Nexa Center for Internet & Society
Politecnico di Torino

The Law of Service Robots

Ricognizione dell'assetto normativo rilevante nell'ambito della robotica di servizio: stato dell'arte e prime raccomandazioni di policy in una prospettiva multidisciplinare

Data di pubblicazione: 04/12/2015
Versione 1.0 beta

Curatori: Claudio Artusio, Monica A. Senor.
Autori: Mauro Alovisio, Carlo Blengino, Marco Ciurcina, Giovanni B. Gallus, Guido Noto La Diega, Ugo Pagallo, Massimo Travostino, Giuseppe Vaciago, Paolo Zampella.
Hanno contribuito inoltre: Miryam Bianco, Gian Piero Fici, Alessandro Mantelero, Federico Morando.

La presente pubblicazione è frutto delle riflessioni svolte in seno alla collaborazione di ricerca sugli aspetti giuridici della robotica di servizio attualmente in corso tra il JOL CRAB di TIM ed il Centro Nexa su Internet & Società del Politecnico di Torino - DAUIN.
Ulteriori informazioni sono disponibili all'indirizzo: http://nexa.polito.it/law-of-service-robots

Studying the Internet, exploring its potential & experimenting new ideas

Nexa Center
for Internet & Society

Via Pier Carlo Boggio 65/A, 10129 Torino, Italia
(dove siamo: http://nexa.polito.it/contact)
+39 011 090 7217 (Telefono)
+39 011 090 7216 (Fax)
info@nexa.polito.it

Indirizzo postale:

Centro Nexa su Internet & Società
Politecnico di Torino - DAUIN
Corso Duca degli Abruzzi, 24
10129 TORINO

Il Centro Nexa su Internet & Società è un centro di ricerca del Dipartimento di Automatica e Informatica del Politecnico di Torino (http://dauin.polito.it).

SOMMARIO

EXECUTIVE SUMMARY

Il settore della robotica attiene alla progettazione e costruzione di un **complesso variegato ed eterogeneo di macchine**, quali robot, soldati, chirurghi, sistemi automatizzati di trasporto aereo, terrestre e marittimo, applicazioni industriali nell'ambito manifatturiero o nell'agricoltura, robotica di servizio e altro ancora. Si tratta di un settore per eccellenza interdisciplinare. La sua varietà di ambiti e applicazioni fa sì che si discuta ancora della definizione di "robot" e di alcune sue proprietà: l'autonomia, l'adattatività, e i gradi di interattività.

Tuttavia, il maggiore problema, attualmente, non è tanto quello di determinare se e in che modo i robot "agiscano". La questione verte piuttosto sulla circostanza che **l'interattività, autonomia e adattabilità dei robot sopra citate comportino l'imprevedibilità delle loro azioni**, sia nei confronti dei loro programmatori e costruttori, sia degli stessi proprietari.

Anche rivolgendo l'attenzione unicamente allo specifico ambito della robotica di servizio, le implicazioni sottese alle caratteristiche di tali agenti artificiali involgono questioni complesse rispetto alle responsabilità connesse al loro operare, rendendo opportuna – per chiunque intenda investire nel settore – una riflessione circa le questioni giuridiche e le normative connesse alla progettazione e commercializzazione di robot di servizio.

Non essendo possibile condurre un'analisi dei profili giuridici rilevanti rispetto ad ogni singolo impiego dei robot di servizio, sono state selezionate **tre macro-categorie** che permettano di analizzare le principali implicazioni giuridiche della robotica di servizio nel suo complesso: 1**) telepresenza mediante robot**; 2) **robot courier** all'interno di ambienti di differente complessità; 3) **droni-multicotteri operanti in contesti urbani**, nell'ottica della spinta evolutiva che le tecnologie ICT imprimono alla progettazione degli spazi urbani (c.d. *smart cities* o città intelligenti).

A corredo delle macro-categorie, è stato considerato anche il peculiare campo emergente della c.d. ***cloud robotic*s**, ossia uno scenario in cui i robot sfruttano infrastrutture di tipo cloud disponibili in rete al fine di migliorare il proprio apprendimento e la relativa performance.

Se una tale perimetrazione può rendere più agevole la conduzione dell'indagine, un tentativo di **aprioristica classificazione dei robot** a seconda dei differenti tipi di automazione – nell'ottica di basare su detta classificazione l'individuazione dei profili e delle norme giuridiche di volta in volta rilevanti – si rivelerebbe invece potenzialmente sterile. Ciò perché, se da un lato il diritto non ha ancora pienamente catalogato e definito molti aspetti legati al digitale ed alle reti di comunicazione elettronica, rendendo così più difficile la regolazione del mondo immateriale dei byte, dall'altro, nel campo della robotica, le cose si complicano ulteriormente, dato che con essa le inedite potenzialità del digitale abbandonano il mondo virtuale, per incidere direttamente, senza mediazione alcuna, sulla realtà fisica. Ecco che, per quanto si cerchino di individuare parametri oggettivi, **la malleabilità logica delle tecnologie digitali**, la **continua evoluzione** delle stesse, **nonché la multi-funzionalità potenziale di ogni macchina**, rendono vano ogni tentativo di catalogazione. Pensare quindi di comporre astratte categorie di robot sulla base delle caratteristiche della macchina, dell'uso cui è destinata, delle sue modalità di impiego, o ancora del suo grado di autonomia nell'agire, costituirebbe, allo stato attuale, un *modus operandi* inattendibile e, in ultima istanza, inutile.

È da preferirsi, invece, un **approccio pragmatico caso per caso**, cosicché giuristi, produttori e inventori non si lascino imbrigliare da categorie e vincoli (anche mentali) che difficilmente possono appartenere ad un mondo che ancora non esiste. A tal fine, è fondamentale un'analisi puntuale dei progetti in via di sviluppo, la cui complessa architettura impone un approccio quanto più concreto possibile.

I **principali aspetti giuridici** potenzialmente rilevanti per gli scenari qui considerati sono stati quindi analizzati in conformità all'impostazione metodologica appena descritta. Laddove possibile, si sono unite – all'analisi di tali profili – anche alcune prime raccomandazioni di policy, con esplicito riferimento alla normativa di volta in volta pertinente. Ogni profilo giuridico è stato esaminato secondo uno **schema espositivo comune**: l'analisi si apre con un'introduzione alla materia giuridica in relazione alle casistiche-tipo dei robot di servizio; sono successivamente considerate le problematiche giuridiche rilevanti e la normativa di riferimento applicabili; infine, è ponderata la possibile ripartizione delle responsabilità tra i vari soggetti coinvolti nella progettazione e realizzazione dei modelli robotici i sviluppati.

Seguendo questa impostazione, i profili giuridici considerati hanno per oggetto: la responsabilità civile e penale; la privacy e il trattamento dei dati; la digital forensics e la cyber security; i diritti su beni immateriali; il Regolamento ENAC per l'impiego di mezzi aerei a pilotaggio remoto

La gestione di profili di **responsabilità civile** nell'ambito degli scenari di robotica di servizio è cruciale nell'ottica della

implementazione concreta dei singoli progetti e della loro sostenibilità economica. Un'analisi delle relazioni tra i vari soggetti e dei rispettivi profili di rischio risulta infatti determinante per individuare gli accorgimenti e le cautele che consentono di ridurre – trasferendolo su altri soggetti, oppure neutralizzandolo – il rischio a carico di determinati attori del sistema.

La costruzione, la commercializzazione e l'uso dei droni rilevano ai fini della responsabilità civile sia sul piano del fatto illecito in senso stretto, sia sul piano della c.d. responsabilità "indiretta" (di padroni e committenti) e della responsabilità oggettiva o quasi oggettiva (c.d. danno imputabile a cose).

L'aspetto più importante, al fine di inquadrare le differenti modalità in cui la responsabilità degli agenti può concretizzarsi, è quello delle **diverse forme di imputabilità**: accanto alla tradizionale imputabilità "soggettiva" per dolo o colpa, vi sono una serie di criteri di imputabilità c.d. "speciale", che prescindono – in tutto o in parte – dall'esistenza di uno stato soggettivo rilevante in capo all'agente, per fondarsi su altri e più variegati elementi (la relazione con l'oggetto/soggetto causatore del danno; l'assunzione del rischio; la valutazione del rapporto socio-economico tra danneggiante e danneggiato e la conseguente imputazione del danno al soggetto che appare maggiormente in grado di sostenerlo economicamente).

In questa seconda categoria di criteri di imputazione, troveranno soprattutto soluzione i casi nei quali l'imprevedibilità delle azioni dei robot induca a teorizzare una capacità di autodeterminazione delle macchine, e a preconizzare così una sorta di "responsabilità del robot". Per il momento, infatti, quest'ultima non può trovare collocazione nel nostro ordinamento, in quanto esso individua – quali possibili centri di imputazione della responsabilità civile – unicamente le persone fisiche e giuridiche. Pertanto, **le conseguenze giuridicamente rilevanti che derivano dall'imprevedibilità dell'azione dei robot – a seconda dei casi – saranno sussumibili nella categoria del caso fortuito/forza maggiore, oppure costituiranno fonte di responsabilità risarcitoria in capo al soggetto o ai soggetti cui potranno venire ricondotte sulla base delle regole di imputabilità** (soggettiva o oggettiva) previste dall'ordinamento.

Per gli operatori del settore, il punto critico è costituito dalla preventiva identificazione del soggetto sul quale possono ricadere le conseguenze della responsabilità civile derivante dai robot, nonché dagli strumenti e modalità con cui detta responsabilità può essere allocata su soggetti diversi, attraverso clausole di esenzione di responsabilità, meccanismi di rivalsa, responsabilità solidale.

Se è generalmente esclusa, nel nostro ordinamento, la possibilità di limitare preventivamente la responsabilità extracontrattuale con apposite clausole di esonero, così non avviene, invece, in ambito contrattuale. Pertanto, un modo per gestire il rischio derivante dalla progettazione, costruzione e utilizzo dei robot, può essere quello di **stipulare contratti adeguati che gestiscano l'allocazione del rischio e delle relative responsabilità tra i diversi soggetti**.

Nei casi in cui non possa essere concluso un contratto, è comunque consigliabile prevedere e cercare di **creare una relazione tra l'attore e il soggetto destinatario delle interferenze causate dalla macchina**: ad esempio, mediante annunci con appositi cartelli posti nell'area di azione del robot; tramite controllo degli accessi all'area; o, ancora, con la tracciatura del raggio di azione del robot. Tali iniziative potranno valere quale limitazione "indiretta" di responsabilità.

In una diversa prospettiva, un altro punto cruciale per la gestione della responsabilità è la **tracciabilità delle operazioni compiute attraverso i robot**, mediante, ad esempio: registrazioni di sistema (*log*) dei parametri rilevanti di funzionamento del robot, riprese video dell'attività svolta, relazioni scritte sulle missioni compiute, rapporti relativi alla situazione ambientale in cui il robot opera.

Quale strumento di gestione del rischio, infine, vi è la stipula di apposite assicurazioni contro la responsabilità civile: sia quelle eventualmente imposte dalla legge, sia quelle che l'agente reputi opportuno adottare a propria tutela.

Le caratteristiche essenziali dei robot di servizio – unitamente alla loro interazione con il mondo reale – aprono scenari nuovi anche in relazione ai profili di **responsabilità penale**.

Poiché la creazione, la gestione e l'utilizzo dei robot di servizio possono coinvolgere numerose persone (dal progettista, al produttore di un singolo componente, all'assemblatore, al gestore della piattaforma cloud che fornisce il servizio per la gestione dell'agente artificiale, fino ad arrivare all'utente finale, o al pilota nel caso dei droni), **eventuali profili di responsabilità dovranno essere ricostruiti, caso per caso, a seconda delle circostanze di fatto che hanno determinato nella fattispecie concreta la lesione** di interessi protetti dall'ordinamento. In caso di responsabilità penale colposa, si dovrà inoltre analizzare lo specifico comportamento, per verificare se siano state previste adeguate misure di sicurezza atte ad evitare l'evento e, in caso affermativo, per quali motivi esse non abbiano nel concreto funzionato.

Se l'eventuale danneggiamento di beni materiali da parte di un robot non integra alcun reato, in quanto non è previsto nel nostro ordinamento un reato di danneggiamento colposo, diversa è la situazione nell'ipotesi di danni cagionati a persone fisiche, condotta qualificata come reato di lesioni personali e punita sia a titolo di dolo che a titolo di colpa**. L'allocazione della responsabilità penale per i danni fisici arrecati dall'interazione di un agente artificiale con uno o più esseri umani sarà determinata dall'analisi del singolo fatto concreto**: a seconda della causa dell'azione del robot, la responsabilità potrebbe essere imputata al produttore, al gestore della piattaforma operativa, fino al pilota nel caso di caduta a terra improvvisa di un drone.

Un secondo profilo giuridico riguarda la **problematica attinente al trattamento di dati personali**: nei casi di robot courier

e di telepresenza – trattandosi di attività prestabilite e ben delineate nei presupposti operativi –, sarà sufficiente redigere una chiara privacy policy per dirimere ogni possibile controversia. Diverso il caso dei droni, per i quali il regolamento ENAC prevede la necessità di una specifica analisi da riportare nella documentazione sottoposta all'Ente Nazionale per l'Aviazione Civile ai fini del rilascio dell'autorizzazione di volo e stabilisce che debba in ogni caso essere rispettato il principio di necessità (secondo cui i sistemi informativi ed i programmi informatici devono essere configurati in modo da ridurre al minimo l'utilizzazione di dati personali e dati identificativi).

In caso di trattamento illecito di dati personali, l'allocazione della responsabilità va calibrata sulla scorta dell'attività posta in essere in concreto dai soggetti che il Codice in materia di protezione dei dati personali (D. Lgs. 196/2003) configura come *"titolar[i] del trattamento"*. Essendo il reato costruito come un illecito di modalità di lesione, **la responsabilità penale potrà essere correttamente allocata solo individuando esattamente chi si sia assunto la responsabilità degli adempimenti previsti dal Codice** di cui sopra. Una concreta valutazione del rischio di integrazione del reato sarà quindi strettamente vincolata a – e dipendente da – una corretta individuazione del tipo di dati trattati e della loro natura, ma soprattutto delle persone che avranno il potere di decidere le finalità e le modalità del trattamento dei dati.

In relazione all'attività svolta dai droni, viene inoltre in rilievo la questione relativa alla possibile **captazione di notizie o immagini attinenti alla vita privata**, che potrebbe integrare il reato di interferenze illecite nella vita privata. Il bene giuridico protetto da tale norma sta lentamente evolvendo – in virtù dell'interpretazione giurisprudenziale – dalla tutela del domicilio alla tutela della riservatezza. Sebbene la Corte di Cassazione e la Corte Costituzionale si siano espresse sul punto restringendo l'ambito di tutela del domicilio, **restano aperte numerose questioni giuridico-interpretative nel caso in cui atti capaci di interferire illecitamente con la vita privata altrui siano posti in essere da agenti artificiali**. In ragione di tali incertezze, l'unico criterio che si può indicare – al fine di orientare coloro che intendano investire nel settore – è che il nostro ordinamento giuridico, seguendo l'attuale tendenza europea, potrebbe nel prossimo futuro propendere per una maggiore protezione della riservatezza e dei dati personali dei cittadini.

Come si è già potuto evincere dai paragrafi precedenti, poiché i robot sono forniti dell'abilità di percepire, elaborare e memorizzare il mondo intorno a loro, essi costituiscono potenzialmente un pericolo per la **privacy**: essi possono, infatti, vedere e sentire ciò che sovente è inibito all'uomo, accedere a luoghi normalmente irraggiungibili, ed essi possiedono inoltre una resistenza e una memoria sempre più spesso superiori a quelle umane.

Uno dei principali problemi di privacy è legato alla circostanza che **la memoria interna dei robot di servizio è spesso alquanto limitata**; per questa ragione, tradizionalmente, tutta una serie di dati viene trasmessa dal dispositivo all'esterno per finalità di analisi e memorizzazione. **D'altra parte, l'avvento della *cloud robotics***, utilizzata per l'archiviazione e per l'elaborazione remote dei dati, **solleva dal dover passare per il produttore**. La sicurezza delle informazioni su cloud – un tempo assai controversa – diviene oggi sempre più solida, specialmente grazie ai nuovi sistemi di cifratura omomorfica, che sarebbe opportuno prevedere nel contratto con il cloud provider, contestualmente a specifiche attinenti alla geo-localizzazione delle server farm.

Per quanto riguarda le potenziali **ricadute su privacy e trattamento di dati personali in caso di telepresenza** a fini universitari e di robot museali, si rileva quanto segue. Nel primo caso, mentre per i dati riguardanti l'osservatore non emergono problemi di riservatezza particolarmente rilevanti, non altrettanto si può dire per i dati di docenti e discenti presenti in aula: sul punto si possono immaginare sia **soluzioni di *privacy by design*** (ad es., un saluto vocale in cui il robot trasmette un'informativa sulla *privacy*), sia **soluzioni più tradizionali** (ad es., l'affissione di cartelli simili a quelli usati per segnalare la presenza di telecamere). Il discorso è analogo per i robot museali, che sollevano ancora minori problemi, considerato che essi si muovono in spazi ridotti e di norma sono totalmente autonomi; in questo caso, l'unico accorgimento consiste nel far sì che l'addetto al robot o chi abbia accesso alla memoria dello stesso (e, nel caso di *cloud robotics*, al web storage) si impegni a non divulgare in alcun modo le informazioni per tal via apprese.

I **robot courier**, invece, si muovono in spazi ampi e complessi, sono in grado di acquisire un considerevole novero di dati anche sensibili e, grazie a sistemi di face recognition, possono riconoscere l'utente. In uno scenario di trial convegnistico potrebbe essere sufficiente inserire un'apposita indicazione nei moduli di registrazione all'incontro; nel caso di centri commerciali o ambienti analoghi, si potrebbe procedere a **limitare, via privacy by design, l'operatività della face recognition** (o, addirittura, la fissazione stessa del video) alla fase in cui il potenziale cliente attiva volontariamente il robot, salvaguardando così l'immagine di quanti si incroceranno nel percorso. Rispetto ai dati sensibili del potenziale cliente, si potrebbe poi immaginare **un'informativa con sistema "a spunta"**, tale per cui non si procederà all'interazione in assenza di consenso.

Quanto ai **droni-multicotteri**, è intuitivo che essi sollevino problemi di privacy maggiori rispetto ai robot di servizio, potendo essere raffigurati, in sostanza, come vere e proprie telecamere volanti.

Una recente **comunicazione della Commissione Europea** sull'uso civile dei sistemi aerei a pilotaggio remoto ha chiarito che la loro progressiva integrazione nello spazio aereo dovrà essere accompagnata da un adeguato dibattito pubblico sullo

sviluppo di misure in grado di affrontare le preoccupazioni della società, tra cui la tutela dei dati e della vita privata.

In Italia è prevista una disciplina specifica, contenuta nel **regolamento ENAC all'art. 34**, disposizione di chiusura della sez. VI ("Disposizioni Generali per i Sistemi Aeromobili a Pilotaggio Remoto") e rubricata "*Protezione dei dati e privacy*. Quantunque la disposizione per lo più rinvii alla disciplina sulla protezione dei dati personali, vanno apprezzate sia l'esplicitazione della necessità che la documentazione richiesta dia conto dei problemi sollevati dal drone in materia di privacy, sia la sensibilità del legislatore nel cogliere il trend della minimizzazione della raccolta dei dati. Il rinvio alla determinazioni del Garante, poi, si potrà rivelare uno strumento assai agile, in considerazione delle semplici e rapide procedure decisionali dell'Autorità.

Risultano altresì di grande importanza le discipline della **digital forensics** e della sicurezza informatica collegata alla robotica. Infatti, un aspetto fondamentale da considerarsi nel momento dell'accertamento della responsabilità in caso di incidente dovuto a malfunzionamento del robot o del drone è rappresentato dalla possibilità di ricostruire le modalità con cui esso sia stato progettato ed abbia operato in concomitanza dell'evento dannoso.. Nel caso in cui un robot subisca un cyber-attacco cui consegua un incidente – od anche solo un malfunzionamento –, la digital forensics diventa allora strategica per cercare di comprendere, **attraverso il recupero e la cristallizzazione di prove digitali, le ragioni di tali accadimenti**.

In caso di utilizzo di sistemi di *cloud robotics*, potrebbe aumentare il **rischio di una responsabilità a carico del gestore del servizio cloud**, il quale, in caso di mancata adozione delle misure di sicurezza previste dal codice privacy, potrebbe incorrere in una sanzione di natura penale o in una richiesta di risarcimento da parte del danneggiato. Allo stesso modo, anche lo **sviluppatore di applicazioni per il robot** o per il drone dovrà sempre tenere in grande considerazione i profili di sicurezza perché, qualora attraverso una sua applicazione fosse possibile perpetrare un attacco informatico, sarebbe possibile far ricadere su di lui la responsabilità dell'evento dannoso o del malfunzionamento. Con un minor grado di rischio, anche altri soggetti – come il produttore o l'assemblatore del robot o del drone o, ancora, l'utente – possono essere responsabili a vario titolo in caso di malfunzionamento. Va anche considerato che, in caso di incidente, l'utente potrebbe essere in grado di alterare significativamente la prova digitale, qualora la stessa non risieda nei cloud server; per questa ragione, sarebbe interessante **ipotizzare per i droni e robot una "black box"** che permetta di registrare, cristallizzare e conservare in modo idoneo tutti gli eventi che precedano l'eventuale incidente.

Tra i prioritari aspetti legali interconnessi cui le discipline della digital forensics e della cyber security dovranno rivolgere la loro attenzione, vi sono dunque: la formalizzazione di regole e procedure per l'acquisizione e l'utilizzo della prova informatica nel rispetto di best practices nazionali e internazionali; la formalizzazione di regole e procedure di cyber security idonee a proteggere il robot o il drone da eventuali attacchi informatici; **il rispetto della privacy dell'utente, rispetto che andrà costantemente bilanciato con esigenze di conservazione e di sicurezza del dato**, proprie della digital forensics e della cyber security.

