La CyberSecurity per i droni

A cura di: Domenico Raguseo, Rosita Galiandro, Giuseppe Marullo e Antonio De Chirico - Pubblicato il 19 Gennaio 2022

Introduzione

La progressiva integrazione dei droni nello spazio aereo civile europeo e l'emergere di numerose applicazioni di questi strumenti (dalle attività ricreative ai servizi, fino ai campi della fotografia, della logistica e della sorveglianza delle infrastrutture) hanno portato alla reale necessità, da un lato, di concentrarsi sulle sfide che il loro utilizzo su larga scala potrebbe comportare per la tutela della privacy, delle libertà civili e politiche di ciascuno e, dall'altro, valutare le misure necessarie per garantire il rispetto dei diritti fondamentali e la protezione dei dati.

Diversi sono, infatti, i rischi per la tutela della privacy che possono derivare dal trattamento di dati (come immagini, suoni e dati di geolocalizzazione relativi a una persona fisica identificata o identificabile) effettuato con i dispositivi a bordo di un drone. Tali rischi possono andare dalla mancanza di trasparenza sui tipi di trattamento, a causa alla difficoltà di vedere i droni da terra, sino alla difficoltà, in ogni caso, di sapere quali siano le apparecchiature a bordo destinate al trattamento di dati, quali siano i fini per cui vengono raccolti i dati personali e da chi. Inoltre, le potenzialità dei droni e la possibilità di interconnetterne più di uno facilita ancor di più la loro capacità di ottenere punti di osservazione unici. Ad esempio, grazie alla possibilità di evitare ostacoli o superare barriere o recinzioni, facilitando la raccolta di un'ampia varietà di informazioni con un alto rischio di raccolta dati in blocco e possibili usi illeciti per molteplici scopi.

Rischi ancora maggiori per i diritti e le libertà delle persone sorgono laddove il trattamento di dati personali mediante droni sia effettuato ai fini di contrasto della criminalità.

Prima di utilizzare un drone è necessario rispettare una serie di obblighi e nello specifico:

- verificare, ove consentito l'utilizzo di droni, se sia necessaria una specifica autorizzazione da parte delle autorità dell'aviazione civile (AAC);
- individuare i criteri più idonei di liceità del trattamento;
- rispettare i principi di limitazione delle finalità, minimizzazione dei dati e proporzionalità (selezionando le tecnologie e le misure più appropriate per evitare la raccolta di dati personali non necessari);

Cerca qui

ULTIMI ARTICOLI

La CyberSecurity per i droni
19 Gennaio 2022

Il trattamento dei dati personali nella lotta all'evasione fiscale: possibilità e tutele

La CyberSecurity per i droni

La CyberSecurity per i droni - ICT Security Magazine18 Gennaio 2022

La CyberSecurity per i droni

Introduzione

La progressiva integrazione dei droni nello spazio aereo civile europeo e l'emergere di numerose applicazioni di questi strumenti (dalle attività ricreative ai servizi, fino ai campi della fotografia, della logistica e della sorveglianza delle infrastrutture) hanno portato alla reale necessità, da un lato, di concentrarsi sulle sfide che il loro utilizzo su larga scala potrebbe comportare per la tutela della privacy, delle libertà civili e politiche di ciascuno e, dall'altro, valutare le misure necessarie per garantire il rispetto dei diritti fondamentali e la protezione dei dati.

Diversi sono, infatti, i rischi per la tutela della privacy che possono derivare dal trattamento di dati (come immagini, suoni e dati di geolocalizzazione relativi a una persona fisica identificata o identificabile) effettuato con i dispositivi a bordo di un drone. Tali rischi possono andare dalla mancanza di trasparenza sui tipi di trattamento, a causa alla difficoltà di vedere i droni da terra, sino alla difficoltà, in ogni caso, di sapere quali siano le apparecchiature a bordo destinate al trattamento di dati, quali siano i fini per cui vengono raccolti i dati personali e da chi. Inoltre, le potenzialità dei droni e la possibilità di interconnetterne più di uno facilita ancor di più la loro capacità di ottenere punti di osservazione unici. Ad esempio, grazie alla possibilità di evitare ostacoli o superare barriere o recinzioni, facilitando la raccolta di un'ampia varietà di informazioni con un alto rischio di raccolta dati in blocco e possibili usi illeciti per molteplici scopi.

