se si usa un DRONE a fini ricreativi

1. SEGUI SEMPRE LE REGOLE

Usare i droni per scopi ricreativi è lecito e divertente, ma occorre sempre **rispettare la privacy degli altri** e informarsi bene sulle **regole previste dall'ENAC** per far volare i Sistemi Aeromobili a Pilotaggio Remoto (www.enac.gov.it).

2. FAI ATTENZIONE ALLE RIPRESE

Se si fa volare a fini ricreativi un drone munito di fotocamera in un **luogo pubblico** (parchi, strade, spiagge) è meglio **evitare di invadere gli spazi personali e l'intimità delle persone**. La diffusione di riprese realizzate con il drone (sul web, sui social media, in chat) può avvenire **solo con il consenso** dei soggetti ripresi, fatti salvi particolari usi connessi alla libera manifestazione del pensiero, come quelli a fini giornalistici. Negli altri casi, quando è eccessivamente difficile raccogliere il consenso degli interessati, è possibile diffondere le immagini **SOLO se i soggetti ripresi non sono riconoscibili**, o perché **ripresi da lontano**, o perché si sono utilizzati appositi software per oscurare i loro volti. Occorre poi **evitare** di riprendere e diffondere immagini che contengono **dati personali come targhe di macchine, indirizzi di casa, ecc.** Le riprese che violano gli **spazi privati altrui** (casa, giardino domestico) sono invece **SEMPRE da evitare**, anche perché si potrebbero violare norme penali.



3. RISPETTA GLI 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. E' quindi buona regola usare questi strumenti **senza invadere la sfera personale degli altri**, magari anche comunicando preventivamente le proprie intenzioni. Ad esempio, se si vuole far volare un drone per riprendere una festa nel proprio giardino di casa, sarebbe bene prima avvisare i vicini, che hanno il diritto di chiedere di **non essere - anche solo inavvertitamente - ripresi** nel loro privato. 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.

4. 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, per pubblicare un video online) **SOLO se NON** rendono riconoscibile il contesto, cioè il contenuto dei discorsi e le persone coinvolte.

5. A PROVA DI PRIVACY

In base a quanto previsto dal nuovo Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679), i droni, come tutti i dispositivi elettronici, devono rispettare i principi di **privacy by design** e **privacy by default**. Cioè devono essere costruiti e configurati per raccogliere meno dati possibile.

6. COME TUTELARE LA TUA PRIVACY

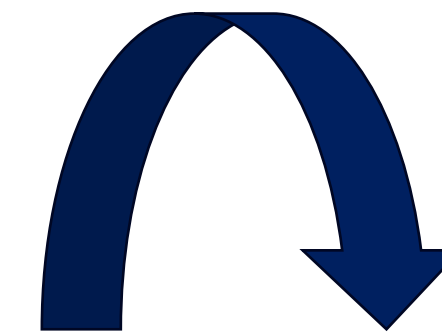
Se è possibile individuare il pilota del drone, si possono chiedere a lui informazioni su come intende utilizzare le riprese ed eventualmente **negare il consenso** al trattamento dei dati raccolti, specie se sono previste forme di diffusione delle immagini. **E nel caso si ritenesse di essere stati vittime di violazioni della propria privacy**, ci si può rivolgere al Garante per la protezione dei dati personali o, in alternativa, all'Autorità giudiziaria.

La scheda ha finalità meramente divulgative e sarà aggiornata in base agli sviluppi tecnologici e normativi

Attenzione alle riprese!!!



Se si fa volare **a fini ricreativi** un drone munito di fotocamera in un luogo pubblico (parchi, strade, spiagge) **è meglio evitare di invadere gli spazi personali e l'intimità delle persone.**



La **diffusione** di riprese realizzate con il drone (sul web, sui social media, in chat) **può avvenire solo con il consenso** dei soggetti ripresi, fatti salvi particolari usi connessi alla libera manifestazione del pensiero, come quelli a fini giornalistici.

Diffusione delle immagini senza consenso

Negli altri casi, quando è **eccessivamente difficile raccogliere il consenso degli interessati**, è possibile **diffondere le immagini** esclusivamente **se i soggetti ripresi non sono riconoscibili**, o perché ripresi da lontano, o perché si sono utilizzati appositi software per oscurare i loro volti.