Per quanto riguarda i **diritti su beni immateriali** (in primis, diritto d'autore e diritti connessi; diritti di proprietà industriale; diritti della personalità), questi conferiscono – ai loro titolari – diritti esclusivi o di credito nei confronti dei terzi che facciano un certo uso di beni immateriali.

Tali set normativi **possono interferire con la robotica di servizio a diversi livelli:** nella produzione d'un robot o di un drone si possono infatti creare od utilizzare elementi tutelati da tali diritti, ed anche nell'uso di un robot o di un drone possono entrare in gioco elementi da essi tutelati. La fitta rete di esclusive che deriva dalla legislazione in materia di beni immateriali rende quindi difficile la collaborazione ed il riuso anche nel campo della robotica di servizio.

Per ovviare a questo genere di problemi, sono stati sviluppati diversi modelli di licenza che stabiliscono esplicitamente la facoltà di riuso da parte dei terzi, in questo modo favorendo anche la collaborazione; grazie ad essi, si sono potuti realizzare "beni comuni" come il software libero, l'open hardware e banche dati di contenuti (ad es., Wikipedia)

Si ritiene perciò opportuno che gli attori coinvolti: individuino **una corretta policy di acquisizione degli elementi tutelati da diritti**, che includa anche la verifica del fatto che non si violino diritti di terzi (tenuto conto dei vincoli imposti dalle licenze che si riferiscono agli artefatti software acquisiti); implementino una corretta policy di licenza dei diritti sugli artefatti messi a disposizione dei terzi; ricordino che la realizzazione di artefatti può essere frutto dell'opera di soggetti diversi (dipendenti, terzi fornitori, o frutto del riuso di componenti disponibili al pubblico secondo i termini di una licenza di software libero).

La distribuzione delle responsabilità tra i diversi soggetti coinvolti (fornitori di soluzioni software/hardware per la connessione di robot di servizio attraverso reti a banda larga, produttori hardware, creatori delle applicazioni software) **si può modulare secondo le modalità di licenza** degli artefatti (software e banche di dati) utilizzati dall'utente per il funzionamento del robot/drone. Inoltre, poiché – nei confronti dei consumatori – è più complesso far valere clausole di esclusione e/o limitazione della responsabilità, potrebbe essere utile evitare di configurarsi come fornitori di servizi ai consumatori. Tuttavia, qualora si fornissero servizi e/o software ai consumatori, si potrebbero adottare due strategie diverse per limitare il rischio di dover rispondere dei danni conseguenti al loro uso: **a) licenziare servizi e software ai propri partner commerciali affinché questi li licenzino a loro volta ai loro clienti assumendo su di sé le responsabilità** derivanti; **b) partecipare alla creazione di "beni comuni"** (software libero; banche dati aperte), eventualmente resi disponibili da enti terzi *no profit* che forniscano

funzionalità (software o servizi) da far usare ai partner commerciali e/o agli utenti, dato che – nei casi in cui si configuri un accesso diretto dal consumatore al "bene comune" – si potrebbe evitare anche al produttore hardware e/o allo sviluppatore software di assumere il rischio conseguente all'uso del servizio/software.

Da ultimo, completa l'analisi una descrizione dell'impianto normativo del **Regolamento emanato dall'ENAC** per l'impiego di mezzi aerei a pilotaggio remoto, regolamento di cui è entrata in vigore – nel settembre 2015 – la seconda edizione.

Il regolamento costituisce, in assenza di definizione di standard a livello internazionale, un prezioso punto di riferimento normativo, in quanto fornisce un **primo inquadramento giuridico del fenomeno**, come pure indicazioni e risposte a utenti, operatori ed imprese. Il regolamento merita di essere segnalato anche per la **preziosa sinergia instaurata dall'ENAC con il Garante per la protezione dei dati personali** ai fini della redazione dell'art. 34 – riguardante quelle operazioni svolte dal drone che comportino un trattamento di dati personali–, costituendo in tal senso un esempio di *best practice* a livello comunitario. Ancora, merito deve essere riconosciuto alla sua seconda edizione, per aver reso meno stringenti le condizioni di volo dei droni nei cieli italiani (si veda, ad es., la novità dei SAPR al di sotto dei 2 chilogrammi), aprendo così la strada per un sempre maggiore sviluppo del mercato, pur senza perdere di vista l'esigenza primaria di tutela della sicurezza.

La difficoltà più grande presentatasi all'ENAC è stata quella di condensare a livello tecnico ed in un unico atto molteplici profili disciplinari relativi al mezzo, all'operatore, ai piloti, nonché alle varie tipologie di droni. **Ci si domanda** altresì **se una criticità applicativa possa essere costituita dall'effettività dei controlli:** l'ENAC sarà effettivamente in grado di effettuare i controlli previsti o si troverà invece, in considerazione delle scarse risorse, a dover delegare tali funzioni ad altri enti?

Per questo motivo, nonostante i lodevoli sforzi, un regolamento potrebbe non rappresentare lo strumento più adatto a disciplinare la materia in oggetto, considerata anche la complessità e dinamicità di quest'ultima; essendo **forse preferibile la scelta** – compiuta da altri Paesi europei (Francia, Svizzera e Gran Bretagna) – **di adozione di linee guida**.

1 INTRODUZIONE ALLA ROBOTICA DI SERVIZIO

(a cura di Ugo Pagallo)

Con il termine inventato da Isaac Asimov nel racconto del 1941 *"Liar!"*, **la "robotica" è il settore che attiene alla progettazione e costruzione di un complesso variegato ed eterogeneo di macchine**, quali robot soldati e chirurghi, sistemi automatizzati di trasporto aereo, terrestre e marittimo, applicazioni industriali nell'ambito manifatturiero o nell'agricoltura, robotica di servizio e altro ancora. Si tratta di un **settore per eccellenza interdisciplinare**, nel quale convergono ricerche d'informatica e cibernetica, matematica e meccanica, elettronica e neuroscienza, biologia e scienze umane, tra cui la psicologia, l'economia e il diritto. Questa varietà di ambiti e applicazioni ha fatto sì che si discuta ancora sulla definizione di "robot" e su alcune sue proprietà, quali l'"autonomia", l'"adattatività" o i gradi di "interattività".

Alcuni studiosi definiscono la robotica come l'area dell'intelligenza artificiale volta alla costruzione di macchine in grado di *"sentire, pensare e agire"*[1]. Altri, come il direttore dei Laboratori d'intelligenza artificiale presso l'Università di Stanford, Sebastian Thrun, presentano i robot come macchine con l'abilità di *"percepire alcunché di complesso e prendere decisioni appropriate"*[2]. Mentre ulteriori definizioni insistono sulle capacità d'apprendimento e adattamento dei robot all'evoluzione dell'ambiente, nell'ambito delle applicazioni industriali può rinviarsi alla definizione ISO 8373 – richiamata dalle Nazioni Unite e dal rapporto della Commissione economica per l'Europa e la Federazione internazionale di robotica – per cui un robot è un *"manipolatore multiuso, controllato automaticamente, riprogrammabile e programmato in tre o più assi, che possono essere mobili o fissi in un luogo"*[3].

Da questo tipo di definizioni, tuttavia, sorgono ulteriori problemi. Basti pensare alla Nota sulla dottrina unitaria del Ministero della Difesa del Regno Unito sui "sistemi aerei senza pilota" del 30 marzo 2011, secondo cui il concetto di autonomia va declinato come *"capacità di comprendere un più alto livello di intento e direzione"*, là dove *"stime di quando l'intelligenza artificiale sarà ottenuta (in opposizione a sistemi complessi e intelligentemente automatizzati) variano, ma un certo consenso ruota attorno a più di cinque anni e meno di quindici, con alcune applicazioni ben oltre questa data"*[4]. Altri studiosi etichettano queste previsioni come *"ridicole"*[5], per cui tornano i problemi di convenire sull'idea che i robot siano macchine in grado di "pensare" e "agire". Un modo per venire a capo dei possibili fraintendimenti consiste nel precisare un livello minimo, ma ben definito, delle nozioni. Anche ammettendo che i robot possiedano l'intelligenza di un frigorifero odierno, bisogna concedere che alcune di queste macchine non solo sentano, ma agiscano. Riprendendo la tripartizione proposta da Allen, Varner e Zinser nel saggio sullo status degli agenti morali artificiali[6], **si può dire che un ente – umano, animale o artificiale – "agisce" allorché esso sia interattivo, autonomo e capace di adattarsi al proprio ambiente. Questo in sostanza significa che:**

a) l'agente risponde agli stimoli dell'ambiente attraverso il mutamento degli stati interni o valori delle sue proprietà (*interattività*);

b) l'agente è in grado di cambiare detti stati indipendentemente da stimoli esterni (*autonomia*);

c) l'agente è capace di accrescere o migliorare le regole attraverso cui tali stati cambiano (*adattatività*).

Su queste basi, il problema, oggi, non è tanto quello di determinare se e in che modo gli agenti artificiali e, in particolare, i robot eventualmente "agiscano". Piuttosto, la questione verte sulla circostanza che **l'interattività, autonomia e adattabilità dei robot comportino l'imprevedibilità delle loro azioni, sia nei confronti dei programmatori e costruttori di tali agenti artificiali sia dei loro stessi proprietari**. Per quanto, queste tre peculiarità siano comunque funzionalità inserite *ad hoc* dall'uomo nella programmazione dell'agente artificiale, e la stessa imprevedibilità sopra menzionata sia causata non tanto da una indeterminabilità intrinseca dell'attività dell'agente, quanto piuttosto dalla impossibilità relativa di padroneggiare completamente gli algoritmi che regolano il suo agire, di ipotizzare tutti gli scenari possibili, nonché di tenere conto dell'influenza di ogni elemento del caso di specie.

---

[1] G. A Bekey, *Autonomous Robots: From Biological Inspiration to Implementation and Control*. The Mit Press, Cambridge, Mass., London, England, 2005.

[2] P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, 2009, p. 77. London, Penguin.

[3] UN WORLD ROBOTICS, *Statistics, Market Analysis, Forecasts, Case Studies and Profitability of Robot Investment*, edited by the UN Economic Commission for Europe and co-authored by the International Federation of Robotics, UN Publication, Geneva (Switzerland), 2005.

[4] U. Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts*, p. 2. Springer, Dordrecht, 2013.

[5] N. Sharkey, *Automated Warfare: Lessons Learned from the Drones*, in *Journal of Law, Information and Science*, 2012, 21(2): 10.5778/JLIS.2011.21.Sharkey.1.

[6] C. Allen, G. Varner, e J. Zinser, *Prolegomena to Any Future Artificial Moral Agent*, in *Journal of Experimental and Theoretical Artificial Intelligence*, 2000, 12, p. 251-261.

Il nuovo scenario consiglia di tornare alla distinzione tra le varie applicazioni robotiche, per cui, a quelle industriali, richiamate in precedenza con la definizione ISO 8373, bisogna quantomeno aggiungere le militari e la robotica di servizio. Questa tripartizione è suggerita dai diversi tipi di responsabilità giuridica in gioco.

Da un lato, nel caso della robotica militare, che pure è di gran lunga il ramo più rilevante del settore in termini d'investimento economico[7], siamo alle prese con il diritto penale militare di guerra e di pace, e con il diritto internazionale umanitario. Come riferito il 9 maggio 2014 dal sito web della BBC[8], *"i robot killer saranno oggetto di dibattito presso le Nazioni Unite"*.

D'altro canto, la distinzione tra robotica industriale e di servizio è suggerita dal già citato rapporto ONU del 2005, per via del diverso tipo e uso di applicazioni in gioco. Oltre a un diverso campo di responsabilità giuridica sul fronte penale, esistono nondimeno, almeno in parte, comuni problemi di natura contrattuale ed extra-contrattuale.

Tornando alle definizioni, **nell'ambito della robotica di servizio occorre distinguere due sotto-classi**. La prima riguarda le **macchine di servizio professionale** che includono sistemi d'ispezione, costruzione e demolizione, logistica, medicina, difesa, salvataggio e sicurezza, pulizia, relazioni pubbliche, etc. La seconda sotto-classe riguarda **l'uso domestico e/o personale di robot per educazione ed intrattenimento, assistenza e trasporto, sicurezza e sorveglianza domestica, etc**. A seconda del tipo di macchina, o agente artificiale, e del suo uso, muta di conseguenza lo spettro di questioni (e tipi di responsabilità) giuridiche cui occorre assegnare priorità. Basti segnalare i due approcci tipici dell'ambito HRI (*Human-Robot Interaction*): l'uno centrato sull'uomo, l'altro sul robot.

Nel primo caso, l'HRI è innanzitutto interessata al modo in cui un robot adempie alla specifica dei suoi compiti in modo tale da essere accettabile e confortevole per gli umani. Nel secondo caso, l'enfasi cade sul robot come una *"creatura, vale a dire un'entità autonoma che persegue i propri fini sulla base delle proprie motivazioni, impulsi ed emozioni"*[9]. Quest'ultima prospettiva dell'umano "badante" del proprio robot risulta del resto meno stravagante di quanto possa apparire a prima vista, non appena si consideri l'interattività, autonomia e adattatività dei robot, cui si è fatto cenno in precedenza. Queste proprietà in pratica comportano che la stessa applicazione robotica che abbiamo intenzione di comprare, poniamo, il prossimo Natale, finirà per comportarsi diversamente, dopo poche settimane o giorni, a seconda di come abbiamo "trattato" il robot. **Ferme restando le eventuali responsabilità dei costruttori e disegnatori di simili macchine, chi risponde nel caso in cui il nostro compagno artificiale provochi un incidente?**

La risposta dipende evidentemente dal tipo di robot domestico e, in genere, di servizio, del quale ci occupiamo. Stante l'importanza di queste distinzioni, la prossima Sezione provvederà a circoscrivere l'ambito della presente ricerca individuando e descrivendo alcune tipologie di impiego dei robot; nello specifico, verranno considerate tre casistiche-tipo rispetto alle quali condurre l'analisi delle pertinenti implicazioni giuridiche.

2 ALCUNE POSSIBILI CASISTICHE-TIPO DI IMPIEGO DEI ROBOT

(a cura di Claudio Artusio)

Come evidenziato nel corso della Sezione precedente, il settore della robotica si riferisce ad un complesso di macchine estremamente eterogeneo, in virtù delle peculiari funzionalità del robot e dei differenti ambiti di applicazione di questo; la sola famiglia della robotica di servizio, cui si rivolge la nostra attenzione, si presta ad un'ampia gamma di possibili impieghi, tra i quali si possono citare, a mero titolo esemplificativo, la sorveglianza di ambienti, il trasporto, l'assistenza, l'educazione e l'intrattenimento.

Non essendo ovviamente possibile, in questa sede, condurre un'analisi puntuale dei profili giuridici rilevanti rispetto ad ogni singolo impiego dei robot di servizio, si rende opportuno **selezionare alcune macro-categorie, che permettano di compendiare quelle tra le principali implicazioni giuridiche che possano riferirsi all'intera famiglia**, a prescindere dalle ulteriori ramificazioni "di genere e di specie" – per così dire – che i molteplici contesti d'uso porterebbero a loro volta ad individuare.

In particolare, l'analisi dei profili giuridici, oggetto della Sezione 4, verrà condotta rispetto a tre macro-categorie: **1) telepresenza mediante robot; 2) robot courier all'interno di ambienti di differente complessità; 3) droni-multicotteri operanti in contesti urbani** (nell'ottica della spinta evolutiva che sempre più le tecnologie ICT imprimono nella progettazione degli spazi urbani – c.d. *smart cities* o città intelligenti).

---

[7] Cfr. P. W. Singer, *cit.*, e U. Pagallo, *cit.*

[8] Si veda: http://www.bbc.com/news/technology-27343076.

[9] K. Dautenhahn, *Socially Intelligent Robots: Dimensions of Human-Robot Interaction*, in *Philosophical Transactions of the Royal Society B: Biological Sciences*, 2007, 362(1480), p. 683.

A corredo di tali macro-categorie, **si terrà in considerazione** – per via delle implicazioni giuridiche che potrebbe concorrere a determinare – **anche quel peculiare campo emergente della robotica che viene definito *"cloud robotics"*, ossia, uno scenario in cui i robot sfruttano infrastrutture di tipo cloud disponibili in rete al fine di migliorare il proprio apprendimento e la relativa performance.**

Tra i possibili servizi basati sulla *cloud robotics*, risultano **in corso di studio soluzioni software/hardware in grado di connettere da remoto robot di servizio attraverso reti a banda larga per fornire funzionalità di supporto allo sviluppo di applicazioni.** Propedeutiche al design vero e proprio di una piattaforma sono le fasi di trial, mediante le quali viene testato il lato hardware dei robot, al fine di verificarne le criticità/potenzialità in specifici contesti. Raccogliere tali evidenze rappresenta una fase necessaria per studiare come e con quali caratteristiche dovrà essere implementato il software, ossia appunto la piattaforma di servizi cloud rivolta ai produttori di tecnologia robotica – che troveranno in essa un ambiente entro cui sviluppare prodotti e applicazioni – ed agli utenti finali del robot di servizio – i quali accederanno ad essa per aggiornare ed incrementare le prestazioni e funzionalità del robot.

Nello specifico, una piattaforma di questo tipo deve essere sufficientemente aperta, in modo da poter accogliere più di una sola tipologia di prodotto e costituire quindi un *layer* di servizi attraente per il mercato dei produttori di robot di servizio. Tipicamente, proprio al fine di agevolare il raggiungimento di tale obiettivo, soccorre – nello sviluppo della piattaforma – **il software open source ROS (*Robot Operating System*)**[10]: alcune caratteristiche del ROS – tra cui, in particolare, l'opportunità di sviluppare software *"robot independent"*, nonché di distribuire in rete le componenti delle applicazioni robotiche – risultano infatti essenziali per dotare la piattaforma dei necessari requisiti di flessibilità e versatilità.

La telepresenza mediante robot – macro-categoria n. 1 – è volta ad aggiungere, alle tradizionali forme di partecipazione ad incontri e attività da remoto (ad es., *videochat*)**, funzioni aggiuntive di mobilità** all'interno di ambienti non strutturati. Alcuni possibili contesti d'uso sono rappresentati dall'ambiente universitario – in cui la telepresenza può impiegarsi per la fruizione di lezioni o la partecipazione a lavori di gruppo/attività ricreative in caso di disabilità o di impossibilità di altro tipo ad essere fisicamente presenti (ad es., partecipazione a programmi di scambio) – e dall'ambito aziendale – in cui incontri o visite possono essere effettuati da remoto senza che l'interazione abbia a svolgersi all'interno di un singolo ambiente, in quanto lo spostamento da un locale all'altro (uffici, strutture, aree, impianti, etc.) è reso possibile dalla deambulazione mediante robot.

Il robot courier – macro-categoria n. 2 – svolge invece una funzione di assistenza all'interno di ambienti complessi, funzione che si espleta nel condurre il visitatore al luogo di interesse prescelto; il robot deve cioè essere in grado di interagire con il visitatore e di accompagnarlo nel punto di interesse, evitando eventuali ostacoli "non previsti" sul percorso (altre persone o oggetti, fissi e in movimento). Ovviamente, il grado di complessità nello svolgimento della prestazione cresce a seconda dell'ambiente entro il quale il robot si trovi ad operare: una conferenza, gli uffici di un'azienda, i reparti di un ospedale, un campus universitario o un centro commerciale, ad esempio, sono spazi tra loro differenti e che involgono differenti interazioni con l'utente, oltretutto in aree progressivamente più ampie e complesse.

Nell'analizzare i profili giuridici inerenti tanto alla prima quanto alla seconda macro-categoria **si assumerà che la prestazione venga effettuata da robot assemblati con le medesime componenti.**

In particolare, si adotterà – quale robot "ideale" – un modello ipotetico, costituito da una base robotica (un carrellino tipo *rover*) e da una telecamera di tipo *pan-tilt* che possa essere orientata indipendentemente dal movimento del robot. Il flusso video è veicolato, mediante rete wireless, sulla stessa connessione dati utilizzata per il controllo del robot. Il robot incorpora un *laser scan* per la localizzazione e la navigazione all'interno dell'ambiente e può utilizzare differenti reti wireless per la connessione (es. WiFi, 3G, 4G).