Rischi ancora maggiori per i diritti e le libertà delle persone sorgono laddove il trattamento di dati personali mediante droni sia effettuato ai fini di contrasto della criminalità.

Prima di utilizzare un drone è necessario rispettare una serie di obblighi e nello specifico:

verificare, ove consentito l'utilizzo di droni, se sia necessaria una specifica autorizzazione da parte delle autorità dell'aviazione civile (AAC);

individuare i criteri più idonei di liceità del trattamento;

rispettare i principi di limitazione delle finalità, minimizzazione dei dati e proporzionalità (selezionando le tecnologie e le misure più appropriate per evitare la raccolta di dati personali non necessari);

soddisfare, nel modo più idoneo alla fattispecie in esame, il principio di trasparenza (informando gli interessati del trattamento effettuato);

adottare tutte le opportune misure di sicurezza;

garantire l'eliminazione o l'anonimizzazione dei dati personali non strettamente necessari.

È inoltre necessario considerare la possibilità di interconnettere più droni al fine di sorvegliare una vasta area. Sciami di droni con canali di comunicazione in tempo reale che li collegano tra loro e con terze parti comportano rischi ancora maggiori per la protezione dei dati; in quanto potrebbero facilmente consentire una sorveglianza coordinata, ovvero il controllo del movimento

di persone o veicoli su vaste aree.
Vi è quindi un alto rischio che il trattamento dei dati personali da parte dei droni diventi segreto e causi significative interferenze nella sfera più privata delle persone. Allo stesso tempo, date le attrezzature messe a bordo potenzialmente sofisticate e la facilità con cui i dati personali raccolti possono essere collegati ad altre informazioni, vi è un maggior rischio di "function creep"; ovvero il rischio di modifica o estensione dell'uso per scopi incompatibili.
Inoltre, il potenziale impatto dell'intrusione nella privacy è aggravato dall'ampia varietà di individui ed entità coinvolti nell'uso dei droni. Anche i produttori di droni, ad esempio, hanno un ruolo da svolgere nella fase di progettazione di tali dispositivi, considerando che le caratteristiche operative possono, in misura minore o maggiore, prestarsi ad applicazioni invadenti per la privacy (ad esempio, nel caso di piccoli o droni di medie dimensioni in grado di volare all'interno di edifici).
Regole di base e regolamenti sui droni
Regolamento europeo
EASA (European Union Aviation Safety Agency)
Il regolamento di base è stato attuato attraverso due regolamenti, di seguito.
Regolamento (UE) 2019/947 e Regolamento (UE) 2019/945
Il Regolamento 2019/947 fornisce regole e procedure incentrate sulle operazioni e basate sul rischio per le operazioni con i droni. Definisce tre categorie di operazioni UAS: Aperte, Specifiche e Certificate sviluppate parallelamente alle categorie JARUS A, B e C.
Categoria aperta (Open Category) – Droni civili
Nella categoria aperta, non esiste un'approvazione operativa ma piuttosto una serie di limitazioni come la Visual Line Of Sight (VLOS), l'altezza massima di 120 metri e la massa massima al decollo inferiore a 25 kg. Il regolamento include "operations over people" (OOP). La categoria aperta è suddivisa in 3 sottocategorie rilevanti per l'OOP indicate di seguito:
A1 – consente il sorvolo di persone isolate, con droni con una massa sotto i 250gr nelle classi C0 e 900gr in C1. È richiesta la formazione online. (Sorvolare persone ma non assembramenti di persone);
A2 – consente di volare vicino alle persone, per droni con una massa massima di 4kg in classe C2. È richiesta una formazione online più una formazione pratica auto-dichiarata (Volare vicino le persone);
A3- consente voli solo lontano dalle persone e dagli aeroporti, per droni con una massa massima di 25kg, classe C3 e C4. È richiesta anche la formazione online. (Volare lontano dalle persone).
Categoria specifica (Specific Category) – Droni civili
La categoria specifica copre tutte le operazioni che non rientrano nelle categorie aperte e certificate. Richiede un'autorizzazione operativa basata sul rischio rilasciata dall'autorità dello Stato membro competente. Gli esempi includono oltre la "Visual Line Of Sight" anche alcune operazioni di delivery dei droni.
Il metodo di compliance accettato utilizzato dagli Stati membri è lo Specific Operation Risk Assesmsment (SORA) sviluppato dalle autorità congiunte per la regolamentazione dei sistemi senza pilota (JARUS). Affronta il rischio terrestre e aereo e combina i due per creare un livello di garanzia e integrità specifico (SAIL) tra I e VI. Un livello di rischio di VII o superiore sposta l'operazione nella categoria certificata superiore. Il SORA definisce anche