Rispetto per gli altri

Occorre evitare di riprendere e diffondere immagini che contengono dati personali come targhe di macchine, indirizzi di casa, ecc.

Le riprese che violano gli spazi privati altrui (casa, giardino domestico) sono invece **sempre da evitare**, anche perché si potrebbero violare norme penali.

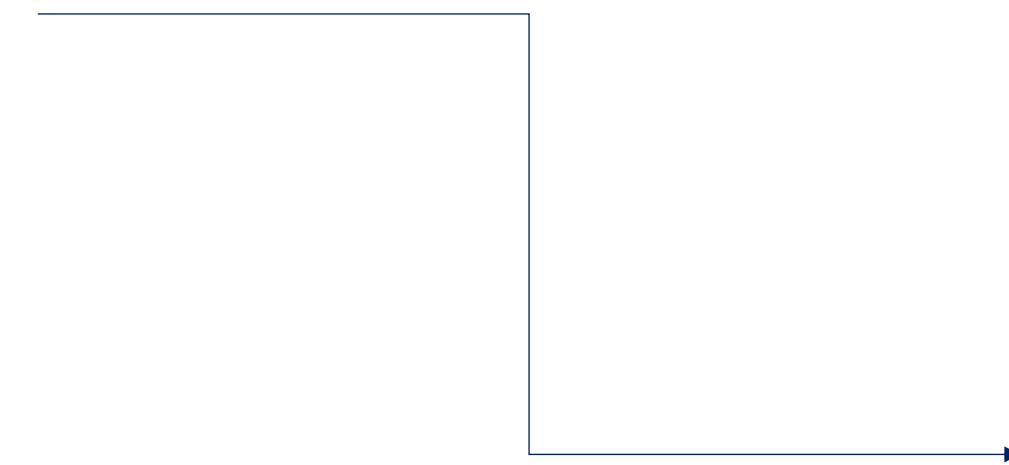


Non si possono usare droni per captare volontariamente conversazioni altrui: eventuali frammenti di conversazione registrati in modo accidentale possono essere utilizzati esclusivamente se non rendono riconoscibile il contesto, cioè il contenuto dei discorsi e le persone coinvolte.

Consigli pratici del Garante

Anche se utilizzato a fini ricreativi, la presenza di un drone che effettua riprese nelle vicinanze può dare ai soggetto ripresi la sensazione di essere osservati, inducendo disagio e influenzando il normale comportamento delle persone.

È quindi **buona regola** – evidenzia il Garante - usare questi strumenti senza invadere la sfera personale degli altri, **magari anche comunicando preventivamente le proprie intenzioni**.