Si noti che **è possibile che il robot sia materialmente assemblato da un soggetto diverso da colui che lo ha progettato e che ne ha curato la fase di sperimentazione. Inoltre, il robot potrebbe integrare componenti realizzate da produttori differenti.**

Come si è già accennato, la realizzazione di robot, applicazioni robotiche e servizi di supporto – nonché, da ultimo, la fruizione di questi da parte dell'utente finale – comporta il coinvolgimento di molteplici soggetti: dal produttore di una o più componenti del robot (che non è necessariamente lo stesso soggetto che le assemblerà) al fornitore del servizio *cloud* cui il robot può connettersi per aggiornare e migliorare le proprie prestazioni; dallo sviluppatore di applicazioni all'utente stesso. Quest'ultimo, acquistando il robot, ne diviene proprietario, e potrebbe dunque essere ritenuto responsabile in caso di utilizzi impropri del prodotto. **Tenere in considerazione i vari soggetti e ponderarne le possibili interazioni risulta pertanto fondamentale al fine di stabilire come si configurino e si ripartiscano le diverse responsabilità di volta in volta rilevanti.**

Tabella 1: Comparto sensori dei robot e relative prestazioni – come assunte ai fini delle macro-categorie nn. 1 & 2

Prestazione della	Scopo della prestazione	I dati raccolti	I dati osservati vengono

[10] Il software, distribuito con licenza BSD, fornisce librerie e tools per aiutare gli sviluppatori nella creazione di applicazioni robotiche.

componente		attraverso la prestazione vengono conservati?	trasmessi dal robot all'esterno? (server/piattaforma online/etc.)
Laser scanner	Riconoscimento di ostacoli, costruzione mappe, localizzazione	Solo in modo parziale	A volte, tramite messaggi verso server e *Graphical User Interface* (GUI)
Telecamera singola	Riconoscimento oggetti, costruzione mappe, localizzazione	Solo in modo parziale	A volte, tramite messaggi verso server e GUI
Telecamera RGB-D	Riconoscimento di ostacoli, costruzione mappe, localizzazione	Solo in modo parziale	A volte, tramite messaggi verso server e GUI
GPS	Determinazione della posizione del robot	Solo in modo parziale	A volte, tramite messaggi verso server e GUI
Sensore inerziale	Determinazione dei movimenti del robot	No	A volte, tramite messaggi verso server
Sonde di temperatura	Misura della temperatura	Sì	Tramite messaggi verso server e GUI
Bumper	Riconoscimento di ostacoli	No	A volte, tramite messaggi verso server
Sonar	Riconoscimento di ostacoli	No	A volte, tramite messaggi verso server
Telecamera termica	Cattura immagini termografiche	Sì	Tramite messaggi verso server e GUI
Sonde di temperatura	Misura della temperatura	Sì	Tramite messaggi verso server e GUI

Per quanto riguarda i **droni-multicotteri operanti in spazi urbani** – macro-categoria n. 3 – ed al pari di quanto effettuato con riferimento alle macro-categorie nn. 1 e 2, si considererà anche l'ipotesi di impiego di tecnologie *cloud*, intese qui alla realizzazione di sistemi di controllo e monitoraggio centralizzato per l'abilitazione di scenari di servizio basati su Aeromobili a Pilotaggio Remoto (APR) in ambiente c.d. *smart city*.

Come è noto, diversi tipi di droni[11] sono sviluppati per l'impiego in contesti militari o in contesti civili. La presente trattazione si rifarà unicamente a questo secondo contesto, assumendo quale modello – ai fini dell'analisi ivi condotta – i droni-multicotteri di derivazione aeromodellistica.

Circa le modalità di controllo dei movimenti di un APR che vengono oggi impiegate, si può distinguere sostanzialmente tra: a) telecontrollo diretto manuale; e b) controllo automatico attraverso una *Ground Control Statio*n (GCS). Nella modalità a), il pilota assume il controllo completo del drone attraverso un comando *joystick*, con il quale si impartiscono i movimenti al drone. Nella modalità b), i comandi sono invece gestiti da una postazione di controllo informatizzata situata a terra, che elabora ed impartisce gli ordini al drone per mezzo di un software. Questo sistema di pilotaggio automatico, simile a quelli utilizzati dagli aerei, consente il tracciamento di una rotta tramite posizioni GPS, usando un link radio diretto fra l'APR e la GS.

I potenziali scenari di sperimentazione nell'ambito degli APR ipotizzano tipicamente la presenza di più droni in contemporanea all'interno di un ambiente complesso, contemplando anche la specifica eventualità di potenziali congestioni dello spazio aereo. Dal momento che – al fine di gestire in via ottimale questi scenari – le modalità di pilotaggio a) e b) rischiano di risultare inefficienti, potrebbero **venire in soccorso le potenzialità offerte dalla *cloud robotics*, soprattutto al fine di**

[11] Dal momento che il termine drone viene a volte inteso come qualsiasi veicolo privo di pilota che sia comandato a distanza – e quindi riferito anche a veicoli acquatici e terrestri – si precisa che all'interno del presente deliverable il termine drone (così come le riflessioni sulle implicazioni giuridiche che sorgono con il suo impiego) viene ricondotto unicamente alla tipologia di veicoli volanti (SAPR, secondo la dizione italiana provvista dal relativo regolamento ENAC – *infra*, Sezione 4.6).

gestire le funzionalità più dispendiose dal punto di vista computazionale: ad esempio, spostando su server dette funzionalità, in modo che queste siano trasmesse al drone, anziché essere effettuate direttamente da quest'ultimo.

Figura 1: Quadricottero presentato nel corso della demo del progetto Fly4SmartCity, in chiusura del workshop "Droni: prospettive di ricerca e scenari applicativi" del 7 luglio 2014 (foto: Mauro Alovisio)

3 CATALOGAZIONE E DEFINIZIONI DEI ROBOT DI SERVIZIO E DEI DRONI

(a cura di Carlo Blengino)

Dal byte all'atomo

L'esigenza di definire e catalogare nasconde la presunzione del giurista di ricondurre ciò che accade – e, nel campo della robotica, ciò che accadrà – in consolidati e noti istituti del diritto: è un tentativo di esorcizzare l'*horror vacui* che ci assale di fronte ad accadimenti realmente nuovi ed inediti.

Il diritto non ha ancora pienamente catalogato e definito molti aspetti legati al digitale ed alle reti di comunicazione elettronica (pensiamo alla corretta allocazione delle responsabilità in rete con il dibattito sugli intermediari), e già ci si trova a dover fare un passo avanti**: la difficoltà incontrata dal diritto a regolare e governare il mondo immateriale dei *byte* si riversa con la robotica nuovamente nel reale**, e lo spazio virtuale – dove il codice è stato (ed è) la (prima) legge – torna ad occupare lo spazio fisico in una pressoché inedita commistione tra la gestione di informazioni/dati e più o meno prevedibili modificazioni ed interazioni fisiche, fatte di atomi e materia.

Gli elementi cardine della robotica, ai fini della presente ricerca, risiedono nella sua fisicità e nell'interazione con il mondo materiale.

L'informatica giuridica, sin dagli albori del digitale, si è confrontata con le complesse interazioni tra l'uomo e la macchina – oggi intesa come sistema informativo complesso –, ma si è sviluppata unicamente sul crinale dell'elaborazione e della comunicazione di beni immateriali quali dati e informazioni. Nei tribunali si è assistito a – ed ancora ci si esercita in – rocambolesche analogie tra il prima ed il dopo, tra il reale ed il virtuale: Internet come l'autostrada, l'e-mail come la lettera, il blog con la stampa, il forum come la bacheca, il link come forma di riproduzione. Sono esercizi ermeneutici spesso inutili, se non dannosi, alla risoluzione delle questioni poste dal mondo digitale. **Il diritto dell'informatica fino ad ora ha interessato sì molteplici beni giuridici degni di tutela, ma tutti riconducibili al campo dell'immateriale. La proprietà è stata toccata dalle nuove reti di comunicazione elettronica, ma le criticità si sono manifestate nel campo della proprietà intellettuale e dei beni immateriali**; la persona è stata oggetto di lesione, ma nelle sue estensioni immateriali (ad es., onore e reputazione, identità e riservatezza, abuso dei dati personali).

Con la robotica – quale che sia l'ampiezza di contenuto che a tale termine si ricollega – le cose si complicano: **le inedite**

potenzialità del digitale abbandonano il mondo virtuale e vanno ad incidere direttamente, senza mediazione alcuna, sulla realtà fisica.

Se uno scanner fagocita improvvidamente un manoscritto cinquecentesco facendolo in pezzi, il problema non è fino ad oggi un problema di informatica giuridica: l'interazione tra macchina e documento è mediata dall'uomo. Per converso, un difetto del software di videoscrittura può danneggiare certamente un documento informatico, ma inteso come rappresentazione di dati ed informazioni, non come oggetto fisico, e può essere un problema di *cyberlaw*.

Con la robotica tutto cambia, ed alle complessità del digitale si somma la prepotente interazione dell'agente artificiale con la realtà fisica senza la mediazione diretta dell'agire umano.

Per questa ragione, nella difficoltà di definire e catalogare i robot, **ciò che pare essenziale è proprio il passaggio alla oggettiva modificazione della realtà prodotta dalla macchina, senza mediazione**.

Se, come si rileva nella Sezione 1, *"<sense-think-act>"* sono le tre caratteristiche dei robot, quella che pone problemi realmente nuovi rispetto al diritto dell'informatica è – almeno allo stato attuale della tecnologia – la terza, ovverosia, appunto, quell'agire che – con un prorompenza sostanzialmente inedita – incide senza mediazione sul mondo fisico.

La robotica industriale da tempo è oggetto di regolamentazione, ma l'utilizzo esclusivamente professionale in ambienti fortemente regolamentati e protetti limita il ventaglio di interrelazione con la collettività in generale (sebbene le implicazioni siano notevoli sul piano economico-sociale). Non dissimile la robotica militare, che coinvolge problematiche del tutto peculiari. Da questi settori ovviamente molto può essere attinto quanto alla classificazione e regolamentazione della robotica di servizio, la quale però evidenzia implicazioni assai più complesse, per il potenziale utilizzo generalizzato e "libero" delle nuove macchine agenti.

Forse, il primo esempio di "fisicità" dell'elaborazione digitale accessibile al "pubblico" è rinvenibile-nelle stampanti 3D. In effetti, il prodotto fisico dell'elaborazione dei dati immessi nella stampante pone problemi nuovi: in particolare, per la prima volta la commistione tra elaborazione dei dati e oggetti potenzialmente atti a ledere fisicamente le persone si pone in modo evidente in ambienti non protetti. Sorgono così problemi nuovi nella regolamentazione della responsabilità da prodotto, che per certi versi richiamano parte delle questioni che si intendono affrontare in questo lavoro[12]; non a caso, le stampanti più note sono denominate *Maker-bot* (contrazione di robot) e la *start-up* di Chris Anderson si chiama *3D Robotics*.

Catalogare e definire: il rischio della legge del cavallo

Dunque, la caratteristica più pregnante del robot – in grado di porre questioni realmente inedite anche rispetto al mondo digitale con cui il giurista si confronta da oltre vent'anni – parrebbe essere quella incentrata sulla interazione fisica con la realtà materiale: attraverso acquisizione ed elaborazione di dati, cioè, la macchina produce una modificazione del mondo circostante senza mediazione, sebbene con diversi gradi di autonomia. **L'output, unitamente al grado di autonomia** – inteso come percentuale di mediazione umana rispetto al risultato (dalla stampante 3D all'intelligenza artificiale del badante robotico del futuro) – **potrebbe rappresentare, teoricamente, un buon parametro per saziare velleità classificatorie**. Ma a che pro?

Il rischio è quello di inventarsi una "legge del cavallo". Fu il giudice Frank Easterbrook che, aprendo i lavori di un convegno sulla *cyberlaw* nel lontano 1996, mise in guardia dagli eccessi di classificazione con l'esempio della "legge del cavallo". Molti casi giuridici interessano questi nobili animali: questioni contrattuali nel loro commercio, problemi legati alle cure veterinarie dei costosi purosangue, ed ovviamente i danni cagionati a cose e persone dalle loro bizzarrie. Ma, ammonisce Easterbrook: *"[a]ny effort to collect these strands into a course on 'The Law of the Horse' is doomed to be shallow and to miss unifying principles"*[13].

Probabilmente qualche ragione Easterbrook l'aveva. Pertanto, un'astratta classificazione dei robot – anche solo nella sotto-categoria dei robot di servizio –, con connessa normativa di riferimento, rischierebbe di rivelarsi un esercizio inutile: **per quanto si possano individuare parametri oggettivi, infatti, la malleabilità logica delle tecnologie digitali, la continua evoluzione delle stesse, e la multi-funzionalità potenziale di ciascuna macchina renderebbe vano ogni tentativo di classificazione**.

Il fatto che un drone dedicato alla videosorveglianza di un parco si sposti volando genera evidentemente problematiche diverse rispetto ad un robot che si muova con le stesse finalità lungo i sentieri del medesimo parco, ma questo non esclude che molte criticità di sicurezza o di privacy siano per le due macchine concettualmente simili.

---

[12] Cfr. N. Freeman Engstrom, *3-D Printing and Product Liability: Identifying the Obstacles*, 162 U. PENN L. REV. ONLINE 35 -2013

[13] F. H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 -1996.

Anche il grado di interazione tra macchina e uomo – che per i robot industriali è definito *"grado di collaboratività nell'esecuzione dei compiti"* – è evidentemente un parametro potenzialmente fondamentale, ma una classificazione basata sul grado di autonomia dell'output della macchina, qualora fosse realizzabile, non potrebbe generare categorie omogenee utili, se non a meri fini speculativi.

Nessuna definizione, nessun vincolo

Pensare dunque di comporre astratte categorie di robot sulla base di questa o quella caratteristica della macchina o dell'uso cui è potenzialmente destinata, oppure alle sue modalità di esecuzione, o ancora al grado di autonomia nell'agire, sarebbe, allo stato, verosimilmente inutile. Se poi la finalità di un tale sforzo definitorio celasse un'esigenza di regolamentazione astratta e generalizzata – per categorie, appunto –, allora l'inutilità si tradurrebbe in errore. La straordinaria innovatività generata da Internet è stata certamente agevolata dalla grande libertà di cui per molto tempo esso ha goduto, per distrazione dei legislatori e per contingenti difficoltà regolatorie. La storia dei robot ovviamente sarà diversa, e la fisicità di queste macchine impone evidentemente un approccio prudenziale; ma pensare oggi di trattare ciò che verrà attraverso categorie e definizioni preconcette, basate su prototipi o su ipotesi astratte, rischia di tradursi – come appena detto – in un *modus operandi* inattendibile e, in ultima istanza, inutile. **Sarebbe da preferirsi, invece, un approccio pragmatico, caso per caso, senza che i giuristi – né, soprattutto, i produttori e gli "inventori" – si lascino imbrigliare da categorie e vincoli, anche mentali, che difficilmente possono appartenere ad un mondo che ancora non esiste.**

Un approccio pragmatico

Se, stando a quanto detto, un qualsiasi tentativo definitorio generico ed astratto pare soddisfare unicamente rischiose e poco utili velleità accademiche, ciò che si ritiene fondamentale è un'analisi puntuale dei singoli progetti in corso di sviluppo. La complessa architettura che ne può risultare (come, ad esempio, nel caso di piattaforme aperte di gestione di servizi svolti da terze parti, a fronte di una interazione diretta con fruitori non professionali) impone, infatti, un approccio quanto più concreto possibile. Sotto questo profilo, in aggiunta alla descrizione puntuale delle casistiche-tipo di cui alla Sezione 2, le normative tecniche "standard" in materia prevalentemente di robotica industriale (ci si riferisce in particolare alle norme ISO e ANSI/RIA) possono offrire spunti significativi per una concreta e utile valutazione dei rischi insiti nella "macchina robot", a qualunque categoria essa appartenga.

4 I PROFILI GIURIDICI E LA NORMATIVA DI RIFERIMENTO NELLA SPERIMENTAZIONE E NELL'IMPIEGO DELLA ROBOTICA DI SERVIZIO

Conformemente all'impostazione metodologica appena descritta, nella presente sezione verranno analizzati i principali aspetti giuridici rilevanti per gli scenari individuati all'interno della Sezione 2. Laddove possibile, si cercheranno di unire all'analisi di tali profili anche alcune prime raccomandazioni di policy, facendo esplicito riferimento alla normativa di volta in volta rilevante.

Ogni profilo giuridico verrà esaminato secondo uno schema espositivo comune: aprirà l'analisi un'introduzione alla materia giuridica in relazione alle casistiche-tipo dei robot di servizio (*Introduzione e principi generali*); verranno poi considerate le problematiche giuridiche di stretta rilevanza (*Problematiche giuridiche rilevanti*), nonché la normativa di riferimento conseguentemente applicabile (*Normativa di riferimento applicabile*); infine, si pondererà la possibile ripartizione delle responsabilità tra i diversi attori coinvolti nella progettazione e realizzazione dei robot (*Allocazione delle responsabilità tra i vari soggetti coinvolti*).

Verranno esaminati i seguenti profili giuridici: responsabilità civile; responsabilità penale; privacy e trattamento dei dati; *digital forensics* e *cyber security*; diritti su beni immateriali.

In chiusura della presente Sezione 4, infine, si esaminerà l'impianto normativo del Regolamento che l'Ente Nazionale per l'Aviazione Civile (ENAC) ha emanato – il 16 dicembre 2013 – per l'impiego di mezzi aerei a pilotaggio remoto. Il 16 luglio 2015, il Regolamento è stato aggiornato alla sua seconda edizione.

4.1 Responsabilità civile

(a cura di Massimo Travostino)

Introduzione e principi generali

Il tema della responsabilità – e della sua gestione – nell'ambito degli scenari di robotica di servizio è cruciale nell'ottica

della implementazione concreta dei singoli progetti e della loro sostenibilità economica in vista di sviluppi orientati al mercato. **Un'analisi quanto più possibile accurata e lungimirante delle relazioni tra i vari soggetti e dei rispettivi profili di rischio è determinante per individuare gli accorgimenti e le cautele che consentano di gestire opportunamente l'allocazione del rischio nell'ambito di progetti che prevedano l'impiego di peculiari dispositivi robotici**.

L'analisi del tema è resa particolarmente complessa dal fatto che i dispositivi in esame – nonché le relative attività ad essi connesse – siano innovativi, frutto del lavoro congiunto e della collaborazione di numerosi soggetti; dal fatto che essi presentino aspetti di incerta qualificazione; nonché dal fatto che siano sottoposti ad una disciplina regolatoria di natura pubblicistica, anche in considerazione di possibili utilizzi di tali applicazioni suscettibili di interferire con l'uso di spazi o luoghi pubblici (spazio aereo; terreni demaniali) o, addirittura, di utilizzi di natura militare (si pensi agli apparecchi ed alle tecnologie *dual use*).

Il tema della responsabilità in ambito civile rileva sia sotto il profilo della responsabilità contrattuale sia sotto quello della responsabilità extracontrattuale (c.d. "responsabilità civile" in senso stretto); nella presente Sezione verrà affrontato questo secondo aspetto.

La progettazione, la costruzione, la commercializzazione e l'utilizzo dei robot, nonché la fornitura di servizi attraverso i robot, sono suscettibili di costituire fonte di responsabilità civile: la costruzione, la commercializzazione e l'uso di tali dispositivi rilevano ai fini della responsabilità civile sia **sul piano del fatto illecito in senso stretto** (ex art. 2043 c.c.), sia sul piano **della c.d. responsabilità "indiretta"** (di padroni e committenti, art. 2049, su cui *infra*, *Normativa di riferimento applicabile*) **e della responsabilità oggettiva o quasi oggettiva** (c.d. danno imputabile a cose, su cui *infra*, *Normativa di riferimento applicabile*).

L'aspetto che qui più rileva per inquadrare le differenti modalità con le quali può concretizzarsi la responsabilità degli agenti è quello delle **diverse forme di imputabilità:** accanto alla tradizionale **imputabilità "soggettiva" per dolo o colpa**, esistono infatti una serie di **criteri di imputabilità cosiddetta "speciale"**. Questi ultimi prescindono (in tutto o in parte) dall'esistenza di uno stato soggettivo rilevante in capo all'agente, per fondare l'imputabilità su elementi diversi (si parla, in questi casi, di responsabilità c.d. oggettiva, quasi-oggettiva o indiretta): la relazione con l'oggetto/soggetto causatore del danno; l'assunzione del rischio; la valutazione (in astratto e a priori) del rapporto socio-economico tra danneggiante e danneggiato, e la conseguente imputazione del danno al soggetto che (in astratto e a priori) appare maggiormente in grado di sostenerlo economicamente.

Sarà soprattutto in questa seconda categoria di criteri di imputazione che troveranno soluzione i casi nei quali l'imprevedibilità delle azioni dei robot (o, meglio, l'incapacità di prevederle da parte di chi li controlla) induca a teorizzare una sorta di capacità di autodeterminazione delle macchine ed a preconizzare una "responsabilità del robot", la quale, però, non può trovare (almeno ad oggi) collocazione nel nostro ordinamento.

Sebbene scontato, è altresì doveroso ricordare che l'analisi è condotta sulla base della legislazione italiana; normative nazionali diverse non sono prese in considerazione.

Problematiche giuridiche rilevanti

Le tre specifiche macro-categorie di utilizzo dei robot prese in considerazione (telepresenza, robot courier, e droni-multicotteri operanti in spazi urbani) sono suscettibili di configurare le più svariate forme e modalità in cui le ipotesi di responsabilità civile possono manifestarsi. Peraltro, va rilevato che ciascuna di tali categorie di applicazione può presentare varianti costruttive, di equipaggiamento e operative pressoché illimitate; di conseguenza, le problematiche giuridiche potenzialmente rilevanti coprono pressoché tutto l'ambito della responsabilità civile.

Provvediamo, quindi, a tentare di dettagliare gli attori suscettibili di essere coinvolti nei progetti presi in esame, nonché gli scenari di maggiore interesse.

I soggetti che partecipano allo sviluppo, all'utilizzo ed alla commercializzazione dei robot e dei relativi servizi, e che in qualche modo possono essere interessati a – o interagire con – il loro utilizzo, possono essere così identificati:

a) **soggetti che a vario titolo contribuiscono alla realizzazione del prodotto e alla prestazione dei servizi offerti dai robot**, fornendo singole componenti hardware, software ovvero servizi propedeutici o funzionali alla produzione o all'utilizzazione dei robot. Tale categoria include i costruttori di componenti meccaniche e componenti elettriche, i fornitori di componenti hardware e software, i progettisti del robot o di alcune sue parti, i fornitori di servizi cloud e di piattaforme di sviluppo, i fornitori di apparati ospitati a bordo dei robot (c.d. *payload*, come ad esempio apparecchiature fotografiche), i soggetti che addestrano, manutengono o pilotano i robot;

b) **soggetti che commercializzano i robot e i relativi servizi** nei confronti dei clienti finali: tali soggetti possono

svolgere anche parte delle attività di cui al punto a);

c) **clienti finali**, che possono essere sia imprese che consumatori: acquirenti dei robot o dei relativi servizi;

d) **autorità pubbliche di controllo e regolazione del settore**;

e) **società che forniscono servizi di assicurazione** contro i rischi derivanti dall'uso dei robot;

f) **terzi estranei alle categorie sopraelencate**, che possono essere danneggiati od ottenere benefici dall'uso dei robot, nonostante non siano entrati in relazione diretta con il fornitore di servizi di robotica.