adeguate misure di mitigazione

Morier, che è stato Presidente della JARUS dal 2017 al 2019, elabora: “Per evitare l’applicazione sistematica di SORA, sono stati definiti scenari standard (operazioni a basso rischio), che consentono di fornire una Dichiarazione di conformità anziché un’autorizzazione formale. Sono state inoltre definite Pre-Determined Risk Assessments (PDRA). Se un’operazione soddisfa questi requisiti, è ancora necessaria un’autorizzazione, ma dovrebbe essere ottenuta più facilmente. Le autorizzazioni nella categoria specifica sono valide in tutti i Paesi dell’UE, ma potrebbe essere necessario verificare le misure di mitigazione legate alla geografia e al tempo”.

BVLOS (Beyond Visual line of Sight) è consentito in categorie specifiche e certificate, a seconda del risk assessment.

Categoria certificata (Certified Category) – Droni civili

Nella categoria certificata, i droni sono certificati, gli operatori ricevono un certificato e il pilota ha una licenza. Questo è molto simile ai voli dell’aviazione con equipaggio. Le operazioni certificate sono state classificate in 3 tipologie:

Operazioni di tipo 1– Instrument flight rules (IFR) operazioni per droni che trasportano merci nelle classi di spazio aereo A–C (ICAO airspace classification) e decollano e/o atterrano negli aeroporti che rientrano nel regolamento di base.

Operazioni di tipo 2 – droni che decollano e/o atterrano in ambienti congestionati utilizzando rotte predefinite nello spazio aereo U-space. Questi includono le operazioni di aeromobili VTOL (Vertical Take-Off and Landing) senza equipaggio che trasportano passeggeri (ad esempio aerotaxi) o merci (ad esempio servizi di consegna di merci).

Operazioni di tipo 3 – come per le operazioni di tipo 2 con velivoli VTOL con pilota a bordo, comprese le operazioni fuori dallo spazio aereo U-Space

Il Regolamento 2019/ 945 stabilisce i requisiti per la progettazione e la fabbricazione di sistemi aeronautici senza equipaggio (UAS) destinati a essere utilizzati secondo le regole e le condizioni definite nel regolamento di esecuzione (UE) 2019/947 e di componenti aggiuntivi per l’identificazione a distanza. Definisce inoltre il tipo di UAS la cui progettazione, produzione e manutenzione sarà oggetto di certificazione. Stabilisce norme sulla messa a disposizione sul mercato di UAS, kit di accessori e componenti aggiuntivi per l’identificazione a distanza e sulla loro libera circolazione nell’Unione.

Il presente regolamento, infine, fissa anche le norme per gli operatori UAS di paesi terzi, quando effettuano un’operazione UAS ai sensi del regolamento di esecuzione (UE) 2019/947 all’interno del single European sky airspace.

Figure 1 – Categoria Open, Specific e Certified

L’immagine mostra chiaramente come vengono identificate le operazioni. Con questo nuovo regolamento, il fatto che si stia pilotando un UAS (Unmanned Aircraft System) per motivi di lavoro o hobby non è più rilevante, conta solo se ciò che stai facendo può essere in qualche modo pericoloso.