Esempio: festa in giardino

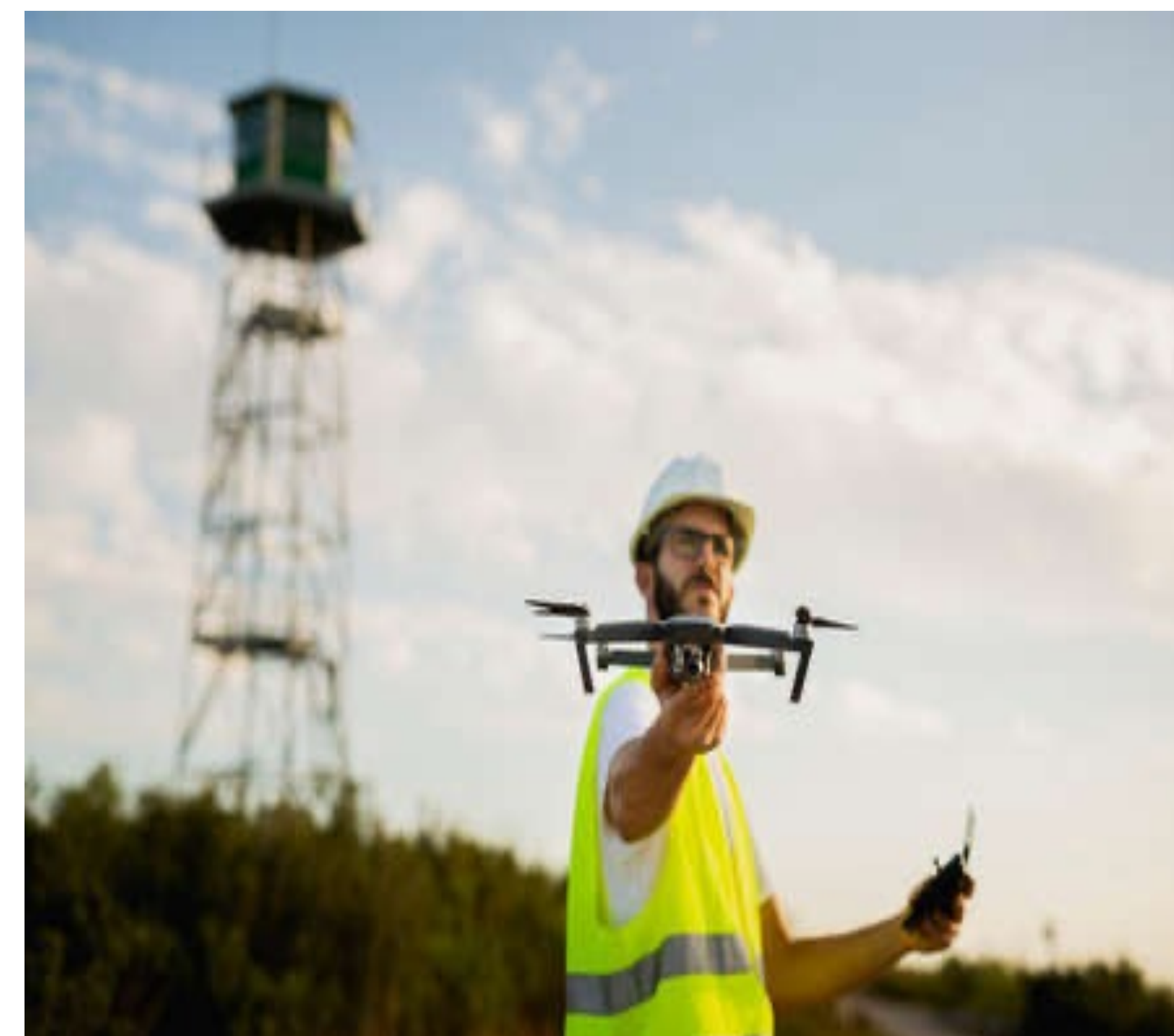
Ad esempio, se si vuole far volare un drone per riprendere una festa nel proprio giardino di casa, sarebbe bene prima avvisare i vicini, che hanno il diritto di chiedere di non essere - anche solo inavvertitamente - ripresi nel loro privato.



Chiedere informazioni al pilota

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.

In questo caso, si mettono i soggetti ripresi nella condizione di **chiedere a lui direttamente le informazioni** su come intenda utilizzare le riprese ed eventualmente **negare espressamente il consenso alla diffusione delle immagini**.



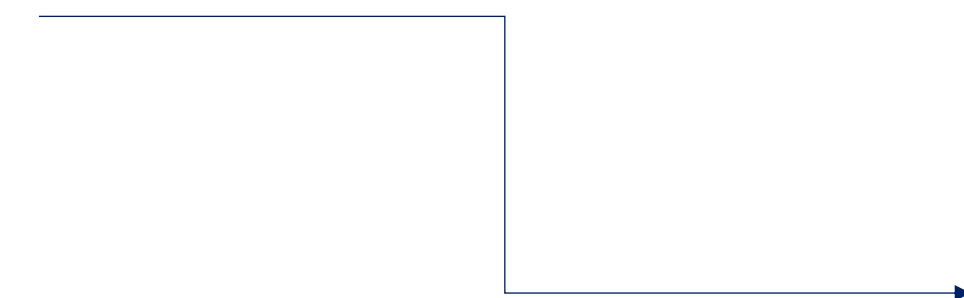
Gli utilizzi del drone: le finalità professionali

In ottica privacy, risulta decisamente diversa la situazione relativa ai droni utilizzati con finalità diverse da quelle ricreative (mediante SAPR - Sistema Aeromobile a Pilotaggio Remoto).

In questo caso trova piena applicazione il Regolamento UE 2016/679 (GDPR)!!