I principali scenari nell'ambito dei quali si manifestano rischi di responsabilità civile in capo agli agenti coinvolti nella produzione, commercializzazione e utilizzo dei robot possono essere riassunti in cinque categorie:

1) **progettazione e produzione delle macchine**;
2) **realizzazione e messa a disposizione di beni e servizi funzionali alla progettazione e produzione delle macchine** (ad es., fornitori dei componenti del robot; fornitori di piattaforme di servizio da utilizzare per la progettazione);
3) **commercializzazione dei robot**;
4) **prestazione di servizi attraverso i robot**;
5) **prestazione di servizi di deposito, conservazione e manutenzione dei robot**.

Per ciascuno di tali scenari potranno rilevare, di volta in volta, svariate ipotesi di responsabilità extracontrattuale, che proveremo ad elencare nel successivo paragrafo. Il tratto comune agli scenari sopra individuati è però costituito dal fatto che **la materia si presta a suggestivi scenari di imputazione della responsabilità ai *robot* e comunque alle macchine, in considerazione di una loro presunta capacità di autodeterminazione**, così come a considerazioni *de jure condendo* sul medesimo argomento. È il tema legato, più in generale, ai principi del rapporto di causalità, dell'imputabilità del fatto dannoso (art. 2046 c.c.) e dell'elemento soggettivo (art. 2043 c.c.) quali presupposti, rispettivamente, dell'esistenza stessa della responsabilità civile e della risarcibilità dei relativi danni, ai quali fanno da contrappunto il principio della causalità omissiva, le disposizioni che regolano la responsabilità di padroni e committenti e la responsabilità oggettiva. Sul punto, è bene evidenziare che **il nostro ordinamento individua quali possibili centri di imputazione della responsabilità civile unicamente i soggetti che ad oggi sono ritenuti tali dall'ordinamento italiano, ovvero le persone fisiche** (artt. 1 e seguenti c.c.) **e le persone giuridiche** (artt. 11 e seguenti c.c.). In altre parole: quell'interattività, adattatività ed autonomia da cui discende l'imprevedibilità delle azioni dei robot, "*sia nei confronti dei programmatori e costruttori di tali agenti artificiali sia dei loro stessi proprietari*" (di cui si è detto alla Sezione 1) non sono suscettibili – *legibus sic stantibus* – di fondare una "responsabilità delle macchine" in base al nostro ordinamento, per la semplice ragione che tali entità non rientrano tra i possibili centri di imputazione di responsabilità previsti dalla legge. **Pertanto, le conseguenze giuridicamente rilevanti che derivano dall'imprevedibilità dell'azione dei robot saranno sussumibili nella categoria del caso fortuito/forza maggiore, oppure costituiranno fonte di responsabilità risarcitoria in capo a quel soggetto o a quei soggetti cui potranno venire ricondotte sulla base delle regole di imputabilità** (soggettiva o oggettiva) previste dall'ordinamento, e su cui si dirà sotto.

Normativa di riferimento applicabile

In primo luogo, ai fini della responsabilità civile, le principali disposizioni rilevanti sono quelle della disciplina generale in materia di **responsabilità extracontrattuale di cui agli articoli 2043 e seguenti del codice civile** (c.d. clausola generale di responsabilità civile, o danno ingiusto atipico). Specifica applicazione troveranno, in particolare, le norme in materia di **responsabilità per esercizio di attività pericolose (art. 2050)**, che possono, ad esempio, essere applicabili ai robot sia in considerazione delle applicazioni utilizzate che dell'utilizzo che ne viene fatto. È altresì di immediata evidenza la **possibile rilevanza dell'art. 2054 in materia di circolazione dei veicoli senza rotaie, di vizi di costruzione e difetto di manutenzione** e conseguente responsabilità del conducente e del proprietario del veicolo. Lo stesso è a dirsi per **la responsabilità di padroni e committenti per i danni arrecati da fatto illecito commesso dai loro sottoposti (art. 2049)**, che potrebbe essere invocata, ad esempio, nel caso di nolo di droni "a caldo" con operatore.

Spazio importante può trovare, poi, **l'art. 2051 relativo al danno cagionato da cose in custodia**, norma che è probabilmente destinata a neutralizzare i tentativi di de-responsabilizzazione del proprietario-utilizzatore di robot; accanto ad esso, può inoltre essere argomento di interessanti analogie anche quanto disposto **dall'art. 2052 sui danni cagionati da animali**, che sono imputabili al proprietario sia che questi si trovino sotto la sua custodia, sia che siano smarriti o fuggiti, salvo la prova del caso fortuito. Autonomo rilievo assumeranno poi – in tutti i casi di responsabilità civile – le **disposizioni generali in tema di solidarietà**, nel caso di imputabilità del fatto dannoso a più persone, **e di criteri di quantificazione del danno**.

In seconda battuta, risultano evidentemente rilevanti le norme che disciplinano l'attività e la responsabilità dei soggetti che a vario titolo contribuiscono alla realizzazione e all'utilizzo dei robot, norme che possono fondare **specifiche ipotesi di responsabilità extracontrattuale tipica**. Particolarmente rilevante per la materia appare la **responsabilità del venditore per i danni derivanti dai vizi della cosa venduta ex art. 1494 comma 2 c.c.**, che risulta applicabile nei casi di vizi dei singoli componenti del robot, vizi che possono essere contestabili direttamente dall'utente finale nei confronti del fornitore del componente a titolo di responsabilità extracontrattuale. Sono poi certamente applicabili, in numerosi casi, le **norme in materia**

di responsabilità per danno da prodotti difettosi e in materia di sicurezza dei prodotti di cui agli artt. 102 e segg. del D. Lgs. n. 206/2005, codice del consumo, nonché la disciplina normativa e regolamentare applicabile ai robot, ai suoi componenti e ai relativi servizi accessori, quale ad esempio il D. Lgs. n. 17/2010, che attua la direttiva 2006/42 relativa alle macchine. Va poi considerato il **Regolamento ENAC** 16 luglio 2015 (seconda edizione) su mezzi aerei a pilotaggio remoto: tale regolamento disciplina soltanto una particolare categoria di robot (c.d. "droni", ovvero "SAPR" – Sistemi Aeromobili a Pilotaggio Remoto – o anche "UAV", *unmanned aerial vehicles*), in attuazione dell'art. 743 del Codice della Navigazione di cui al R.D. n. 327/1942: il regolamento definisce e classifica i droni, disciplina le condizioni minime per l'operatività e l'utilizzo, il ruolo e la responsabilità dei piloti, l'assicurazione obbligatoria (per ulteriori approfondimenti si rimanda alla Sezione 4.6 – *Regolamento ENAC*). Questi, insieme ad altri elementi, forniscono agli operatori un contesto specifico e dettagliato nell'ambito del quale, per queste specifiche categorie di robot, è possibile calare in concreto e dettagliare la gestione delle responsabilità connesse alla produzione e all'uso dei droni; tale assetto è particolarmente interessante in quanto può essere utilizzato anche per implementare, nei limiti del possibile, soluzioni analoghe per la gestione di altre tipologie di robot. In ultima analisi, le normative tecniche standard (ad es., ISO) applicabili al settore costituiscono parametri di riferimento qualitativi essenziali – specie per quanto riguarda la robotica industriale – che possono essere utilizzati per fondare o, al contrario, scongiurare l'imputazione del fatto dannoso.

Infine, saranno ovviamente rilevanti, in generale, tutte le norme che sanciscono diritti soggettivi (o, più in generale, interessi ritenuti meritevoli di tutela dall'ordinamento) suscettibili di essere violati dall'uso dei robot: diritto di proprietà, diritto alla protezione dei dati personali, e così via.

Allocazione delle responsabilità tra i vari soggetti coinvolti

Fatti costitutivi di responsabilità possono derivare:

- **da vizi "tradizionali" del prodotto** (malfunzionamenti dell'hardware, errori del software, errori di progettazione);
- **dalla programmazione e dall'impostazione del funzionamento del robot**, programmazione ed impostazione che possono essere di carattere generale (es. errate coordinate di riferimento o errata taratura della macchina) o speciale (errate impostazioni della specifica missione);
- **dal pilotaggio**;
- **dallo specifico contesto operativo dei robot** (ambiente di funzionamento; condizioni meteorologiche, e così via; a tal fine, rilevano in particolare i luoghi dove i robot operano e dove vengono prestati i relativi servizi: spazi chiusi privati, luoghi aperti al pubblico, spazi pubblici);
- **da fatti sui quali il soggetto imputabile non ha alcun controllo** (in caso di responsabilità oggettiva o quasi oggettiva derivante, ad es., da cose in custodia, esercizio di attività pericolose, responsabilità di padroni e committenti).

Per gli operatori del settore, il punto critico è – da un lato – la preventiva identificazione del soggetto sul quale possono ricadere le conseguenze della responsabilità civile derivante dai robot; dall'altro, gli strumenti e le modalità con cui la medesima responsabilità – o le sue conseguenze – possono essere allocate su soggetti diversi, attraverso clausole di esenzione di responsabilità, meccanismi di rivalsa, responsabilità solidale.

Si possono quindi tentare di individuare **alcuni dei principali strumenti con i quali il relativo rischio può essere affrontato e gestito**.

L'aspetto fondamentale della riflessione sul punto si fonda sul fatto che **è generalmente esclusa, nel nostro ordinamento, la possibilità di limitare preventivamente la responsabilità extracontrattuale con apposite clausole di esonero**, al contrario di quello che invece può avvenire in ambito contrattuale. Pertanto, **il primo modo con il quale può essere gestito il rischio derivante dalla progettazione, costruzione e utilizzo dei robot è quello di "contrattualizzare" per quanto più possibile i rapporti con i soggetti che a vario titolo si interfacciano con l'agente**. La stipula di contratti adeguati – che gestiscano in modo appropriato e per quanto più possibile dettagliato l'allocazione del rischio e delle relative responsabilità – è un aspetto cruciale per l'allocazione del rischio: ciò deve avvenire non soltanto sul piano strettamente giuridico, attraverso la previsione di apposite (e valide) clausole, ma anche sul piano tecnico, attraverso un'approfondita e adeguata analisi preventiva delle caratteristiche tecniche, delle prestazioni, dei livelli di servizio delle macchine, e di tutto quanto sia suscettibile di essere oggetto di regolamentazione e disciplina, che dovrà essere allegato e divenire parte integrante del contratto. Sullo stesso piano si pone l'acquisizione di documenti a comprova di elevati standard qualitativi di prodotto e di processo. La stipula di un

adeguato contratto è lo strumento attraverso il quale può essere gestita la stragrande maggioranza dei rapporti tra i diversi attori che partecipano e si relazionano a vario titolo con il robot: in questo modo, si riduce l'area dell'imprevisto e del conseguente rischio.

Nei casi in cui non possa essere concluso un contratto (si pensi, ad esempio, all'interazione della macchina con terzi casualmente presenti nel raggio di azione, o all'uso di robot da parte di enti pubblici per offrire servizi alla cittadinanza), **è comunque consigliabile prevedere e cercare di creare – per quanto possibile – una relazione tra l'attore ed il (possibile) soggetto destinatario delle interferenze causate dalla macchina:** ad esempio, mediante annunci con appositi cartelli posti nell'area di azione del robot, controllo degli accessi all'area, tracciatura del raggio di azione del robot. Tali iniziative, quand'anche non consentano di escludere direttamente la responsabilità del soggetto agente, potranno valere quale limitazione "indiretta" di responsabilità, in quanto costituiranno elementi a favore dell'agente nella valutazione del suo grado di diligenza, nel caso in cui questi dovesse, ad esempio, provare di avere adottato tutte le misure idonee ad evitare il danno, al fine di evitare l'imputazione per esercizio di attività pericolose ai sensi dell'art. 2050 c.c.

Il tema dell'instaurazione di una relazione preventiva con il possibile soggetto passivo del danno va inoltre letto in un'ottica di concertazione tra i diversi soggetti agenti: la strada verso un'efficace gestione del rischio passa anche attraverso l'individuazione di azioni congiunte tra i diversi attori, quali, ad es., il fornitore di servizi robotici e il proprio cliente. Si faccia il caso dell'organizzatore dell'evento sportivo che concluda un contratto di nolo "a caldo" (con operatore) di un drone destinato a riprendere la manifestazione sportiva: fornitore dei servizi robotici e organizzatore della manifestazione provvederanno a valutare preventivamente i possibili rischi di tale attività nei confronti dei partecipanti e del pubblico e, conseguentemente, a porre in essere le misure necessarie a scongiurare – o, comunque, limitare – i relativi rischi (zone vietate all'accesso del pubblico, condizioni generali di acquisto del titolo di ingresso con ulteriori sintetici richiami sui biglietti, posizionamento di adeguata cartellonistica), misure che saranno utili a entrambi. In questo modo, il fornitore dei servizi robotici, pur non entrando in relazione contrattuale diretta con il terzo (atleta o spettatore), si vale del rapporto contrattuale che il proprio cliente ha con tali soggetti per limitare a sua volta il proprio rischio.

In una diversa prospettiva, **un altro punto cruciale per la gestione della responsabilità è la tracciabilità delle operazioni compiute attraverso i robot**. Registrazioni di sistema (*log*) dei parametri rilevanti di funzionamento del robot, riprese video dell'attività svolta (con videocamere a bordo ovvero esterne), relazioni scritte sulle missioni compiute, rapporti relativi alla situazione ambientale in cui il robot opera (ad es., condizioni meteo), sono tutti elementi che potranno essere utilizzati per dimostrare, ad esempio, che lo scontro del drone con i tralicci elettrici è stato causato da un calo improvviso della batteria, da una manovra errata, o ancora da un colpo di vento improvviso (su questo aspetto si rimanda anche alla Sezione 4.4 – *Digital forensics e cyber security*).

Quale strumento di gestione del rischio vi è, infine, la stipula di apposite assicurazioni contro la responsabilità civile: sia quelle eventualmente imposte dalla legge, sia quelle che l'agente reputi opportuno adottare a propria tutela. Sul punto, è peraltro auspicabile un rapido sviluppo sul mercato di proposte diversificate, che con il tempo potrebbero consolidarsi in una serie di polizze "standard".

4.2 Responsabilità penale

(a cura di Monica A. Senor)

Introduzione e principi generali

Come delineato nelle Sezioni 1 e 2 della ricerca, le caratteristiche essenziali dei robot di servizio – interattività, autonomia e adattatività –, unitamente alla loro ineludibile interazione con il mondo reale, aprono **scenari nuovi anche in relazione ai profili di responsabilità penale**.

Si pensi, *in primis*, al principio cardine – espresso all'art. 27 della Costituzione Italiana – secondo cui la responsabilità penale è personale. Tale articolo sancisce un principio inderogabile del nostro ordinamento giuridico (salvo le ipotesi di responsabilità amministrativa degli enti di cui alla legge 231/2000), in base al quale la responsabilità per un fatto di reato può essere riconosciuta esclusivamente nei confronti di una persona fisica.

Quid iuris nell'ipotesi in cui un fatto di reato (ad es., la lesione ad un terzo provocata dalla collisione con un agente artificiale) venga commesso da un robot che ha agito elaborando in "piena" autonomia gli input esterni che ha ricevuto?

Ed ancora, considerato che ogni reato è costituito da un elemento oggettivo (fatto materiale) e da un elemento soggettivo (rappresentato da coscienza e volontà di porre in essere un'azione o un'omissione prevista dalla legge come reato), come può essere configurato in capo ad un robot il c.d. *animus nocendi*?

Delle tre caratteristiche dei robot indicate nella Sezione 1, è sufficiente prendere in considerazione anche solo la prima fase operativa – l'interattività, ovverosia quella in cui l'agente artificiale risponde agli stimoli esterni dell'ambiente attraverso il mutamento degli stati interni o dei valori delle sue proprietà – per rilevare come droni e piccoli robot di servizio possano, nella inevitabile interazione tra la loro attività e la realtà fisica del mondo che li circonda (interazione che, peraltro, rappresenta la ragione stessa della loro creazione), potenzialmente causare fatti di rilevanza penale.

Problematiche giuridiche rilevanti

Sulla scorta di quanto illustrato nella Sezione 2 con riferimento alle casistiche-tipo prese in esame (telepresenza mediante robot, robot courier, e droni-multicotteri operanti in contesti urbani), è opportuno ora delineare le principali questioni di rilevanza penalistica connesse all'attività posta in essere dai robot di servizio.

Come emerge pacificamente dai recenti studi accademici[14], dai comunicati ufficiali dell'ENAC[15] e dai numerosi articoli di stampa in materia[16], la preoccupazione maggiore degli esperti e, di conseguenza, dell'opinione pubblica attiene al rischio che gli agenti artificiali (sia robot terrestri che droni) provochino danni nel mondo fisico in cui si trovano ad operare. Questo sarà dunque il primo profilo giuridico da analizzare.

Il rischio di cagionare danni a cose e persone va ovviamente declinato diversamente a seconda della capacità di movimento dei robot: in questo senso, è del tutto evidente che un robot che svolga un'attività di telepresenza in un locale chiuso con limitata capacità di movimento è potenzialmente meno pericoloso – nei confronti del mondo fisico che lo circonda – di un drone che effettui attività di sorveglianza su di un centro abitato (non a caso, anche il regolamento ENAC distingue tra APR adibiti al sorvolo di aree critiche e non).

Da un punto di vista penalistico, è doveroso precisare che **l'eventuale danneggiamento di beni materiali da parte di un robot non integra alcun reato**, in quanto il delitto di danneggiamento di cui all'art. 635 del codice penale punisce la condotta di chi dolosamente "*distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui*": in altri termini, non è previsto nel nostro ordinamento un reato di danneggiamento colposo, ipotesi che ricorrerebbe nel caso di danni a cose arrecati colposamente per mezzo di un robot.

Diversa la situazione nell'ipotesi di danni cagionati a persone fisiche, condotta che viene qualificata come reato di lesioni personali, e che è punita sia a titolo di dolo (art. 582 c.p.) che a titolo di colpa (art. 590 c.p.).

L'allocazione della responsabilità penale per i danni fisici arrecati dall'interazione di un agente artificiale con uno o più esseri umani che entrano nell'alveo delle sue dinamiche motorie ed informatiche sarà determinata dall'analisi del singolo fatto concreto: in altri termini, a seconda della causa dell'azione del robot (volendo escludere in questa sede – come sopra detto – una capacità del robot di agire in piena autonomia), la responsabilità potrebbe confluire in capo al produttore, al gestore della piattaforma operativa, fino al pilota nel caso di caduta a terra improvvisa di un drone.

Un secondo profilo giuridico di immediata percezione riguarda la **problematica attinente al trattamento di dati personali.**

Un'attenta e approfondita disamina della problematica è oggetto di una specifica Sezione della ricerca (Sezione 4.3 – *Privacy e trattamento dati*), ma in questa sede pare comunque opportuno analizzare la materia, al fine di individuare i presupposti, di fatto e di diritto, che potrebbero condurre all'integrazione del reato di cui all'art. 167 del D. Lgs. 196/2003, codice in materia di protezione dei dati personali (di seguito, codice privacy).

In particolare, verranno esaminati i presupposti che determinano l'illiceità di un trattamento di dati personali, partendo dalla definizione stessa di "dato personale", da intendersi come qualunque informazione relativa ad una persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione (art. 4, comma 1, lett. b) codice privacy).

Sotto questo profilo, è di immediata evidenza che **un robot courier** che non memorizzi immagini, ma solo le caratteristiche fisiche dell'ambiente in cui opera, **non effettua alcun trattamento di dati personali in relazione alla captazione, alla trasmissione al server di controllo ed alla conservazione dei dati ambientali rilevati** nello spazio, chiuso od aperto, in cui opera; lo stesso robot, **per contro, tratterà i dati personali delle persone che si mettono direttamente in relazione con lui per usufruire del servizio** (ad es., il visitatore da accompagnare in uno specifico punto vendita del centro commerciale). Anche per i **robot di telepresenza** si pongono **problemi di trattamento di dati personali**, atteso che il robot verosimilmente

---

[14] Cfr. l'articolo di R. Calo dell'University of Washington, *Robotics and the new Cyberlaw*: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2402972.

[15] Posizione confermata *apertis verbis* dall'ing. Delise, program manager APR, Direzione Regolazione Navigabilità dell'ENAC, nel corso del suo intervento al workshop – svoltosi al Politecnico di Torino il 7 luglio 2014 – "*Droni: prospettive di ricerca e scenari applicativi*": http://www.politocomunica.polito.it/press_room/news/%28idnews%29/5457.

[16] Si veda, ad esempio: http://www.washingtonpost.com/sf/investigative/2014/06/20/when-drones-fall-from-the-sky/.

videoriprenderà persone che frequentino il suo spazio di azione.

In entrambi i casi, tuttavia, trattandosi di attività prestabilite e ben delineate nei presupposti operativi, **sarà sufficiente redigere una chiara *privacy policy* per dirimere ogni possibile controversia**.

Diverso il caso dei droni, per i quali lo stesso regolamento ENAC (cfr. art. 34) prevede la necessità di una specifica analisi da riportare nella documentazione sottoposta all'Ente, ai fini del rilascio dell'autorizzazione di volo, laddove le operazioni svolte da un APR possano comportare un trattamento di dati personali (ipotesi verosimilmente piuttosto frequente nell'ipotesi di sorvolo di centri abitati), **e stabilisce che debba in ogni caso essere rispettato il principio di necessità di cui all'art. 3 del codice privacy**, secondo cui i sistemi informativi ed i programmi informatici debbono essere configurati in modo da ridurre al minimo l'utilizzo di dati personali e dati identificativi.