JARUS

Le Joint Authority for Rulemaking on Unmanned Systems (JARUS) sono un gruppo di esperti di 60 autorità aeronautiche nazionali mondiali (NAA) e 2 organizzazioni regionali per la sicurezza aerea (EASA ed EUROCONTROL), il cui obiettivo è sviluppare regole armonizzate per gli UAS. Il concetto di regolazione incentrata sulle operazioni con le tre categorie (aperta, specifica e certificata) è stato sviluppato all’interno delle categorie

JARUS.

La missione di JARUS è sviluppare requisiti tecnici e operativi per il funzionamento sicuro, protetto ed efficiente degli UAS, per fungere da riferimento comune per l'uso nei rispettivi regolamenti e linee guida dei membri JARUS, facendolo in modo efficace ed efficiente, evita la duplicazione di sforzi con altre organizzazioni aeronautiche internazionali.

JARUS è responsabile dello sviluppo della metodologia per Specific Operations Risk Assessment (SORA). È stato approvato dall'Agenzia europea per la sicurezza aerea (EASA) come mezzo di conformità accettabile (AMC) per soddisfare i requisiti dei regolamenti europei UAS (Basic Regulation, Implementing Act, Delegated Act e Annexes).

EUROCONTROL

Nell'ambito delle proprie attività volte all'integrazione sicura degli UAS, EUROCONTROL ha condotto diversi webinar basati su alcuni temi caldi nel dominio UAS, con la partecipazione delle parti interessate più rilevanti nelle diverse sessioni. L'obiettivo di questi webinar era quello di sviluppare linee guida che non fossero direttamente correlate a un particolare regolamento.

EUROCAE (European Organisation for Civil Aviation Equipment)

EUROCAE è il leader europeo nello sviluppo di standard industriali riconosciuti a livello mondiale per l'aviazione. EUROCAE sviluppa standard per l'industria che:

si basano sull'esperienza all'avanguardia dei suoi membri affrontando le slide globali dell'aviazione;

sono idonei allo scopo per essere adottati a livello internazionale;

supportano i processi operative, di sviluppo e normativi.

Regolamento italiano

Regolamento UAS-IT: integrazione di ENAC al regolamento droni EASA

Il 1° gennaio 2021 è entrato in vigore il Regolamento UAS-IT, che disciplina gli aspetti di competenza dell'Autorità nazionale per le operazioni con droni che non rientrano nelle disposizioni del Regolamento di esecuzione (UE) 2019/497.

Requisiti del pilota

In termini pratici il regolamento UAS-IT, ad una prima lettura, non fa altro che ribadire ciò che è già contenuto nel regolamento europeo in quanto non aggiunge nessun requisito aggiuntivo per il pilota di droni che opera nelle Open Category, per i droni privi di marcatura CE.

Rimangono validi i requisiti relativi ad altezza, distanza da infrastrutture e persone non informate.

Assicurazione

Secondo l'art. 27 dell'UAS-IT non è consentito condurre operazioni con un UAS se un'assicurazione relativa alla responsabilità verso terzi, adeguata allo scopo e con massimali non inferiori ai parametri minimi di cui alla tabella dell'art. 7 del Regolamento (CE) 785/2004.

Registrazione

Secondo quanto previsto dal regolamento di cui all'art. 6, gli operatori UAV sono tenuti a registrarsi sul portale D-Flight, anche ai fini dell'identificazione e imputazione di responsabilità civile e penale, e ad apporre il codice identificativo QR sull'UAV.

Sicurezza

La sicurezza riguarda il contrasto di tutte le azioni dolose intraprese per compiere un attacco deliberato attraverso l'utilizzo di un UAV: un'area in cui ricade il terrorismo, ad esempio. Ma anche spionaggio, aggressione, utilizzo dell'UAV per testare le difese di una struttura per poi compiere atti illeciti come intrusioni, furti, danneggiamenti. È chiaro che

le leggi possono fare poco contro le operazioni illecite e criminali, ma il Regolamento ENAC ha alcune disposizioni per complicare l'uso degli UAV per scopi illegali. Il principale è l'articolo 33, che tratta esplicitamente di Sicurezza.