Come chiarito dall'Autorità Garante per la Protezione dei Dati spagnola (AEPD – Agencia Española de Protección de Datos) nel proprio ***vademecum*** sul trattamento dei dati personali mediante l'utilizzo di droni, ci si può trovare di fronti a **tre tipi di attività:**



- i) **Attività che non include – neanche potenzialmente – il trattamento di dati personali (es. ispezione infrastrutture, rilievi topografici):** in questo caso, prima di condividere i dati raccolti con il drone è bene assicurarsi che non contengano immagini o dati relativi a persone, veicoli, case o altri oggetti che possono portare all'identificazione dei soggetti, e in tal caso, renderli anonimi.
- ii) **Attività che di regola non include il trattamento di dati personali, ma che involontariamente potrebbe comportare un trattamento di dati personali.**
- iii) **Attività espressamente finalizzate a trattare dati personali (es. videosorveglianza).**

Gli adempimenti privacy indispensabili

Comune a tutte e tre le ipotesi è la necessità di rispettare i principi di **privacy by design** e **privacy by default**: i droni devono essere in ogni caso costruiti e configurati per raccogliere meno dati possibile.



Data Protection by Design &
Data Protection by Default

Nel caso in cui l'attività comporti effettivamente il trattamento di dati personali, occorre inoltre mettere in campo **una serie di ADEMPIMENTI previsti dal Regolamento**:

1. occorre definire i **ruoli privacy** dei soggetti coinvolti: del pilota, del proprietario e di tutti gli altri soggetti che processano, archiviano, trattano i dati raccolti e **che possono agire, a seconda dei casi, in qualità di Titolari autonomi del trattamento, di Responsabili del trattamento ovvero di Contitolari del trattamento**;

2. è fondamentale ponderare attentamente la **scelta dei fornitori** coinvolti nelle attività. Ad esempio il fornitore del software per la gestione del drone e/o per la conservazione delle immagini. E' sempre preferibile optare per un fornitore che abbia sede in UE;

3. prima di iniziare il trattamento, è necessario verificare il rispetto del **principio di liceità (art. 5, par. 1 lett. a) GDPR)**, in particolare, occorre **verificare che la normativa nazionale consenta l'uso dei droni:** in caso contrario il trattamento dei dati effettuato si considererebbe non conforme al principio di liceità del trattamento.

4. occorre garantire il costante rispetto **del principio di minimizzazione (art. 5, par. 1, lett. c) GDPR:** indurre al minimo la cattura delle immagini a quelle assolutamente necessarie; ridurre le possibilità che le persone appaiano inavvertitamente nelle immagini; regolare la risoluzione dell'immagine al minimo necessario; ridurre le funzionalità di geolocalizzazione.

5. occorre **impedire la memorizzazione di informazioni inutili relative alle persone.**

Ad esempio, se lo scopo delle immagini è un rilevamento topografico di una zona costiera, non avrebbe senso memorizzare riprese che consentano di identificare i bagnanti che si trovano in quella zona;

6. il Titolare del trattamento deve **informare** i soggetti interessati, fornendo loro tutte le informazioni previste dall' art. 13 GDPR (ed eventualmente nelle forme previste per il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali).



7. Il Titolare deve inoltre effettuare un'**analisi dei rischi** sulla base della quale determinare ed applicare, ai sensi dell'art 32 GDPR le misure di sicurezza di **natura tecnica** (es. l'anonimizzazione delle immagini o i protocolli di comunicazione sicuri che impediscano l'accesso di terzi ai trasferimenti dei dati catturati) e le misure di sicurezza di **natura organizzativa** nelle attività di gestione, conservazione ed archiviazione delle immagini.



8. il Titolare è tenuto ad effettuare una **Valutazione di impatto sulla protezione dei dati (Art. 35 GDPR)**, qualora il trattamento:

- i) rientri nelle circostanze stabilite nel GDPR (art. 35 GDPR) oppure
- ii) nell'elenco delle tipologie di trattamenti da sottoporre a DPIA presenti nell'Allegato 1 al Provvedimento del Garante per la Protezione dei Dati Personali n. 467 dell'11 ottobre 2018.

In quali casi non si applica il GDPR?

Dalle FAQ del Garante privacy **sulla videosorveglianza**, emerge un dato importante: **la normativa in materia di protezione dati non si applica** al trattamento di dati che **non consentono di identificare le persone**, direttamente o indirettamente, **come nel caso delle riprese ad alta quota, effettuate mediante l'uso di droni.**



Gli interventi del Garante italiano – Il Comune di Bari

Nel **2021** il Garante ha invitato una richiesta di informazioni al Comune di Bari, che in aggiunta alla flotta di droni già utilizzata dalla Polizia locale, avrebbe voluto utilizzarne altri per monitorare «eventuali assembramenti incompatibili con le limitazioni dovute alla gestione della pandemia da Covid».