Pare doveroso ricordare che l'art. 5 del codice privacy prevede un'**esclusione di responsabilità, qualora il trattamento di dati personali venga effettuato a fini meramente personali** (c.d. *household exemption*), salvo le ipotesi di comunicazione sistematica o diffusione dei dati stessi e salvo, in ogni caso, il rispetto delle misure minime di sicurezza (art. 31 codice privacy) e la responsabilità civile per danni a terzi (art. 15 codice privacy). Ciò significa che – nell'ipotesi in cui un drone venga utilizzato da un privato per operazioni strettamente personali – non troverà applicazione il codice privacy nella parte in cui prevede la fattispecie criminosa di trattamento illecito di dati personali.

Pur essendo poco verosimile una circostanza del genere allo stato dei progetti, l'aspetto non è da sottovalutarsi in relazione alla potenziale implementazione a fini commerciali di piattaforme di *cloud robotics*, in relazione alle quali gli utenti finali del robot di servizio saranno con grande probabilità soggetti privati.

Da ultimo, ed esclusivamente in relazione all'attività svolta dai droni, viene in rilievo la questione relativa alla **possibile captazione di notizie o immagini attinenti alla vita privata**[17], che potrebbe integrare il reato di cui all'art. 615 bis c.p. (interferenze illecite nella vita privata). Con riferimento a questo specifico delitto, vedremo – nel prossimo paragrafo – come l'elaborazione giurisprudenziale del concetto di domicilio richiamato dalla norma incriminatrice determini una portata applicativa particolarmente estesa del reato *de quo*.

Normativa di riferimento applicabile

Il reato di lesioni personali

Come anticipato, **il codice penale punisce, sia a titolo di dolo che di colpa, la condotta di chi cagiona ad altri una lesione personale dalla quale deriva una malattia nel corpo o nella mente**. Per pacifica interpretazione giurisprudenziale, per malattia si intende qualunque alterazione, anatomica o funzionale, dell'organismo (fisico o psichico).

Il bene giuridico protetto dalla norma incriminatrice è quindi costituito dall'incolumità della persona fisica.

La colpa, elemento soggettivo del reato che ci interessa, è generica se l'evento lesivo si verifica a causa di negligenza, imprudenza o imperizia; specifica se l'autore del reato non ha osservato specifiche disposizioni di legge, regolamenti, ordini o discipline.

Come visto, nell'ambito della presente ricerca si può facilmente ipotizzare che l'interazione dei robot con il mondo reale, che comporta necessariamente anche un'interazione diretta tra l'agente artificiale robot e gli esseri umani che entrano nell'alveo delle sue dinamiche motorie ed informatiche, potrebbe potenzialmente cagionare lesioni agli esseri umani. Trattandosi di lesioni cagionate da una macchina (come, ad es., una lesione da sinistro stradale o un infortunio sul lavoro), **risponderà penalmente della condotta criminosa chi sia responsabile del corretto assemblaggio, funzionamento ed utilizzo della macchina stessa**.

Allo stato attuale della normativa nazionale, non esistono previsioni di legge che disciplinino *ad hoc* l'attività dei robot di servizio terrestri: non è dunque ipotizzabile una colpa specifica correlata alla violazione di una specifica disciplina normativa. Tuttavia, ciò non significa che, a seconda dei casi concreti, non possano trovare applicazione altre previsioni legislative che regolamentino, più in generale, la costruzione ed il funzionamento delle macchine (ad es., la direttiva macchine).

Diversa la situazione in relazione ai danni che potrebbero essere cagionati dai droni: l'art. 1, comma 3 del Regolamento ENAC, infatti, prevede che "*[i] mezzi aerei a pilotaggio remoto impiegati o destinati all'impiego in operazioni specializzate o in attività scientifiche, sperimentazione e ricerca, costituiscono i* Sistemi Aeromobili a Pilotaggio Remoto *(SAPR) e ad essi si applicano le previsioni del Codice della Navigazione secondo quanto previsto dal presente Regolamento*". Questo significa che, per quanto riguarda i droni, si possono sin d'ora ipotizzare **profili di responsabilità penale da colpa specifica, ovverosia per violazione delle regole sulla navigazione aerea**, così come previste dal Titolo II della Parte II, Libro I del Codice della Navigazione, come modificato dal D. Lgs. 9 maggio 2005, n. 96 recante "Revisione della parte aeronautica del Codice della navigazione, a norma dell'articolo 2 della L. 9 novembre 2004, n. 265".

[17] A titolo esemplificativo della fattispecie in oggetto, si consideri la vicenda descritta qui: http://seattle.cbslocal.com/2014/06/23/seattle-woman-sees-drone-peeping-into-her-apartment-window/.

Sempre sotto il profilo soggettivo, ai sensi dell'art. 43, comma 3 del codice penale, potrebbe integrare un elemento di colpa specifica la mancata osservanza anche delle disposizioni previste dal Regolamento ENAC, che, pur non essendo una fonte normativa di rango primario, è sicuramente speciale rispetto al codice della navigazione.

Il reato di trattamento illecito di dati personali

L'**art.167 del codice privacy** stabilisce che: "*Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.*

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni".

Al fine di delineare i presupposti previsti dal codice privacy per il perfezionamento del reato di cui all'art. 167 del codice privacy, occorre necessariamente partire dalla definizione di trattamento e di dato personale. Ai sensi dell'art. 4, comma 1, lett. a) del codice privacy, sono considerati "trattamento" qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati; ai sensi dell'art. 4, comma 1, lett. b), **è considerata "dato personale" qualunque informazione relativa ad una persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione**.

Se il dato personale è un'informazione, va da sé che i robot, nell'ambito della fisiologica acquisizione del flusso di informazioni dall'ambiente esterno da parte del sistema operativo, ben possono raccogliere anche informazioni di carattere personale. In prima battuta, il pensiero va al dato immagine o al dato audio, ma una riflessione più approfondita porta a rammentare che il codice privacy (nonché la proposta europea di Regolamento generale in materia di protezione dei dati personali) tutela anche i dati c.d. biometrici, ovverosia quei dati informatizzati di misurazione del corpo e dei comportamenti umani che costituiscono i moderni sistemi di autenticazione e riconoscimento (si pensi, ad es., all'eventuale memorizzazione di un'impronta digitale da parte di un *touchscreen*, o alla registrazione di una camminata umana nell'ipotesi in cui il robot sia demandato ad accompagnare un utente dalla posizione A alla posizione B).

Come si possono allocare eventuali responsabilità in caso di trattamento illecito di dati personali da parte del robot di servizio? E cosa si intende per trattamento illecito?

L'art. 167 codice privacy non descrive, come invece in genere accade nella formulazione dei precetti penali, una specifica, dettagliata e tassativa condotta, ma richiama altre norme del codice privacy che connotano, in caso di violazione, la condotta, conferendole meritevolezza di pena: queste norme sono spesso lunghissime previsioni che rimandano ad altre norme, i cui contenuti, a volte, sono demandati a provvedimenti emanati o emanandi dell'Autorità Garante, in casi da determinarsi a seguito di particolari situazioni da definire.

Il bene giuridico protetto dalla norma incriminatrice non è dunque la signoria dell'interessato sul singolo dato personale, ma la tutela di un difficile equilibrio tra interessi e diritti contrapposti.

Purtroppo, è noto in dottrina che se l'illecito penale è privo di riferimenti empirici, ovverosia non ha alla base fenomeni delittuosi ben profilati nella realtà sociale, ma unicamente realtà normative o mere astrazioni giuridiche, sarà difficile costruire una precisa fisionomia dell'illecito. Questo è precisamente ciò che avviene con riguardo alla fattispecie del trattamento illecito di dati personali. Infatti, nonostante tale reato sia strutturato come un reato comune (in base alla formulazione letterale dell'art. 167 del codice privacy, che punisce "chiunque" effettui un trattamento illecito), occorre modulare il precetto in base ai concetti di "dato personale" (già definito *supra*), "trattamento" e "titolare", così come definiti nel codice privacy.

Ai sensi dell'art. 4, comma 1, lett. a) del codice privacy, per "trattamento" si intende qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Ai sensi dell'art. 4, comma 1, lett. f) del codice privacy, si definisce "titolare" la persona fisica, la persona giuridica, la

pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Potrà, dunque, essere considerato penalmente responsabile solo il titolare del trattamento, ovverosia colui che, per un interesse proprio, conferisce al dato personale che tratta un significato autonomo e ne dispone un utilizzo per fini diversi ed indipendenti rispetto a quelli delineati dell'interessato. In difetto, chiunque "maneggi" un dato diventerebbe potenzialmente sanzionabile (anche il mero esecutore materiale di un'operazione di trattamento).

In altri termini, essendo il reato costruito come un illecito per modalità di lesione – nel senso che la sanzione non consegue direttamente ad una condotta empirica, bensì alla violazione di alcuni specifici obblighi imposti dalla legge affinché la condotta possa essere considerata lecita –, **la responsabilità penale potrà essere correttamente allocata solo individuando esattamente chi si sia assunto la responsabilità degli adempimenti previsti dal codice privacy** (consenso, rispetto delle prescrizioni, etc.), per quale trattamento e su quali dati personali.

Volendo trasporre gli argomenti sopra esposti alla robotica di servizio, pare evidente che una concreta valutazione dei rischi – *rectius*, dello specifico rischio di integrazione del reato di cui all'art. 167 codice privacy – sarà strettamente vincolata a – e dipendente da – una corretta individuazione del tipo di dati trattati e della loro natura (dati sensibili o non sensibili), ma soprattutto delle persone (costruttore, progettista, proprietario/gestore) che avranno il potere di decidere le finalità e le modalità del trattamento (ad es.: quali dati il robot potrà acquisire; quali dati verranno memorizzati e conservati; dove, come, per quanto tempo e che utilizzo successivo alla prima raccolta ne verrà fatto).

Con riferimento all'attività dei droni, potrebbe assumere rilevanza anche una raccolta di dati personali che concretizzi un'ipotesi di videosorveglianza in luogo pubblico o aperto al pubblico: in tale ipotesi, la legittimità del trattamento di dati personali passerà attraverso il rigoroso rispetto anche degli specifici provvedimenti del Garante privacy in materia.

Il reato di interferenze illecite nella vita privata

L'**art. 615 *bis* del codice penale** prevede che: "*Chiunque, mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni.*

Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo.

I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato".

Il bene giuridico protetto da tale norma sta lentamente evolvendo in virtù dell'interpretazione giurisprudenziale – dalla tutela del domicilio (il reato è inserito nella sezione IV del titolo XII che prevede appunto i reati contro l'inviolabilità del domicilio) **alla tutela della riservatezza** (bene costituzionalmente protetto ai sensi dell'art. 2 della Costituzione Italiana).

Questo slittamento dal domicilio alla riservatezza *determina una più controversa area di applicazione* della norma incriminatrice. Vediamo perché.

L'art. 615 *bis* c.p., nel delineare la condotta perseguita penalmente, fa espresso riferimento a notizie ed immagini attinenti alla vita privata che si svolge nei luoghi indicati dall'art. 614 c.p., il quale a sua volta menziona espressamente *"l'abitazione o altro luogo di privata dimora e le appartenenze di essi"*.

Per fare un esempio concreto, un balcone, un cortile o un giardino sono, in base ad una concezione oggettiva di domicilio mutuata dal diritto civile, pertinenze (appartenenze) di un luogo di privata dimora.

Con una innovativa sentenza a sezioni unite (n. 26795/2006), la **Corte di Cassazione**[18] è però intervenuta sul punto, affermando che **la tutela costituzionale del domicilio è fondata** non sulla natura astratta del luogo, ma **sul rapporto esistente tra un soggetto ed il luogo in cui il soggetto stesso svolge la sua vita privata**, che deve essere un rapporto stabile, tale da giustificare la tutela del luogo stesso anche quando la persona è assente.

A distanza di due anni (sentenza n. 149/2008), anche la **Corte Costituzionale**[19] è intervenuta sul tema, restringendo ulteriormente l'ambito di tutela del domicilio, sancendo che "*...affinché scatti la protezione dell'art. 14 Cost., non basta che un certo comportamento venga tenuto in luoghi di privata dimora; ma occorre, altresì, che esso avvenga in condizioni tali da renderlo tendenzialmente non visibile ai terzi. Per contro, **se l'azione – pur svolgendosi in luoghi di privata dimora – può***

[18] Il testo integrale del dispositivo è disponibile al seguente indirizzo: http://servizi.ceda.unina.it/PHP/spec/spec/Cass_26795_2006.pdf.

[19] Il testo integrale è disponibile al seguente indirizzo: http://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2008&numero=149.

essere liberamente osservata dagli estranei, senza ricorrere a particolari accorgimenti *(paradigmatico il caso di chi si ponga su di un balcone prospiciente la pubblica via),* ***il titolare del domicilio non può evidentemente accampare una pretesa alla riservatezza***".

Come facilmente si può intuire, **il concetto di visibilità ai terzi è assai rilevante in relazione alle potenziali capacità di ripresa visiva dei droni**: *quid iuris*, allora, nell'ipotesi in cui un drone sorvoli il giardino di un'abitazione privata e memorizzi quel che in un determinato momento stanno facendo le persone che vi abitano?

Sarà pacificamente un'interferenza illecita nella vita privata altrui, o dovremo applicare il concetto di "libera visibilità altrui"? E, in questa seconda ipotesi, dovremo applicare al drone i parametri della visibilità umana – per cui, se quel giardino era liberamente osservabile anche da un passante sulla pubblica via, dovrà essere considerato liberamente osservabile anche dal drone? E se applicassimo detti parametri, come potremmo valutare *ex post* con giudizio *ex ante* la visibilità del giardino da parte dell'uomo medio?

Sono **questioni giuridiche aperte**, cui non è possibile, considerata la fase evolutiva della giurisprudenza in materia, dare risposte univoche. L'unico criterio che si può indicare al fine di soddisfare la legittima esigenza di certezza del diritto da parte di chi si appresta ad investire nel settore è che **il nostro ordinamento giuridico, seguendo l'attuale tendenza europea[20], nel prossimo futuro tenderà probabilmente ad una maggiore protezione della riservatezza e dei dati personali dei cittadini**.

Non a caso, in altra recente pronuncia, la Corte di Cassazione[21] ha ravvisato la sussistenza del reato di interferenze illecite nella vita privata nel caso di videoriprese effettuate nell'abitazione altrui anche se chi abitava l'immobile aveva prestato consenso all'uso della telecamera, sancendo il principio secondo cui "*chi frequenta un luogo di privata dimora, anche se si tratta della dimora altrui, fa affidamento, appunto, sul carattere di "privatezza" dello stesso e, dunque, agisce sul presupposto che la condotta che egli tiene in quel luogo sarà percepita solo da coloro che in esso siano stati lecitamente ammessi*".

Un secondo aspetto, non meno problematico, attiene al **concetto di ripresa mediante particolari accorgimenti:** allo stato, ad esempio, si considera accorgimento che non rende lecita la condotta l'utilizzo, a fine di ripresa, di un teleobiettivo, ma si tratta di mera interpretazione giurisprudenziale, perché la norma incriminatrice nulla dice al riguardo. A tal proposito, è verosimile ipotizzare che sorgeranno, nel prossimo futuro, questioni giuridiche strettamente connesse alla rapida evoluzione delle tecniche di ripresa visiva in relazione ad un concetto di "accorgimento" troppo lasso ed indeterminato.

Allocazione delle responsabilità tra i vari soggetti coinvolti

Come visto, la creazione, la gestione e l'utilizzo dei robot di servizio possono potenzialmente coinvolgere numerose persone: dal progettista, al produttore di un singolo componente, all'assemblatore, al gestore della piattaforma cloud che fornisce il servizio per la gestione dell'agente artificiale, fino ad arrivare all'utente finale, o al pilota nel caso dei droni.

Come e per quali profili tali soggetti possono essere chiamati a rispondere penalmente?

Alla domanda non esiste una risposta univoca. **Eventuali profili di responsabilità dovranno essere ricostruiti, caso per caso, a seconda delle circostanze di fatto che hanno determinato nella fattispecie concreta la lesione di uno dei sopra delineati interessi protetti** dal nostro ordinamento giuridico.

Un esempio può essere di aiuto: ipotizziamo che un drone cada rovinosamente al suolo colpendo un comune cittadino che passeggia sulla pubblica via, cagionandogli lesioni gravi; chi sarà penalmente responsabile dei danni causati dall'agente artificiale?

La risposta, come facilmente intuibile, non può essere data se non dopo un'accurata analisi delle cause che hanno determinato la caduta del drone. Questa analisi, verosimilmente, costituirà oggetto di una consulenza tecnica, il cui esito consentirà di individuare le cause e – di conseguenza – i soggetti potenzialmente responsabili.

Va da sé che – nel caso in cui la causa venga individuata nella rottura di un componente meccanico – dovrà essere valutata la posizione del progettista/produttore, mentre – laddove la causa venga attribuita alla perdita della connessione Internet con cui il drone comunica con la piattaforma di controllo a terra – dovrà essere esaminata la posizione del gestore che ha fornito il servizio, e del programmatore che non ha previsto l'ipotesi di perdita di connessione.

L'individuazione della causa e del soggetto che risponde dello specifico settore coinvolto nel sinistro, ovviamente, non rappresenta ancora la "soluzione del caso". **Trattandosi di responsabilità penale colposa dovrà, infatti, essere analizzato**

[20] Cfr., ad esempio: http://www.medialaws.eu/il-volo-radente-dei-droni-su-privacy-e-data-protection/.

[21] Il testo integrale è disponibile al seguente indirizzo: http://www.personaedanno.it/attachments/article/38246/Sent%20G.pdf.

lo specifico comportamento, per verificare se il soggetto avesse previsto adeguate misure di sicurezza atte ad evitare l'evento e, in caso affermativo, per quali motivi esse non abbiano nel concreto funzionato (come, ad es., nel caso in cui – pur essendo stata prevista una procedura per cui, in caso di assenza di link drone-ground station per un certo numero di minuti, il drone debba automaticamente tornare alla base – esso abbia invece perso quota e sia caduto).

Argomentazioni analoghe valgono per il trattamento illecito di dati personali, in cui, come si è detto, l'allocazione della responsabilità va calibrata sulla scorta dell'attività posta in essere in concreto dai soggetti che, ai sensi del codice privacy, possono essere configurati come *"titolar[i] del trattamento"*, ovverosia coloro che decidono finalità e mezzi del singolo trattamento dei dati personali.

Infine, va ricordato che l'art. 41 del codice penale stabilisce il principio secondo cui il "*concorso di cause preesistenti o simultanee o sopravvenute, anche se indipendenti dall'azione od omissione del colpevole, non esclude il rapporto di causalità fra l'azione od omissione e l'evento*".

Ciò significa che – **in ogni singola fattispecie concreta – sarà necessario analizzare l'eventuale sussistenza di concause**, con conseguente estensione dei profili di penale responsabilità in capo a più soggetti, i quali dovranno dunque tutti rispondere del fatto di reato, ognuno per la parte di comportamento colposo a lui attribuibile.

4.3 Privacy e trattamento dati

(a cura di Guido Noto La Diega)

Introduzione e principi generali

Costruire un discorso unitario sul tema "privacy e robot" sarebbe infecondo e forse anche impossibile. Occorre, infatti, diversificare il ragionamento a seconda che si abbia riguardo, rispettivamente, ai robot (e segnatamente quelli "di servizio", oggetto della presente indagine) ed ai droni. In considerazione della sede, prioritaria attenzione sarà dedicata ai primi, pur non omettendo cenni ai secondi, sui quali si registra una produzione normativa ormai considerevole, che consente, fra l'altro, qualche considerazione in chiave comparatistica.

Come recita la prima legge della robotica di Asimov, "*a robot may not harm a human being, or, through inaction, allow a human being to come to harm*". Ora, **fra i principali danni che può provocare l'uso dei robot nella vita quotidiana, vi sono senz'altro le minacce alla *privacy*** dei cittadini. E l'unico modo per venirne a capo – come avvertiva Carlo Sarzana di S. Ippolito già vent'anni fa – è l'istituzione di *"*equipes *miste, secondo un approccio multidisciplinare, onde evitare di trovarsi in un* vuoto giuridico*"*[22].

Nell'articolare un ragionamento sulla relazione fra robot e *privacy*, bisogna aver ben presente che non è sufficiente porre in luce i pericoli per quest'ultima in un ambiente robotizzato: essa, infatti, può anche risultare tutelata dalle macchine in parola. Se è, forse, più intuitivo immaginare le ragioni per cui l'uso dei robot possa costituire una minaccia per la *privacy*, non altrettanto lo è aver coscienza dell'uso protettivo di queste macchine, che ben potrebbero essere utilizzate come cani da guardia meccanici, in grado di tutelarci da indesiderate invasioni della sfera privata dell'individuo[23]. Va da sé, però, che il discorso verrà portato avanti avendo primario riguardo al risvolto negativo dell'uso delle tecnologie esaminate, posto che è esso a far emergere la necessità di chiarire e (ri)costruire un *framework* giuridico adeguato.

Giova sin da subito precisare, però, che ogni approccio nichilistico va abbandonato. Mentre, infatti, non è tanto chiaro come e se si possa reagire all'impatto sociale e psicologico di robot sempre più interattivi e simili all'uomo[24], non lo stesso è da dirsi con riferimento alla sorveglianza e all'accesso: rispetto a questi ultimi, infatti, è ben possibile immaginare soluzioni basate su

---

[22] C. Sarzana di S. Ippolito, *I riflessi giuridici delle nuove tecnologie informatiche*, in *Dir. inf.*, 1994, III, 505, che però non tocca la questione della *privacy*, menzionando solo i problemi della responsabilità per il comportamento dannoso dei robot, la comparazione fra *offendicula* e robots-cani da guardia, nonché la già allora *vexata quaestio* dei diritti civili dei robot, quantomeno sotto forma di personalità giuridica (si pensi ai notissimi lavori di P. McNally, S. Inayatullah, *The rights of robots: Technology, culture and law in the 21st century*, in *L. & Tech.*, 1987, IV, 20; H. Putnam**,** *Mente, linguaggio e realtà*, Milano 1987, 426 e S. Gozzano, *I cinque sensi dei robot. Percezioni artificiali: l'informatica non imita solo l'intelligenza ma anche le capacità sensoriali*, in *Sapere*, 1990, IV, 9.