Sicurezza del radio link

Contrastare le minacce alla sicurezza comporta anche obblighi e doveri nei confronti del Pilota e dell'Operatore. A partire dall'obbligo di protezione del radio link, cioè del collegamento tra il drone e la radio, previsto dall'art. 33 comma 1:

"L'operatore deve adottare misure adeguate per proteggere gli UAS per prevenire atti illeciti durante le operazioni anche al fine di prevenire l'interferenza volontaria del radio link".

Le minacce a cui fa riferimento questo paragrafo sono essenzialmente due: da una parte il cosiddetto "drone Hijack", il dirottamento del drone, ovvero la possibilità che un malintenzionato si impossessi del nostro UAS per compiere azioni illegali.

Dall'altra parte, invece, l'accesso abusivo ai dati trasmessi a terra dai SAPR: immaginiamo il caso di svolgere un'operazione specializzata per conto di un'azienda che ha segreti industriali da proteggere. Ovviamente avremo firmato stringenti accordi di riservatezza, ma un malintenzionato potrebbe essere in grado di ricevere il video link di ritorno del nostro UAV e quindi rubare informazioni riservate. Per ottemperare alle prescrizioni del comma, l'operatore e il pilota devono proteggere in ogni modo il radio link di controllo e ritorno, installando eventuali patch e aggiornamenti di sicurezza, utilizzando connessioni crittografate ove possibile e proteggendo la chiave per decrittografarle.

Proteggere l'area delle operazioni

Se il primo comma dell'articolo 33 riguarda la protezione del collegamento radio, ovvero dei collegamenti radio, dati e di controllo, tra l'UAV e la stazione di terra, il secondo comma riguarda le intrusioni meno sofisticate e tecnologiche ma non per questo meno pericolose:

"L'operatore deve stabilire procedure per impedire l'accesso di personale non autorizzato all'area operativa, alla stazione di controllo e per lo stivaggio del sistema."

Il significato è chiaro: non c'è bisogno di hackerare una connessione radio se si può facilmente ottenere la stessa cosa rubando l'hard disk dove abbiamo registrato i dati della missione. E se i malintenzionati possono entrare, possono anche rubare l'UAV e la radio e fare quello che vogliono. Il secondo comma ci invita essenzialmente, anzi ci obbliga, a monitorare e proteggere le nostre apparecchiature, poiché ci sono casi in cui una possibile intrusione non danneggia solo noi, ma potenzialmente l'intera comunità.

Conclusioni

Pur riconoscendo i benefici a livello sociale ed economico dell'uso civile dei droni e il loro potenziale in termini di crescita, è necessario porre l'attenzione sulle minacce e sui rischi per la protezione dei dati e la propria privacy derivanti da un impiego su larga scala della tecnologia dei droni e valutare le misure necessarie per garantire il rispetto di tutti i diritti fondamentali coinvolti.

Attualmente ricopre il ruolo di Responsabile Osservatorio CyberSecurity presso Exprivia. Contribuisce alle attività di prevendita, ha partecipato a progetti di risk assessment e GDPR compliance e collabora in piani di insegnamento con diverse università nell'ambito CyberSecurity e nel progetto CyberChallenge.IT. Fa parte della community

Women For Security.

Condividi sui Social Network:

Ti potrebbe interessare

12 Gennaio 2022

ISCRIVITI ALLA NEWSLETTER

Una volta al mese riceverai gratuitamente la rassegna dei migliori articoli di ICT Security Magazine

19 Gennaio 2022

Il trattamento dei dati personali nella lotta all'evasione fiscale: possibilità e tutele

12 Gennaio 2022

11 Gennaio 2022

15 Dicembre 2021

ICT Security

La rivista che da oltre 15 anni offre informazione, aggiornamento e riflessioni sui temi della sicurezza informatica.

Segreteria: Humana Srls C.F e P.IVA: 13642431004

redazione@ictsecuritymagazine.com

ISCRIVITI ALLA NEWSLETTER DI ICT SECURITY MAGAZINE

Una volta al mese riceverai gratuitamente la rassegna dei migliori articoli di ICT Security Magazine