Il Garante ha chiesto al Comune di fornire (entro 20 giorni dalla notifica di avvio dell'istruttoria) tutte le informazioni necessarie per valutare le circostanze del trattamento (caratteristiche tecniche dei droni, finalità perseguite, tempi di conservazione delle immagini, comunicazioni a soggetti terzi), nonché una copia dell'eventuale valutazione d'impatto sulla protezione dei dati.

Gli interventi del Garante italiano – Roma Capitale

Nello stesso anno un'analoga richiesta di informazioni è stata inviata al Comune di Roma Capitale che, secondo notizie di stampa, si sarebbe dotata presto di 9 piccoli droni per il monitoraggio ed il controllo del territorio cittadino (illeciti ambientali, rifiuti abusivi, roghi tossici, abusi edilizi, esigenze di traffico).

Con l'avvio dell'istruttoria il Garante intendeva verificare l'impatto dell'iniziativa sulla privacy delle persone interessate e il puntuale rispetto della normativa in materia di trattamento dei dati.

Anche in questo caso è stato richiesto all'Ente di fornire entro 20 giorni dalla notifica dell'avvio dell'istruttoria tutte le informazioni necessarie ed una copia della valutazione d'impatto (o i motivi per i quali non è stata effettuata).

Gli interventi del Garante italiano – Azienda USL Roma 3

Sempre nel 2021, il Garante ha inviato una richiesta di informazioni alla Azienda UsI Roma 3 per verificare il corretto trattamento dei dati personali, anche di tipo sanitario, nell'ambito di una iniziativa in programma sulle **spiagge di Ostia**. L'azienda sanitaria, mediante un drone, avrebbe infatti **volut**
rilevare la temperatura corporea a tutte le persone presenti in spiaggia.

Considerata la delicatezza dei trattamenti di dati personali oggetto di trattamento e in assenza di una chiara base giuridica che legittimasse il trattamento, il Garante ha chiesto all'azienda di fornire una serie di chiarimenti – questa volta - **entro 7 giorni**.

In particolare, il Garante ha richiesto all'azienda di specificare, oltre al resto, **i dati del titolare del trattamento** dei dati delle persone sottoposte alla rilevazione della temperatura corporea, **i motivi** della rilevazione, **l'affidabilità degli strumenti** utilizzati, **le conseguenze** previste per chi risultasse avere una temperatura superiore a quella fisiologica, i contenuti e **le modalità di distribuzione dell'informativa**.

Gli interventi del Garante Francese

La Commission Nationale de l'Informatique et des Libertés (CNIL) – Garante privacy francese – ha infatti sanzionato il Ministero dell'Interno Francese reputando illecito il trattamento dei dati personali effettuato mediante l'utilizzo dei droni per il controllo del rispetto delle misure di contenimento nell'ambito del Covid-19.

Il CNIL ha rilevato un utilizzo dei droni **eccedente** rispetto alle finalità dichiarate, poiché venivano effettivamente utilizzati anche per il controllo delle manifestazioni e per missioni di polizia giudiziaria.

Tra le violazioni riscontrate dal CNIL, è stata inoltre accertata la **mancaza di una DPIA** ai sensi dell'articolo 35 del GDPR e la **mancaza di informativa** resa ai sensi del GDPR.

Conclusioni

Utilizzo dei droni consentito MA:

- rispetto della normative sulla protezione dei dati applicabile, in particolare privacy by design e by default;
- individuazione della finalità di utilizzo del drone (ricreativa o professionale);
- necessità di un motivo legittimo;
- scelta di una tecnologia sicura, adeguata e proporzionata;
- implementazione di misure tecniche ed organizzative adeguate a garantire la protezione dei dati personali e la tutela dei diritti fondamentali = “adempimenti privacy minimi”
- necessità di un monitoraggio continuo da parte delle Autorità competenti, comprese soprattutto le autorità di controllo responsabili della protezione dei dati personali.

Grazie per l'attenzione!!!

giulia.escurole@ipglex.it