[23] Formula osservazioni convergenti R. Calo, *Robots and privacy*, in *Robot Ethics: The Ethical and Social Implications of Robotics*, a cura di P. Lin, K. Abney, G.A. Bekey, Cambridge, 2011, 187 (consultato nella versione *online* disponibile all'indirizzo ssrn.com/abstract=1599189), là dove scrive che "*nor the implication of robots for privacy is entirely negative – vulnerable populations such as victims of domestic violence may one day use robots to prevent access to their person or home and police against abuse*" (p. 3 della versione *online*).

[24] Basti pensare all'impossibilità di ritagliarsi degli spazi di reale solitudine, oppure al fenomeno dell'*uncanny valley*, avvallamento perturbante, illustrato dal notissimo e controverso saggio di M. Mori, *Bukimi no tani - The uncanny valley*, in *Energy*, 1970, IV, 33, che descrive il fenomeno – di dubbia scientificità, ma certamente affascinante – per cui la familiarità e piacevolezza prodotta dalla visione di robot simili all'uomo aumenta in modo direttamente proporzionale all'aumento dell'antropomorfismo degli stessi, sino a giungere ad un punto in cui la curva (di un grafico avente in ascisse la somiglianza all'uomo e in ordinata la reazione empatica) produce un radicale avvallamento, il quale indicherebbe sentimenti di ripulsa o inquietudine.

buone leggi e accorgimenti ingegneristici[25], fra i quali spicca, senz'altro, la c.d. *privacy by design*, che si ottiene "*by building fair information practice principles into informations technology, business practices, and physical design and infrastructures*"[26].

Posto che i robot sono provvisti dell'abilità di sentire, elaborare e memorizzare il mondo intorno a loro[27] e considerato che il principale uso degli stessi, dopo la manifattura industriale, è quello a fini di sorveglianza, non è arduo comprendere come essi costituiscano un pericolo per la *privacy*. Essi possono, infatti, vedere e sentire ciò che sovente è inibito all'uomo, ed accedere a luoghi normalmente irraggiungibili, con una resistenza ed una memoria sempre più spesso superiori all'umana[28]. Chiaramente, i droni, con la loro maggiore motilità, costituiscono un'insidia di massima assai maggiore dei robot non volatili, ma casi come il Ninja di Shigeo Hirose – che può scalare altezze rilevanti tramite un sistema a ventose – mostrano come il confine sia labile, e come un approccio casistico sia pressoché irrinunciabile.

Problematiche giuridiche rilevanti

Sino a tempi recenti, il tema delle problematiche connesse all'impiego dei robot è stato per lo più ignorato dai giuristi; detta circostanza si spiega alla luce del fatto che i robot erano confinati all'uso militare[29] o industriale.

Oggi che i "*robot leave the factory floor and battlefield and enter the public and private sphere in meaningful numbers*"[30], diviene però improcrastinabile una riflessione su di un fenomeno che si appresta ad incidere sulla società come e più dei computer, a detta di un operatore più che qualificato[31]. C'è chi ha provato a superare il più immediato inquadramento metaforico orwelliano, in favore di uno kafkiano[32], là dove si è sostenuto che il problema della vita contemporanea sia il non sapere mai effettivamente se un'informazione sarà utilizzata contro di noi; ma il punto sembrerebbe essere proprio quello al centro di "*1984*": non siamo, cioè, in grado di stabilire quale sia il livello di controllo delle nostre vite portato avanti tramite i nuovi ritrovati tecnologici[33].

Malgrado tanto le nuove capacità di sorveglianza, quanto quelle di accesso giochino un ruolo centrale nella relazione robot-*privacy*, non si può negare che siano le seconde a dover essere tenute in maggiore considerazione quando si parla di robot di

---

[25] I produttori di robot faranno bene a tenere a mente lo studio di T. Denning *et al*., *A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and* Lessons, Proceedings of the 11th International Conference on Ubiquitous Computing, 30-09/3-10-2009, New York, 2010, i quali, scegliendo come *case studies* il *WowWee Rovio*, l'*Erector Spykee* e il *WowWee RobotSapien V2*, hanno posto in evidenza la vulnerabilità di questi robot – equipaggiati con videocamere e connessione ad Internet – sia agli *hacker* che allo Stato. Si aggrava pertanto un problema esistente: la sicurezza delle *webcams* installate sui computer di casa (così come di quelle degli altri dispositivi elettronici) non ha mai raggiunto un approdo del tutto rassicurante; la situazione si complica, però, con apparecchi in grado di muoversi attraverso tutti gli spazi disponibili e, non infrequentemente, dotati di sensori ben più raffinati delle tradizionali *webcams* domestiche.

[26] A. Cavoikian, S. Taylor, M. E. Abrams, *Privacy by Design: essential for organizational accountability and strong business practices*, 04-06-2010, Springerlink.com, 409. Cfr. pure, *ex multis*, I. S. Rubinstein, N. Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, Public Law & Legal Theory Research Paper Series Working Paper n. 12-43, 2012, 1333.

[27] Cfr. P. W. Singer, *cit.*; Denning *et al*., *cit*.; R. Calo, *Robots and privacy*, *cit*.

[28] V. B. J. Fogg, *Persuasive Technologies: Using Computers to Change What We Think and Do*, San Francisco, 2003, 313, il quale pone in luce che il robot può essere ben più persuasivo di un essere umano, atteso che ha una memoria perfetta, non soffre il sonno e non si imbarazza.

[29] Si segnala, da ultimo il d.m. 7-5-2014 del Ministero della Difesa recante *"Approvazione del nuovo elenco dei materiali d'armamento da comprendere nelle categorie previste dall'articolo 2, comma 2, della legge 9 luglio 1990, n. 185, in attuazione della direttiva 2014/18/UE"*, che comprende anche *""robot", unità di comando di "robot" e "dispositivi di estremità" di "robot", aventi almeno una delle caratteristiche seguenti: 1. appositamente progettati per uso militare; 2. dotati di mezzi di protezione dei collegamenti idraulici contro perforazioni prodotte dall'esterno causate da frammenti balistici (ad esempio, sistemi di autosigillatura dei collegamenti idraulici) e progettati per l'uso di fluidi idraulici con punto di infiammabilità superiore a 839 K (566°C); o 3. appositamente progettati o predisposti per funzionare in ambiente sottoposto a impulsi elettromagnetici (*Electro Magnetic Pulse*, EMP)"* (Allegato, categoria 17, lett. e).

[30] R. Calo, *Robots and privacy*, *cit*.

[31] Ci si riferisce a B. Gates, *A Robot in Every Home*, in *Scientific American*, gennaio 2007, 58, che descrive quella in parola come la prima grande rivoluzione tecnologica successiva a quella del computer, per cui "*we may be on the verge of a new era, when the PC will get up off the desktop and allow us to see, hear, touch and manipulate object in places where we are not physically present*".

[32] D. Solove, *The Digital Person: Technology and Privacy in the Digital Age*, New York, 2004, 36.

[33] Il discorso vale non solo per i robot, ma anche, ad es., per il *cloud computing*, là dove non siamo in grado di avvederci dell'accesso non autorizzato di terzi ai nostri dati in *web storage*. Anche in considerazione dell'ampiezza oggi raggiunta dal fenomeno della *cloud robotics*, si rinvia sul punto a G. Noto La Diega, Cloud computing *e protezione dei dati nel* web *3.0*, in *Giustiziacivile.com*, 05-04-2014.

servizio (le prime rilevando principalmente per i droni, specialmente quando ad uso militare), se è vero – e lo è – che "*the home robot in particular presents a novel opportunity for government, private litigants, and hackers to access information about the interior of a living space*"[34]. E non v'è chi non veda che, quantunque costituisca un pericolo pure l'accesso di un pirata informatico a un computer, una cosa è disporre di *file* e cartelle, altra è accedere ad un'abitazione e agli oggetti più privati, interferendo nei comandi del robot di casa.

Quanto al profilo della sorveglianza, quindi, basti qui dire che il tema non è confinato all'ambito militare, se è vero, da una parte, che le *law enforcement agencies* di tutto il mondo stanno facendo ricorso ai robot a detto fine[35]; dall'altra, che ormai anche i privati vi fanno ricorso per fini securitari o di monitoraggio dei dipendenti.

I robot di servizio, però, più che intersecare il piano della sorveglianza, rilevano per l'accesso a luoghi e dati tradizionalmente privati. Aumentando la concorrenza ed abbassandosi i prezzi, diviene sempre meno infrequente la presenza di queste macchine, le quali, essendo per lo più connesse a Internet, sono in grado di trasmettere all'esterno – alla pubblica autorità, a controparti e, potenzialmente, anche a pirati informatici – dati sensibili, potendo altresì essere dagli stessi terzi guidate e manovrate. Per immaginare la quantità e qualità delle informazioni attingibili, basti pensare che, accanto a connessioni in grado di mandare *online* in diretta immagini, suoni e video, questi apparecchi sono equipaggiati viepiù sovente con videocamere a infrarossi, *sonar*, nasi elettronici[36], accelerometri e GPS.

I problemi sono analoghi, *mutatis mutandis*, a quelli già noti a quanti abbiano riflettuto sull'*Internet of Things*: si pensi, ad esempio, alla possibilità di attivare, all'insaputa del conducente, il microfono in un'automobile[37]. Allo stesso modo, si possono intercettare i flussi audio e video del robot, e deciderne spostamenti e direzionamento dei sensori. Il robot, inoltre, può fare parte di una rete di oggetti interconnessi nella disponibilità dell'utente del robot medesimo, per cui vi è il rischio che terzi possano incrociare i dati prodotti dagli oggetti del network per trarne informazioni commercialmente rilevanti[38].

Uno dei principali problemi di *privacy* sollevati dalla robotica di servizio è legato alla circostanza che la memoria interna di tali dispositivi risulta sempre alquanto limitata; per questa ragione, tradizionalmente, "*lacking the onboard capability to process all of the data, the robot periodically uploads it the manufacturer for analysis and retrieval*"[39]. Da ciò consegue che, lungo questo itinerario, si può facilmente assaltare la "diligenza" informativa.

D'altra parte, negli ultimi anni, ha preso sempre più campo la *cloud robotics*, che consente, fra l'altro, di sfruttare "la nuvola" per l'archiviazione (ma anche l'elaborazione stessa) dei dati, senza dover passare dal produttore. **La sicurezza delle informazioni *cloudified*, un tempo assai controversa, diviene oggi sempre più solida, specialmente grazie ai nuovi sistemi di cifratura omomorfica, che è bene fare inserire nel contratto col *cloud provider*, insieme a specifiche attinenti alla geolocalizzazione delle *server farm***.

Robot "di servizio", però, come detto, non vuol dire solo *home* robot. La sostituzione dello staff commerciale con robot costituisce un'inedita opportunità per la raccolta di dati in sede di trattative e transazioni commerciali, come mostra l'esempio degli *shopping assistants*, già da anni in auge in Giappone e ormai presenti anche in Europa e U.S.A. Essi identificano il potenziale cliente e lo indirizzano verso un prodotto; nel far ciò, però, a differenza dei tradizionali addetti, questi robot possono registrare ed elaborare ogni aspetto della transazione, potendo, ad es., riconoscere il cliente ad un successivo incontro grazie alla tecnologia *face recognition*[40]. I dati così raccolti potrebbero essere di straordinaria utilità "*in both loss prevention and*

---

[34] R. Calo, *Robots and privacy*, *cit.* Non si consideri superfluo precisare che, anche prima dei robot di servizio, era possibile accedere a informazioni private (ad es., tramite una *webcam*), ma oggi aumentano le possibilità tecniche di raccolta e analisi dei dati e, inoltre, cambiano la quantità e qualità dei dati (una cosa è una *webcam* fissa, un'altra un robot che si muove per la casa e che oltre la telecamera è munito, di norma, di sensori di varia natura).

[35] Lo segnala N. Sharkey, *2084: Big Robot is Watching You. Report on the Future of Robots for policing, surveillance and security*, 2008, www.scribd.com/mobile/doc/139971746 (consultato il 22-05-2014).

[36] Su questo non molto noto dispositivo, cfr., ad es., N. Schactman, *Drones See, Smell Evil from Above*, in *Wired.com*, 24-03-2003 e J. B. Chang, V. Subramanian, *Electronic Noses Sniff Success*, in *IEEE Spectrum*, marzo 2008 (disponibile all'indirizzo http://spectrum.ieee.org/biomedical/devices/electronic-noses-sniff-success/).

[37] Vi fa menzione J. Zittrain, *The Future of the Internet – And How to Stop It*, New Haven, 2008, 110.

[38] Si pensi, *ex multis*, al problema del *cross-device tracking* tramite messaggi pubblicitari che non possono essere uditi dall'essere umano, ma che consentono di identificare i dispositivi della rete considerata. Il problema e' scottante: non a caso, la *Federal Trade Commission* (FTC) ha organizzato recentemente un workshop sul tema; v. soprattutto C. Calabrese *et al.*, *Comments for November 2015 Workshop on Cross-Device Tracking*, Center for Democracy & Technology, 16-10-2015, https://cdt.org/files/2015/11/10.16.15-CDT-Cross-Device-Comments.pdf.

[39] R. Calo, *Robots and privacy*, *cit*.

[40] Su *face recognition* e robot vedere Article 29 Data Protection Working Party, Opinione 27-04-2012 n. 3 *"sugli sviluppi nelle tecnologie biometriche"*, là dove si ipotizza, come scenario considerato irreale, *"un sistema di sorveglianza video di prossima generazione, pensato per centri commerciali, in grado di riconoscere le persone, individuare i movimenti in maniera automatica e distinguere caratteristiche del volto quali il sorriso o la rabbia. Esso potrebbe riconoscere i clienti abituali già all'ingresso del parcheggio riservato e guidarli verso i loro posti preferiti. Nel momento in cui i clienti entrano nel centro commerciale, il sistema potrebbe identificarne l'abbigliamento per suggerire i negozi da visitare in base alle offerte disponibili, ciò a fronte di dati raccolti sui precedenti acquisti o di una serie prevista di indicatori. Potrebbe inoltre essere organizzata una pubblicità su misura nelle vetrine o potrebbe essere posto un divieto di accesso automatico a negozi,*

marketing research"[41].

Normativa di riferimento applicabile

Veniamo alla normativa applicabile, là dove viene colta l'intersezione robot-privacy.

In ragione dell'attuale dinamica delle fonti del diritto, non si può non prendere le mosse dalla normazione europea e, quindi, per quanto qui più direttamente interessa, dalla **Dir. 2006/42 (anche nota come "direttiva macchine"), recepita con D. Lgs. n. 17/2010.**

Con lodevole sensibilità per i problemi sopra lumeggiati, l'art. 18 della suddetta direttiva contempla un'apposita disciplina in materia di riservatezza. Ivi si prevede che "*1. Ferme restando le disposizioni e le prassi nazionali in materia di riservatezza, gli Stati membri operano affinché tutte le parti e le persone coinvolte nell'applicazione della presente direttiva siano obbligate a mantenere riservate le informazioni ricevute nello svolgimento delle loro funzioni. In particolare i segreti aziendali, professionali e commerciali sono considerati come informazioni riservate, eccetto quando la loro divulgazione sia necessaria al fine di tutelare la salute e la sicurezza delle persone. 2. La disposizione di cui al paragrafo 1 si applica fatti salvi gli obblighi degli Stati membri e degli organismi notificati riguardanti l'informazione reciproca e la diffusione degli avvertimenti*".

Va notato che non si tratta di una disciplina speciale che *derogat generali*, bensì di un rafforzamento di tutela che si giustappone a quella generale vigente in materia di protezione dei dati personali (e di tutela dei segreti aziendali, professionali e commerciali). D'altronde, in termini analoghi si pronunzia l'art. 14, D. Lgs. n. 17/2010, là dove tiene "*ferme [...] le disposizioni di cui al decreto legislativo 30 giugno 2003, n. 196, in materia di protezione dei dati personali ed al decreto legislativo 10 febbraio 2005, n. 30, recante codice della proprietà industriale*". Per il resto, è riprodotta *verbatim* la disposizione europea, con l'eccezione che, a poter rendere "non riservato" un segreto, nella disciplina italiana, sono non soltanto la salute e la sicurezza delle persone, ma anche "*se del caso, degli animali domestici o dei beni, o, qualora applicabile, dell'ambiente*".

Il legislatore del recepimento avrebbe potuto essere più coraggioso e non limitarsi a ricalcare acriticamente e pedissequamente le norme della direttiva macchine; ad ogni modo, con un'attenta operazione ermeneutica, è possibile trarre ulteriori indicazioni rilevanti per la *privacy* dal complesso dall'articolato normativo. Anzitutto, è previsto che **il fabbricante o il suo mandatario, prima di immettere sul mercato ovvero mettere in servizio una macchina si accerti che questa soddisfi i pertinenti requisiti essenziali di sicurezza e di tutela della salute, e che il fascicolo tecnico sia disponibile (art. 3, co. 3, D. Lgs. n. 17/2010)**. I requisiti essenziali di sicurezza sono previsti dall'allegato I in calce alla direttiva (ed al decreto), ove si prevede, fra l'altro, che "*con il processo iterativo della valutazione dei rischi e della riduzione dei rischi di cui sopra, il fabbricante o il suo mandatario stabilisce i limiti della macchina, il che comprende l'uso previsto e l'uso scorretto ragionevolmente prevedibile*" (punto 1). Non sembra una forzatura sostenere che fra i rischi che vadano tenuti presenti rientri la riservatezza, e che – nei limiti da porre alla macchina per impedirne un uso scorretto – siano sussumibili le misure di *privacy by design*. Residua sempre, beninteso, un margine ineliminabile di pericolo per i dati, ma anche questa circostanza è tenuta in considerazione dal primo allegato, là dove si prescrive che "*nel caso in cui permangano dei rischi, malgrado siano state adottate le misure di protezione integrate nella progettazione, le protezioni e le misure di protezione complementari, devono essere previste le necessarie avvertenze*" (punto 1.7.2). Quanto, poi, al menzionato fascicolo tecnico, esso è regolato dall'allegato VII, il quale vuole che ivi confluisca, fra l'altro, la "*documentazione relativa alla valutazione dei rischi che deve dimostrare la procedura seguita, inclusi: i) un elenco dei requisiti essenziali di sicurezza e di tutela della salute applicabili alla macchina, ii) le misure di protezione attuate per eliminare i pericoli identificati o per ridurre i rischi e, se del caso, l'indicazione dei rischi residui connessi con la macchina*" (punto 1, a).

Vale la pena di ricordare che **l'art. 15 del D. Lgs. n. 17/2010 contempla delle sanzioni amministrative** per chi immetta sul mercato o metta in servizio macchine non conformi all'allegato I, nonché per il fabbricante o il mandatario che non esibisca la documentazione tecnica di cui al settimo allegato. In via interpretativa, il sistema sembra già potersi considerare completo, ma, *de iure condendo*, si auspica che il legislatore espliciti la necessità di valutare i rischi per la riservatezza e di prevedere misure tecniche di *privacy by design*.

---

ristoranti e altri luoghi. Potenziali ladri di automobili potrebbero essere identificati prima ancora che tocchino un'automobile. Se necessario, la presenza di velivoli telecomandati (droni) con videocamere e altri sensori potrebbe essere utile a conservare le tracce dei sospettati fino alla smentita o alla conferma del sospetto. Potrebbe essere rilevata la presenza di oggetti nascosti negli indumenti (coltelli o articoli rubati nei negozi). Questa tecnologia non si basa unicamente sui nuovi sistemi biometrici ma combina ed elabora informazioni già disponibili con altri dati raccolti da una serie di sistemi diversi".

[41] R. Calo, *Robots and privacy, cit.*

Per quanto riguarda i droni, a livello europeo, uno dei documenti principali[42] è la **comunicazione di aprile 2014 sull'uso civile dei sistemi aerei a pilotaggio remoto**[43], che – nell'enunciare il nucleo della strategia europea – chiarisce che "*La progressiva integrazione dei sistemi RPAS nello spazio aereo a partire dal 2016 deve essere accompagnata da un adeguato dibattito pubblico sullo sviluppo di misure in grado di affrontare le preoccupazioni della società tra cui protezione, tutela dei dati e della vita privata, responsabilità civile e assicurazione o sicurezza*"[44]. Non è senza significato che il paragrafo 3.4 della suddetta comunicazione, dedicato a *"Tutelare i diritti fondamentali dei cittadini"*, sia in realtà un breviario del rapporto droni-*privacy*. Si prendono le mosse dalla notazione per cui, nella vasta gamma delle potenziali applicazioni civili dei sistemi RPAS (*Remote Piloted Aircraft System*, in italiano Sistemi Aeromobili a Pilotaggio remoto – SAPR), alcune possono comportare la raccolta di dati personali e sollevare questioni riguardanti l'etica, la tutela della vita privata o la protezione dei dati, in particolare in settori quali sorveglianza, monitoraggio, mappatura e registrazione video. Dopodiché si prescrive che gli operatori dei sistemi aerei a pilotaggio remoto rispettino le disposizioni vigenti in materia di protezione dei dati, "*in particolare quelle stabilite dalle misure nazionali istituite a norma della direttiva 95/46/CE sulla protezione dei dati e della decisione quadro 2008/977*"[45]. Vengono, poi, individuati come "*rischi più comunemente identificati*" quelli derivanti dall'uso di apparati di sorveglianza installati su detti sistemi, e si prescrive, per ovviare ad essi, che "*qualsiasi trattamento dei dati personali dovrà basarsi su un motivo legittimo. Di conseguenza, l'apertura del mercato del trasporto aereo ai sistemi RPAS dovrà prevedere una valutazione delle misure necessarie a garantire il rispetto dei diritti fondamentali, la protezione dei dati e la tutela della vita privata. La questione della tutela della vita privata necessiterà di un monitoraggio continuo da parte delle autorità competenti, comprese le autorità nazionali di controllo responsabili della protezione dei dati*". A tal fine, conclusivamente, l'Unione prende l'impegno d'intraprendere un'azione: la Commissione valuterà come rendere le applicazioni RPAS conformi alle norme sulla protezione dei dati e, a tal fine, consulterà esperti e parti interessate; adotterà misure che rientrino nel suo settore di competenza – possibilmente comprendendo eventuali azioni di sensibilizzazione per proteggere i diritti fondamentali – e, infine, promuoverà misure di competenza nazionale.

