

## ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3802 di mercoledì 15 giugno 2016

### Tema attualissimo: droni e protezione dei dati

*Purtroppo l'Italia è rimasta un poco indietro nella individuazione di regole che possano permettere di proteggere in modo adeguato i dati personali, che possono essere catturati durante l'utilizzo dei droni: il punto della situazione. Di A. Biasiotti.*

Mentre altri paesi europei hanno già pubblicato delle norme che permettono di proteggere i dati personali, che vengono acquisiti, anche accidentalmente, durante l'utilizzo dei droni per attività di pattugliamento e di vigilanza ispettiva, in Italia stiamo attendendo che venga emanata una normativa europea.

Una bozza di normativa è già disponibile ed è stata sottoposta all'esame dell'ormai famoso organo di consulenza articolo 29 working party, che ha avanzato alcune osservazioni.

Per quanto riguarda il regolamento vigente di ENAC, esso fa riferimento al fatto che l'operatore deve applicare le tutele previste dal decreto legislativo 196/2003, che ovviamente fa riferimenti assolutamente generici a questo problema, così specifico.

Vediamo quali suggerimenti possono essere offerti a tutti coloro che devono utilizzare dei droni per attività di pattugliamento e soprattutto agli istituti di vigilanza privata, che dovranno utilizzare i droni per la vigilanza ispettiva, come previsto dal bando di gara CONSIP per i servizi di vigilanza attiva e passiva.

In assenza di specifici riferimenti, è bene prendere buona nota di una sentenza della corte di cassazione, che non è specificamente applicabile all'attività dei droni, ma che introduce un principio che certamente va rispettato, in fase di effettuazione di riprese con droni.

Il ragionamento fatto dalla cassazione è relativamente lineare: la suprema corte ha detto che la volontà di un cittadino di proteggere la sua privacy può essere esplicitata dal fatto che egli ha adottato delle misure di protezione, che appunto garantiscano la sua privacy.

Se il cittadino prende il sole in giardino, circondato da una rete metallica fronte strada, evidentemente non può pretendere una elevata privacy. Se invece il cittadino ha messo, tutto attorno al suo giardino, una siepe fitta alta un paio di metri, chi utilizzando una scala effettuasse una ripresa all'interno indubbiamente violerebbe la misura di protezione adottata dlla cittadino.

Letteralmente la cassazione afferma che una ripresa è illecita se la ripresa fotografica o video, anche audio, è stata fatta utilizzando accorgimenti che superano le barriere che altrimenti impedirebbero la visione o ascolto. Se invece le riprese o ascolto avvengono in luoghi liberamente accessibili, senza dover superare o rimuovere ostacoli, si ritiene che le persone riprese siano consapevoli della loro esposizione e non possano quindi pretendere particolari tutele (Corte di Cassazione, Sentenza 47165/2010).

Pubblicità

<#? QUI-PUBBLICITA-MIM-[AP1002] ?#>

Ciò premesso, e nell'attesa che possa uscire presto uno specifico provvedimento del garante, coordinato con altre iniziative europee, offro ai lettori un prezioso documento, recentemente pubblicato negli Stati Uniti, che dà indicazioni analitiche su come si possano tutelare i dati personali, che possono essere accidentalmente catturati durante un'attività di vigilanza ispettiva.

1. Se l'operatore del drone ritiene che sia possibile la cattura di dati personali, anche in forma accidentale, deve dotarsi di una politica di gestione di questi dati.
2. Quando il soggetto ripreso, cioè l'interessato, dimostra nei fatti di avere ragionevoli aspettative di tutela dei suoi dati personali, si presti la massima attenzione a non catturare dati, salvo situazioni estreme
3. Occorre evitare la raccolta sistematica di dati personali, se non si è in possesso di una specifica autorizzazione da parte dell'interessato o esistano altri motivi di valenza superiore, come ad esempio la tutela della sicurezza e dell'incolumità pubblica.

4. Nel pianificare l'attività di vigilanza ispettiva, occorre ridurre al minimo il sorvolo di proprietà private, almeno nei limiti in cui questo sorvolo è assolutamente necessario, per realizzare le finalità stesse dell'attività per cui il drone viene utilizzato.
5. Si provveda immediatamente alla cancellazione o alla anonimizzazione di dati personali che non siano necessari per le finalità per le quali il drone viene utilizzato.
6. Si offra la possibilità a qualunque interessato, accidentalmente ripreso, di esercitare il diritto di accesso ai dati che lo riguardano e in particolare il diritto alla cancellazione dei dati stessi, salvo che altre ragioni, da documentare, si oppongano alla cancellazione.
7. Tutti i dati personali raccolti durante le operazioni del drone devono essere limitati al minimo necessario per raggiungere gli obiettivi previsti e non possono essere utilizzati in alcun altro modo, salvo la presenza di speciali esigenze di protezione del sito sotto controllo o della popolazione in generale.
8. Non si devono condividere dati personali acquisiti durante le operazioni del drone per nessun altro motivo, che non sia direttamente legato alla operatività del drone.
9. I dati personali eventualmente acquisiti durante l'operatività del drone non devono essere mai diffusi, salvo esigenze di protezione della sicurezza e salute del pubblico, e non devono essere comunicati a soggetti terzi, se non nell'ambito di rigide e garantistiche procedure di tutela dei dati stessi.
10. L'utilizzo di dati personali acquisiti durante l'attività operativa del drone deve essere limitata alle sole finalità della ripresa e tali dati non possono essere utilizzati per attività di promozione commerciale od altre finalità non inerenti alla ripresa.

Mi sembra un decalogo ben fatto che può certamente aiutare un operatore a comportarsi correttamente, in attesa di un provvedimento specifico dell'autorità garante.

**Adalberto Biasiotti**



Questo articolo è pubblicato sotto una [Licenza Creative Commons](#).

---

[www.puntosicuro.it](http://www.puntosicuro.it)