Intorno a detta comunicazione si e' sviluppata una vivace attività consultiva, di cui è espressione degna di nota ai presenti fini l'Opinione dello *European Data Protection Supervisor* (EDPS)[46], avente come scopo l'identificazione delle situazioni in cui i SAPR trattano dati personali e in cui, conseguentemente, i responsabili sono soggetti alla relativa disciplina. In detta sede si osserva come la protezione dei dati personali e la privacy *by design* siano essenziali per lo sviluppo del mercato dei SAPR, al punto che "*only those RPAS that will have integrated data protection and privacy in their design will be well regarded by society at large*". A quanto pare, si ritiene che, nella maggior parte dei casi, i SAPR trattino dati personali non in quanto velivoli, bensì a causa del loro variegato campo applicativo e, soprattutto, dei sensori e delle altre tecnologie con cui interagiscono[47]. Lo scenario si complica qualora si pensi al *machine learning* ed alla creazione di macchine propriamente autonome (impropriamente "intelligenza artificiale"). Da ciò seguirebbe che gli Stati Membri e le istituzioni dell'Unione Europea debbano assicurare il rispetto dell'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea (CDFUE) – e del diritto derivato – con riguardo al trattamento effettuato tramite SAPR, *"be it for commercial or professional, law enforcement, intelligence or private purposes"*. Non si vede come il *law enforcement* possa essere incluso, considerato che pubblica sicurezza, difesa e sicurezza dello Stato non rientrano nel campo di applicazione della direttiva 95/46/CE[48] e, più in generale, rientrano ancora nel nocciolo duro della sovranita' nazionale. Inoltre, andrebbe aggiornata l'affermazione secondo cui la disciplina europea considerata si applichi "*as long as the processing takes place in the context of the activities of an establishment of the controller in the EU or with equipment or means located in the EU*". Secondo un'interpretazione estensiva del diritto dell'Unione, infatti, la Corte di Giustizia ha statuito – nel caso *Weltimmo*[49] – che non importa che non vi sia uno stabilimento o, comunque, degli equipaggiamenti nell'Unione, dovendosi analizzare, alla luce di un insieme di fattori (quali, ad es., la lingua di un sito) se il

---

[42] La citata comunicazione non è, certamente, l'unico atto che meriterebbe approfondimento. Si pensi alla com. 13-02-2008, recante *"esame della creazione di un sistema europeo di sorveglianza delle frontiere (EUROSUR)"* (COM/2008/68), nella parte in cui si osserva che "*[l]e varie attività indicate nelle sezioni precedenti* [NOTA: fra cui anche il controllo delle frontiere tramite UAV] *possono comportare il trattamento di dati a carattere personale. Vanno quindi rispettati i principi in materia di tutela dei dati personali applicabili nell'Unione europea: i dati personali devono essere trattati in modo corretto e lecito, devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento dei dati personali nel contesto di EUROSUR deve quindi basarsi su misure legislative appropriate, che ne definiscano la natura e prevedano adeguate garanzie*" (§ 4).

[43] Com. 08-04-2014, "*Una nuova era per il trasporto aereo. Aprire il mercato del trasporto aereo all'uso civile dei sistemi aerei a pilotaggio remoto in modo sicuro e sostenibile*" (COM/2014/207), § 3.

[44] Com. 2014/207, § 3.

[45] La seconda, meno nota, è la decisione del consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale.

[46] EDPS, *Opinion on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner",* 26-11-2014.

[47] L'EDPS fa l'esempio di una videocamera con annesso software per trattare il video; essa potrebbe essere capace di high power zoom, facial recognition, behaviour profiling, movement detection, e number plate recognition.

[48] V. soprattutto l'art. 3, co. 2 dir. 95/46/CE.

[49] Corte di Giustizia, sez. III, 01-10-2015, C- 230/14 *Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639.

servizio sia comunque rivolto ad uno Stato Membro.

Un altro punto su cui si pone l'accento è che i SAPR tratterebbero piu' dati personali, se paragonati ad aereoplani e videocamere a circuito chiuso. Quanto agli aeroplani, l'EDPS osserva che *"the capacities embedded can reveal far more than the naked eye"*; così si mostra di ignorare che, ormai, pressoché tutti i velivoli sono dotati di sensori e tecnologie ad altissima precisione. Il punto è, semmai, che i SAPR – di norma – volano ad una distanza tale da poter captare immagini, suoni e video senza poter essere agevolmente scoperti. La questione della visibilità è invece riportata con riguardo al rapporto con le telecamere a circuito chiuso, rispetto alle quali pure si osserva che *"their mobility and discretion offers more and also increasingly different uses"*. Mobilità e clandestinità li rendono, inoltre, ottimi strumenti di sorveglianza.

Facendo proprio il *ruling* della Corte Europea dei Diritti dell'Uomo nel caso *Von Hannover v. Germany*[50], si osserva poi che il fatto che le attività si svolgano sovente in luoghi pubblici o aperti al pubblico non esclude aspettative di privacy; infatti, "*[t]here is thus a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life*". Resterebbe dunque fermo, ad es., il diritto a non essere presi di mira con zoom o microfoni direzionali per la registrazione dei movimenti e delle conversazioni in pubblico.

Per quanto riguarda le attività private (ad es., a fini di hobby), l'EDPS enuncia un'interpretazione restrittiva dell'eccezione riguardante le attività a carattere esclusivamente personale o domestico (art. 3, comma 2, secondo trattino, direttiva 95/46/CE), perfettamente in linea con la proposta ermeneutica che – di lì a due settimane – sarebbe stata avanzata dalla Corte di Giustizia, nel caso *František Ryneš c. Úřad pro ochranu osobních údajů*[51]: in quest'ultima, si concluderà che la direttiva in parola si applica alla registrazione di video effettuata con una videocamera per sorveglianza installata in una privata abitazione e diretta su un sentiero pubblico. L'EDPS, dal canto suo, si richiama al noto caso *Lindqvist*[52], per desumerne che il trattamento effettuato da soggetti privati non ricadrebbe nell'eccezione *de qua*[53], qualora sia diretto "*at sharing or even publishing the resulting video/sound captures/images or any data allowing the direct or indirect identification of an individual on the Internet and, consequently, to an indefinite number of people (for instance, via a social network*)".

Per ciò che concerne, poi, gli usi commerciali e amministrativi, per giustificare l'applicazione extraterritoriale del diritto dell'Unione Europea si richiama il notissimo caso *Google Spain*[54], che – a determinate condizioni – consente l'applicazione della direttiva 95/46 a trattamenti posti in essere da imprese stabilite al di fuori dell'Unione. Se ne desume che i produttori di SAPR – anche per non ritrovarsi in aperta violazione dell'approvando Regolamento sulla protezione dei dati personali (GDPR)[55] – dovrebbero implementare misure di *privacy by design* e *by default*, nonché porre in essere *data protection impact*

---

[50] Corte Europea dei Diritti dell'Uomo, sez. III, 24-06-2004, app. n. 59320/00 *Von Hannover v. Germany*, in *Reports of Judgments and Decisions 2004-VI*, riguardante la Principessa Carolina di Monaco e i suoi tentativi di vietare la pubblicazione di foto della sua vita privata sui tabloid.

[51] Corte di Giustizia, sez. IV, 11-12-2014, C-212/13, *František Ryneš c. Úřad pro ochranu osobních údajů*, ECLI:EU:C:2014:2428.

[52] Corte di Giustizia, 06-11-2003, C-101/01, *Procedimento penale a carico di Bodil Lindqvist*, in *European Court Reports*, 2003 I-12971.

[53] Secondo l'Art. 29 Data Protection Working Party, i fattori da valutare ai fini della *household exception* sono "- *if the personal data is disseminated to an indefinite number of persons, rather than to a limited community of friends, family members or acquaintances, - if the personal data is about individuals who have no personal or household relationship with the person posting it, - if the scale and frequency of the processing of personal data suggest professional or full-time activity, - if there is evidence of a number of individuals acting together in a collective and organised manner,- if there is a potential adverse impact on individuals, including intrusion into their privacy*". V. *Annex 2, Proposals for Amendments regarding exemption for personal or household activities*, disponibile all'indirizzo: http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2013/20130227_statement_dp_annex2_en.pdf.

[54] Corte di Giustizia, grande sez., 13-05-2014, C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (*AEPD) e *Mario Costeja González*, ECLI:EU:C:2014:317, in particolare nella parte in cui si stabilisce che *"[l]'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 deve essere interpretato nel senso che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai sensi della disposizione suddetta, qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro"*.

[55] Il GDPR sostituirà la dir. 95/46/CE. V. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation), COM(2012) 11 final, 25-01-2012, 2012/0011 (COD). La bozza è disponibile all'indirizzo http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. Per quanto riguarda la versione approvata dal Consiglio, v. Nota n. 9565/15 dell'11-06-2015 della Presidenza del Consiglio dell'Unione Europea (disponibile all'indirizzo http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf). A tenore dell'art. 3, comma 2 GDPR (2012), il regolamento si applica al "*processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour*". La versione del Consiglio precisa che sussiste

assessments (DPIAs).

L'EDPS é consapevole che la privacy debba essere specialmente oggetto di bilanciamento quando sia in gioco la libertà d'espressione, al cui scopo la direttiva dà la possibilità agli Stati Membri di introdurre apposite deroghe. Così, l'opinione tratta anche dell'uso dei SAPR per fini giornalistici, i quali devono essere intesi conformente al *dictum* della sentenza *Satamendia*[56], alla stregua della quale la diffusione deve avere come *"unica finalità [...] la divulgazione al pubblico di informazioni, opinioni o idee"*. Ne segue che la mera pubblicazione di dati su Internet o su un giornale non cade, in sè e per sè, nel campo applicativo dell'eccezione *de qua*.

Per quel che riguarda, poi, l'uso dei SAPR da parte delle *law enforcement authorities* (LEAs), l'EDPS non dice apertamente che la direttiva 95/46 non trova qui applicazione, ma ciò può tuttavia essere inferito dall'affermazione che si applicano l'art. 8 della Convenzione Europea dei Diritti dell'Uomo (CEDU) e la relativa giurisprudenza[57]. Quando si tratta di precisare in cosa consista l'applicazione di tale disciplina alle LEAs, il Supervisor specifica che l'attività dev'essere basata sulla legge o prescritta dalla legge, e che questa dev'essere chiara, dettagliata, accessibile pubblicamente, dimodoché i cittadini possano ottenere informazioni su come i loro diritti possano interferire con le attività delle LEAs. Ciò dovrebbe consentire di prevedere quando si sia soggetti a misure che coinvolgano l'uso di SAPR. Sia consentito notare che è veramente raro – se non impossibile – che una legge, per sua natura, sia talmente dettagliata da consentire di prevedere ogni possibile ipotesi applicativa. Anche qualora una consimile legge esistesse – e, si ripete, così non è – sarebbe utopistico ritenere che il cittadino l'abbia letta e compresa, e che ne sappia desumere le conseguenze applicative qualora si svolgano attivita' di *law enforcement* condotte mediante SAPR.

L'unica disciplina positiva[58] che sembra effettivamente applicabile, per il caso di uso di SAPR per la cooperazione giudiziaria o di polizia, è la decisione-quadro 2008/977/GAI[59]. Non è qui necessario ripercorrere la disciplina nel dettaglio; basti dire che, chiaramente, essa lascia più ampi margini di manovra nel trattamento dei dati personali, se paragonata al regime "ordinario" di cui alla direttiva 95/46/CE. Ad es., per quanto riguarda i dati sensibili (dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati relativi alla salute e alla vita sessuale), non si richiede il consenso esplicito, ma solo che il trattamento sia strettamente necessario e che la legislazione nazionale preveda adeguate garanzie (art. 6). Ad ogni modo, l'EDPS auspica che le LEAs "*only use an RPAS in the framework of a specific investigation when their use is considered necessary and where no other less intrusive mean would achieve the same purpose*".

Se il *law enforcement* rimane per molti versi una zona grigia fra Stati e Unione, i servizi di *intelligence* pertengono certamente alle competenze domestiche. Ora, nonostante la chiara esclusione di cui all'art. 3 della direttiva 95/46, e per quanto – a mente dell'art. 4, comma 2, del Trattato sull'Unione Europea (TUE) – *"la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro"*, l'EDPS fa propria un'interpretazione sottile proposta dalla Corte di Giustizia nel caso *Rundfunk* del 2003[60]. Ora, come è noto, ai sensi dell'art. 8 , comma 2 CEDU, un'ingerenza nel diritto al rispetto della vita privata è ammessa se è prevista dalla legge e se costituisce un provvedimento che, in una società democratica, è necessario alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine ed alla prevenzione delle infrazioni penali, alla tutela della salute o della morale, alla tutela dei diritti e delle libertà altrui. E però la Corte, in un'inversione logica se non altro discutibile, ignora i dati normativi testuali qui richiamati, e afferma che, comunque, prima di valutare il ricorrere delle ipotesi di interferenze lecite *ex* art. 8, comma 2 CEDU, occorrerebbe preliminarmente accertare se vi sia stata o meno un'ingerenza nella vita privata (e solo successivamente, eventualmente, se tale ingerenza sia giustificata alla luce dell'art. 8, comma 2, CEDU). L'art. 8, infatti, imporrebbe in ogni caso che le misure intese alle finalità richiamate debbano essere necessarie e – secondo la Corte – proporzionali. Anche ammesso che la necessità non debba essere valutata dagli esecutivi interni, in ogni caso lo *screening* di proporzionalità è una superfetazione giurisprudenziale derivante da un'interpretazione creativa dell'art. 13 della direttiva 95/46/CE (che tace sul punto) e dall'ignoranza del tenore testuale dell'art 3, comma 2, e delle altre disposizioni sopra richiamate. In ogni caso, i responsabili dei SAPR tengano a mente i filtri di necessità e

applicabilità territoriale anche qualora i beni e i servizi non siano offerti dietro corrispettivo e, per quanto riguarda il monitoraggio, esso ha rilievo solo se l'attività monitorata si svolge all'interno dell'Unione.

[56] Corte di Giustizia, grande sez., 16-12-2008, C-73/07, *Tietosuojavaltuutettu c Satakunnan Markkinapörssi Oy e Satamedia Oy*, in *Racc.*, 2008 I-9831.

[57] Non è un caso che non constino precedenti della Corte di Giustizia, e che l'unico caso sembri essere stato affrontato dalla Corte Europea dei Diritti dell'Uomo, grande sez., 04-12-2008, app. 30562/04 e 30566/04, *S. e Marper c. Regno Unito*, in *Reports of Judgments and Decisions 2008*: caso *sui generis*, perché si trattava della conservazione di campioni di DNA di soggetti arrestati, ma poi liberati o comunque dichiarati innocenti. Il punto, quindi – più che la privacy in sè –, sembra essere la perpetrazione di attivita' successive al vero e proprio *law enforcement*, e, illegali (o, comunque, divenute illegali).

[58] Ci si limita, qui, al diritto propriamente unionista, ma v. la Convenzione del Consiglio d'Europa n. 108, e la Raccomandazione n. R(87)15 del Comitato dei Ministri degli Stati Membri.

[59] Decisione Quadro 2008/977/GAI del Consiglio del 27-11-2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale.

[60] Corte di Giustizia, 20-05-2003, C-465/00, C-138/01 e C-139/01, *Rechnungshof c Österreichischer Rundfunk e a. e Christa Neukomm e Joseph Lauermann c Österreichischer Rundfunk*, in *Racc.*, 2003 I-4989.

proporzionalità di cui si è detto.

Infine, alcune raccomandazioni specifiche. La Commissione non è competente per SAPR sotto i 150 chilogrammi, ma le regole su privacy e protezione dei dati personali si applicano comunque, e di ciò i responsabili dei SAPR devono essere resi consapevoli, specialmente a fini di implementazione *by design*. Per quel che concerne la consapevolezza degli utilizzatori finali, si propone l'inserimento di *"privacy notices"* nei pacchi con cui si vendono i droni di peso inferiore a 150 chilogrammi.

Un secondo punto è l'alimentazione del dibattito pubblico, rispetto alla quale l'EDPS loda il lavoro di alcune *Data Protection Authorities* (DPAs), riferendosi a un lavoro di revisione dell'*Information Commissioner's Office* (ICO, Regno Unito), che – ai tempi dell'opinione dell'EDPS – stava portando avanti una consultazione pubblica per emendare il *Code of Conduct* sulle CCTV (*Closed Circuit Televisions*), in modo tale da includervi i SAPR. Frattanto, la consultazione è terminata e – a maggio 2015 – è stato pubblicato il *"Code of practice for surveillance cameras and personal information*"[61], che si applica a tecnologie eterogenee, quali: *Automatic Number Plate Recognition* (ANPR); *body worn video* (BWV); *unmanned aerial systems* (UAS); nonché non meglio identificati *"other systems that capture information of identifiable individuals or information relating to individuals"*.

E' apprezzabile, poi, che – con riguardo alla privacy *by design* – l'EDPS ponga l'accento sulla necessità di tenere in considerazione le particolarità dei SAPR (per quanto, come si vedrà, i problemi sollevati sono comuni a buona parte del più ampio universo dell'*Internet of Things*). Infatti, i SAPR consistono in un veicolo aereo, il vettore, ed in un c.d. *payload* (letteralmente, "carico"), che può essere un sistema per il trattamento dei dati; le due componenti possono essere prodotte da soggetti diversi, i quali possono non essere consapevoli della futura combinazione, né delle sua potenzialità. La soluzione proposta, però, non persuade. Infatti, si impongono comunque a tutti i soggetti coinvolti implementazioni *by design*[62] qualora sia prevedibile un uso non *privacy-friendly* (come se il produttore della singola componente potesse effettivamente effettuare certe previsioni) e, "*when the combination done by the user and the modalities of use of the RPAS result in privacy-intrusive acts, the final responsibility will be with the user*". Tant'è.

Occorre, infine, ricordare, l'opinione dell'*Article 29 Working Party* (WP29)[63] "*on Privacy and Data Protection Issues relating to the Utilisation of Drones*"[64].

I primi soggetti a cui tale opinione si rivolge sono policy makers e autorità di regolazione del settore. Ad essi si raccomanda che l'apertura del mercato dell'aviazione all'uso civile dei droni sia accompagnato, fra l'altro: dalla subordinazione delle autorizzazioni a dichiarazioni di aver preso in considerazione i requisiti di protezione dei dati personali (come qui proposto); dal coinvolgimento degli *stakeholders* nello sviluppo di *Data Protection Impact Assesments* (DPIA) e – più in generale – di un quadro giuridico che tenga conto non solo della sicurezza dei voli, ma anche del rispetto dei diritti fondamentali (prevedendo, ad es., *no-fly zones*); dall'aggiornamento delle policy sui droni, al fine di armonizzarle e tener conto delle operazioni transfrontaliere; dall'obbligo di commerciare piccoli droni accompagnati da adeguate informazioni sulla privacy (contenute, ad es., nel manuale operativo)[65].

Produttori e operatori, fra l'altro, sono a loro volta chiamati: ad incorporare opzioni di privacy *by design* e *by default* (coinvolgendo nel design anche un *Data Protection Officer*); ad adottare codici di condotta accompagnati da sanzioni (sembrerebbe, secondo un modello di co-regolazione *sui generis*[66]); a rendere il drone identificabile (ad es., tramite l'emissione

---

[61] Information Commissioner's Office, *In the picture: A data protection code of practice for surveillance cameras and personal information*, v. 1.1., 21-05-2015, disponibile all'indirizzo https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf. Si segnala che l'ICO, nella pagina FAQ sull'uso dei droni, risponde alla domanda incipitaria "*Are drones covered by the Data Protection Act (DPA)?*" col dire che "*[i]f a drone has a camera, its use has the potential to be covered by the DPA*", ciò che appare invero restrittivo, dato che anche altre tecnologie possono consentire la raccolta di dati personali.

[62] Fra queste, l'utilizzo di sensori poco intrusivi (videocamere a bassa definizione), *data retention by design* (cancellazione periodica dei dati), automatico oscuramento dei volti, registrazione non continua bensì solo su iniziativa dell'utente, impostazioni di *privacy by default.*

[63] Si tratta di un gruppo di lavoro istituito *ex* art. 29, Dir. 1995/46, ed è un organo europeo indipendente con funzioni consultive in materia di protezione dei dati e privacy.

[64] 29WP, *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones*, 16-06-2015, disponibile all'indirizzo http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf.

[65] Come visto, l'EDPS consiglia invece un'apposita *privacy notice*. L'opzione suggerita da WP29 rischia che le informazioni sulla privacy si perdano nel mare delle istruzioni, ma concettualmente è più appropriata, perché il rispetto delle norme *de quibus* dovrebbero costituire parte integrante dei modi in cui si usano i droni.

[66] Il codice di condotta è, per la verità, il paradigma dell'autoregolazione, ma – poiché qui lo si accompagna a sanzioni – è dato di ipotizzare una forma di collaborazione pubblico-privato (la quale, di norma, si esplica – quando si parla di co-regolazione – nella fissazione di una

di segnali wireless o con colori accesi)[67].

Si conclude con la raccolta dei dati per finalità di *law enforcement*, rispetto alla quale non si ripeteranno – per ragioni di sintesi – le considerazioni brevemente svolte *supra*. Nel fare uso dei droni a detti fini, le LEAs dovrebbero, *inter alia*: rispettare i principi di necessità, proporzionalità, e minimizzazione; rispettare la severa fissazione del periodo di conservazione dei dati; informare i soggetti del trattamento (alquanto improbabile, visto il contesto; infatti, si precisa "*as far as possible*"); far sì che il monitoraggio continuo sia limitato ad indagini assistite da mandato; per quanto riguarda l'esecuzione automatica delle decisioni, assicurare che i dati trattati dal drone siano sottoposti a controllo da parte di un operatore umano; sottoporsi ad un controllo giudiziale.

La disciplina di riferimento in Italia, quindi, è da considerarsi quella contenuta nel già menzionato regolamento ENAC. In particolare, l'art. 34, disposizione di chiusura della sez. VI ("Disposizioni Generali per i Sistemi Aeromobili a Pilotaggio Remoto") e rubricato "*Protezione dei dati e privacy*", si candida a costituire modello per le future legislazioni che dovessero, come si auspica, svilupparsi in materia. La formulazione è diversa dall'omologa disposizione della direttiva macchine, posto che si prevede che: i) ove le operazioni svolte attraverso un SAPR comportino (o possano comportare) un trattamento di dati personali, tale circostanza dev'essere menzionata nella documentazione sottoposta ai fini del rilascio della pertinente autorizzazione; ii) il trattamento dei dati personali deve essere effettuato in ogni caso nel rispetto del codice in materia di protezione dei dati personali[68], con particolare riguardo al ricorso a modalità che permettano di identificare l'interessato solo in caso di necessità ai sensi dell'art. 3 di detto codice; iii) il trattamento deve rispettare, altresì, le misure e gli accorgimenti a garanzia dell'interessato prescritti dal Garante per la protezione dei dati personali.

Quantunque sia una disposizione quasi integralmente di mero rinvio alla disciplina comune sulla protezione dei dati personali, va apprezzata l'esplicitazione – auspicata sopra *de iure condendo* con riferimento alla direttiva macchine – della necessità che la documentazione richiesta ai fini dell'autorizzazione dia conto dei problemi sollevati dal drone in materia di *privacy*. Degna di attenzione, poi, la sensibilità del legislatore che coglie, con la seconda regola, il *trend* della minimizzazione della raccolta dei dati[69]. Infine, il rinvio alla determinazioni del Garante si potrà rivelare uno strumento assai agile, in considerazione delle semplici procedure decisionali dell'Autorità, che le consentono di intervenire rapidamente sui problemi di privacy via via emergenti (ciò che ancora non si è avuto nella materia d'interesse[70]). Sarebbe auspicabile che il rinvio non fosse limitato al nostro Garante, ma fosse esteso all'EDPS e al 29WP.

Per concludere, può essere utile **qualche cenno comparatistico**.

Presso l'**ordinamento statunitense**, come è noto, per lungo tempo la protezione della *privacy* di cui al Quarto Emendamento è stata ricondotta al *law of trespass*, con la conseguenza, fra l'altro, che non si sarebbe potuta lamentare infrazione alcuna allorquando non vi fosse stata una violazione della proprietà in senso fisico. Cambiando radicalmente il precedente orientamento, la *Supreme Court* separò la violazione dei diritti della persona di cui al Quarto Emendamento dal

---

quadro generale da parte del legislatore o del regolatore, quadro che viene specificato poi dagli attori privati del settore considerato). Ciò a meno che le sanzioni non vengano intese molto latamente come inclusive, ad es., dell'esclusione da un'associazione di categoria, nel qual caso si ricadrebbe di diritto nell'autoregolazione.

67 Si noti che siffatti droni potrebbero non essere particolarmente appetibili, considerato che la non visibilità è proprio una caratteristica ricercata da potenziali acquirenti.

68 Con un chiaro errore materiale, la prima edizione del regolamento rinviava non al D. Lgs. n. 196/2003, bensì al *"decreto legislativo 30 giugno 2013, n. 196 e successive modificazioni"*, che non esiste.

69 Cfr., ad es., Article 29 Data Protection Working Party, *Remotely Piloted Aircraft Systems (RPAS) – Response to the Questionnaire*, 16-12-2013, § 3, là dove si osserva che "*A need for policy guidelines has been identified in order to address the practical difficulties regarding the enforcement of some data protection rules regarding the use of data processing equipment onboard RPAS, for example fair processing, information notice, data minimization and compliance with data subjects' access rights*".

70 Si rinviene, qui e là, qualche cenno incidentale ai robot, intesi – si badi bene – come *internet bots* (*software* deputati a performare specifiche funzioni in modo automatico su Internet), il più rilevante dei quali sembra: Garante Protezione Dati Personali (GPDP), par. 04-07-2013, doc. web n. 2574977 sulle "*Linee guida redatte dall'Agenzia per l'Italia Digitale ai sensi dell'art. 58, comma 2, del D. Lgs. 7 marzo 2005, n. 82 (CAD)*", introdotte affinché le Amministrazioni titolari di banche dati accessibili per via telematica predispongano apposite convenzioni – aperte all'adesione di tutte le amministrazioni interessate – volte a disciplinare le modalità di accesso ai dati da parte delle stesse amministrazioni procedenti, senza oneri a loro carico. A tenore del § 5.5.2.3 ("Istruzioni e correttezza del trattamento"), "*[i]l fruitore deve utilizzare le informazioni acquisite esclusivamente per le finalità dichiarate in convenzione, nel rispetto dei principi di pertinenza e non eccedenza, nonché di indispensabilità, per i dati sensibili e giudiziari. Il fruitore deve, altresì, garantire che non si verifichino divulgazioni, comunicazioni, cessioni a terzi, né in alcun modo riproduzioni dei dati nei casi diversi da quelli previsti dalla legge, stabilendo le condizioni per escludere il rischio di duplicazione delle basi dati realizzata anche attraverso l'utilizzo di strumenti automatizzati di interrogazione. A tal fine il fruitore si impegna ad utilizzare i sistemi di accesso ai dati in consultazione on line esclusivamente secondo le modalità con cui sono stati resi disponibili e, di conseguenza, a non estrarre i dati per via automatica e massiva (attraverso ad esempio i cosiddetti "robot") allo scopo, ad esempio, di velocizzare le attività e creare autonome banche dati non conformi alle finalità per le quali è stato autorizzato all'accesso*".

trespass[71]. Oggi, quindi, i giudici devono controllare se il cittadino appellantesi alla citata disposizione costituzionale avesse un'aspettativa di *privacy* e, in secondo luogo, se questa sia riconosciuta ragionevole dalla società. Uno dei casi in cui si ritiene che il test di ragionevolezza non si possa superare è quello in cui la tecnologia sia "*in general public use*". La giurisprudenza ha mostrato di intendere latamente questo concetto, considerando ragionevole l'uso di elicotteri e aerei per filmare campi di marijuana, quantunque non si possa a rigore sostenere che detti mezzi siano nel generale uso del pubblico[72]. Ora, anche considerato che non si può allo stato sostenere che i robot siano parte dello scenario quotidiano dei cittadini, non è scontato che attività di raccolta dati automatizzate siano vietate dalla normativa rilevante. Non è un caso che vi sia una importante corrente di pensiero dottrinale[73], con appigli giurisprudenziali[74], che sostiene che non vi sia "*search*" nel senso di cui al Quarto Emendamento quando non vi sia un essere umano che acceda all'informazione. Sarebbe pienamente legittimo, in prospettiva, l'uso di robot dotati dei più avanzati sensori per vedere di notte o attraverso superfici solide, specie qualora in grado di trasmettere l'informazione solo nel caso di oggetto o attività illeciti.

Con specifico riguardo, poi, ai robot di servizio, bisogna tenere a mente che, sebbene le attività che si svolgono nelle private abitazioni siano oggetto del più alto livello di tutela[75], qualora si affidino informazioni a terzi si perde in certa misura la relativa protezione[76]. E però, l'*Electronic Communications Privacy Act* pone delle limitazioni alla *disclosure* delle comunicazioni elettroniche, che devono essere rispettate anche dall'entità che vi abbia accesso in conseguenza della fornitura di un servizio (§ 2510, 18 U.S.C.[77]). Come è stato correttamente notato, d'altra parte, l'applicazione di questa legge al campo d'interesse dipenderà dalla nozione di "entità", di talché non si può escludere che si possa avere accesso ad alcuni dati registrati dal robot senza passare dall'*expedit* giudiziale.

Dando, in conclusione, un veloce sguardo comparatistico agli **Stati europei**, invece, basti qui notare che, nel Regno Unito, l'*Information Commissioner's Office* e la *Civil Aviation Authority* lavorano fianco a fianco in un gruppo di lavoro governativo; in Germania, la *Luftverkehrs-Ordnung* (LuftVO) – ossia il regolamento di circolazione aerea[78] – è stata emendata per includere il rispetto dei requisiti in materia di protezione dei dati come condizione che le autorità aeronautiche dei *Länder* devono valutare nel concedere permessi di volo; in Macedonia, la locale autorità dell'aviazione civile (*Агенција за цивилно воздухопловство*) sta preparando, insieme alla commissione sulla protezione dei dati (*Дирекција за заштита на лични податоци*), un *rulebook* per usare i sistemi aerei a pilotaggio remoto; a Malta, poi, il Direttorato dell'aviazione civile collabora assiduamente con l'*Office of the Information and Data Protection Commissioner on data protection matters*; l'Italia, dal canto suo, è lodata per aver inserito nel regolamento ENAC un'apposita norma sulla riservatezza, grazie anche al contributo del nostro Garante. Invece, bisogna denunciare che "*no contacts with CAAs* [Civil Aviation Authorities] *have yet been established by the DPAs [Data Protection Authorities] in Austria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary,*

---

[71] Vero e proprio *leading case* è *Killo v. United States*, 533 U.S. 27 (2001).

[72] V. *California v. Ciraolo*, 476 U.S. 207 (1986) e *Florida v. Riley*, 488 U.S. 445 (1989).

[73] Cfr., fra gli altri, O. S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, in *Michigan Law Review*, 2004, 801.

[74] Si pensi al caso *United States v. Place*, 462 U.S. 696 (1983), in cui si statuisce che non è necessario un mandato affinché un cane annusi una borsa, considerato che l'ufficiale di polizia non vi ha accesso diretto.

[75] Cfr. *Silverman v. United States*, 365 U.S. 505 (1961).

[76] Il riferimento è *United States v. Miller*, 307 U.S. 174 (1939).

[77] Vedere anche il § 2511, co. 3, a tenore del quale "*(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient. (b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication— (i) as otherwise authorized in section 2511 (2)(a) or 2517 of this title; (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication; (iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency*".

[78] La LuftVO, ufficialmente "*Luftverkehrs-Ordnung vom 10. August 1963 (BGBl. I S. 652), die zuletzt durch Artikel 3 des Gesetzes vom 8. Mai 2012 (BGBl. I S. 1032) geändert worden ist*", contiene regole di dettaglio concernenti tutti i piloti e le compagnie aeree che volino in Germania e costituisce il complemento del *Luftverkehrsgesetz* (LuftVG,"*Luftverkehrsgesetz vom 1. August 1922 (RGBl. 1922 I S. 681), das zuletzt durch Artikel 2 Absatz 175 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist*", che può essere considerato il codice tedesco della navigazione aerea. Cfr. C. Kornmeier, *Der Einsatz von Drohnen zur Bildaufnahme: eine luftverkehrsrechtliche und datenschutzrechtliche Betrachtung*, Münster, 2012, passim.

Lithuania, Luxembourg, Netherland, Poland, Portugal, Spain, Slovak Republic, Sweden, Slovenia"[79].

Ad eccezione del regolamento ENAC, non constano – almeno a livello europeo – normative che affrontino specificamente il tema d'interesse. Resta fermo, però, che le disposizioni della nuova disciplina europea sul trattamento dei dati personali riguardanti la valutazione d'impatto sulla protezione dei dati, i principi della privacy by design e privacy by default e le previsioni sulla certificazione delle operazioni di elaborazione dei dati assumono un rilievo non trascurabile per affrontare i problemi della riservatezza e della protezione dei dati connessi all'uso dei droni.

Allocazione delle responsabilità tra i vari soggetti coinvolti

Le considerazioni svolte sopra circa le **potenziali ricadute su privacy e trattamento di dati personali** valgono, con alcune variazioni, per tutte e tre le macro-categorie robotiche qui avute presenti: la telerobotica, i robot *courier* e i droni-multicotteri in contesto *smart city*.

I due *trial* di **telepresenza** immaginati sono l'uso a fini universitari e i robot museali. Quanto al primo, dietro il robot presente in aula v'è sempre chi è interessato all'apprendimento a distanza, il quale sovente si palesa (ad es., mediante un tablet, come in *VGo*[80]). Ora, **mentre per i dati riguardanti l'osservatore non emergono problemi di riservatezza particolarmente rilevanti (è egli stesso a decidere cosa mostrare nell'interfaccia), non si può dire lo stesso per quelli dei docenti e discenti presenti in aula. Sul punto, si possono immaginare sia soluzioni di *privacy by design*** (ad es., un saluto vocale in cui il robot trasmette un'informativa sulla *privacy*)**, sia soluzioni più tradizionali, come l'affissione di cartelli sul genere di quelli usati per segnalare la presenza di telecamere. Il discorso è analogo per i robot museali**, che sollevano ancora minori problemi, considerato che si muovono in spazi ridotti. In questo caso**, l'unico accorgimento consiste nel far sì che l'addetto al robot o, comunque, chi abbia accesso alla memoria dello stesso (e, nel caso di *cloud robotics*, al *web storage*) si impegni a non divulgare in alcun modo le informazioni per tal via apprese**.

I **robot *courier*** costituiscono una sfida già più ardua per la *privacy*: essi, infatti, si muovono in spazi ampi e complessi, sono in grado di acquisire un considerevole novero di dati anche sensibili (da sfruttare, ad es., a fini di *marketing*) e, come detto, possono riconoscere – specialmente grazie a sistemi di *face recognition* – l'utente che torni una seconda volta, sfruttando le informazioni immagazzinate per indirizzarne la volontà in modi imprevedibili. In uno **scenario di *trial* convegnistico** basterebbe, tutto sommato, **inserire un'apposita indicazione nei moduli di registrazione all'incontro**. Il discorso muta **nel caso di centri commerciali o ambienti analoghi**; in quel caso, si potrebbe anzitutto **procedere via *privacy by design*, limitando l'operatività della *face recognition* (quando non la fissazione stessa del video) alla fase in cui il potenziale cliente attiva *sua sponte* il robot**, tipicamente toccandone lo schermo o con modalità equivalenti: si può, così, salvaguardare l'immagine di quanti si incroceranno nel percorso atto a condurre il potenziale cliente alla meta desiderata. **Quanto, invece, ai dati sensibili del potenziale cliente, si potrebbe immaginare un'informativa con sistema "a spunta", tale per cui, in assenza di consenso, non si procederà all'interazione**.

Andando, poi, ai **droni-multicotteri**, è intuitivo che essi sollevino problemi di *privacy* ben maggiori dei robot di servizio, potendo essere raffigurati, con robusta semplificazione, come vere e proprie telecamere volanti, della cui esistenza (e operatività) i cittadini per lo più non sono consapevoli[81]. Come notato dall'Article 29 Data Protection Working Party, "*the increasingly powerful techniques drones may be equipped with would allow collecting personal data through high resolution image and video recordings as well as storing and, if necessary, transferring such data to the relevant ground station. Data subjects would hardly be aware of this kind of processing as it is difficult to notice RPAS, because of their small size and the altitude of operation*"[82]. Il gruppo tiene fermo che l'elaborazione di immagini, suoni e geolocalizzazioni collegati a individui identificabili, portata avanti con i droni, è in ogni caso soggetta all'applicazione delle normative europea e nazionale in materia di protezione dei dati.

Riguardo al trattamento di dati che dovesse eventualmente venire in essere durante le operazioni svolte dai droni, come detto, **specifiche disposizioni sono state esplicitamente previste all'interno dell'art. 34 del regolamento emanato**

---

79 Article 29 Data Protection Working Party, *Remotely Piloted Aircraft Systems (RPAS) – Response to the Questionnaire*, *cit.*, § 2.

80 Sul controllo del robot di telepresenza *VGo* mediante tablet v. http://www.vgocom.com/can-i-use-tablet-drive-vgo.

81 La letteratura giuridica dedicata a droni e *privacy* comincia a essere significativa, basti vedere T. T. Takahashi, *Drones and Privacy*, in *Columbia Science&Tech. L. Rev.*, 2012, 72; H. B. Farber, *Eyes in the Sky: Constitutional and Regulatory Approaches to Domestic Drone Deployment*, in *Syracuse L. Rev.*, 2014, 1; M. E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, in *California Law Review Circuit*, 2013, IV, 57 e T. G. Matiteyahu, *Drone Regulations and Fourth Amendment Rights: The Interaction of State Drone Statutes and the Reasonable Expectation of Privacy*, in *Columbia J. of L. and Social Problems*, 2014 (consultato all'indirizzo ssrn.com/abstract=2425776). Si segnala, altresì, il dibattito "*Introducing Drones in the EU Civilian Airspace*", tenutosi il 25-01-2013 a Bruxelles (nell'ambito della *6th International Conference* dell'associazione *no profit* "Computer, privacy & data protection", dal 23 al 25-01-2013 e intitolata "*Reloading Data Protection*"), indirizzato a rispondere, come prima questione, alla domanda "*What are the potential privacy implications that come along with the use of drones in the EU's civilian airspace?*".

82 Article 29 Data Protection Working Party, *Remotely Piloted Aircraft Systems (RPAS) – Response to the Questionnaire*, *cit.*, § 1. Quella in parola è la risposta elaborata da detto gruppo a un questionario commissionato dal Direttorato Generale "Impresa e Industria" della Commissione.

dall'ENAC sui mezzi aerei a pilotaggio remoto (per una disamina dell'impianto complessivo del regolamento, invece, si rinvia alla Sezione 4.6 – *Regolamento ENAC*).

4.4 Digital forensics e cyber security

(a cura di Giuseppe Vaciago)

Introduzione e principi generali

Le caratteristiche di interattività, autonomia e adattatività dei robot citate nella Sezione 1 hanno come possibile conseguenza l'imprevedibilità delle loro azioni, sia nei confronti dei programmatori e costruttori di tali agenti artificiali sia dei loro stessi proprietari. Da ciò ne consegue che **un aspetto fondamentale da considerare nel momento patologico dell'accertamento della responsabilità in caso di incidente dovuto a malfunzionamento del robot o del drone è la possibilità di ricostruire le modalità con cui esso è stato progettato e ha operato in concomitanza dell'evento**. Allo stesso modo, è opportuno non sottovalutare – al di là della rispondenza ai requisiti di sicurezza richiesti ai robot e ai droni dalla normativa comunitaria in materia (c.d. "direttiva macchine"[83]) – la sicurezza del sistema operativo o degli applicativi che gestiscono il robot o il drone, in quanto un potenziale attacco informatico a tali software potrebbe avere effetti devastanti sul funzionamento dello stesso.

Prima di entrare nel merito di queste considerazioni, tuttavia, è opportuno specificare **cosa si intenda per *digital forensics* e *cyber security***.

La maggior parte delle pubblicazioni scientifiche fino ad ora scritte in materia hanno utilizzato il sintagma "computer forensics", espressione coniata nel 1984, quando il *Federal Bureau of Investigation* (FBI) elaborò il progetto *Magnetic Media Program*, divenuto, qualche anno più tardi, *Computer Analysis and Response Team* (CART)[84].

A distanza di quasi trent'anni, Ken Zatyko, docente della John Hopkins University, è uno dei primi autori che ha preferito utilizzare il sintagma "digital forensics" in luogo di "computer forensics"[85], in quanto le analisi forensi sul dato digitale riguardano sempre di meno il personal computer e sempre di più altre tipologie di supporti (smartphone, lettori mp3, console di videogiochi, navigatori satellitari) e di risorse hardware o software distribuite in remoto (c.d. *cloud computing*), dove sono normalmente archiviati i dati utili ad un'indagine. Seguendo questa logica, non è da escludere che si possa arrivare a coniare il nuovo sintagma "robot forensics", anche se sarebbe improprio, in quanto – anche in ambito di robotica – oggetto di analisi sarà sempre il dato digitale.

Sgombrato il campo da possibili equivoci terminologici, è opportuno ripercorrere le varie definizioni di *digital forensics* che si sono susseguite negli ultimi anni, a livello nazionale e a livello statunitense.

Il National Institute for Standard and Technology (NIST) distingue **quattro fasi all'interno della *digital forensics*:** la raccolta, l'esame, l'analisi, e la presentazione, tutte riferite alla prova digitale[86].

La **raccolta** è data dall'identificazione, etichettatura, registrazione e acquisizione dei dati digitali, nel rispetto di procedure che preservino l'integrità degli stessi.

L'**esame** consiste nel processo di valutazione del dato digitale attraverso metodi automatizzati e manuali, che preservino l'integrità del dato digitale.

L'**analisi**, invece, si sostanzia nel processo di verifica dei risultati dell'esame dei dati, al fine di ottenere le risposte ai quesiti per i quali è stato raccolto ed esaminato il dato digitale stesso.

La **presentazione dei risultati** dell'analisi comprende, infine, la descrizione delle attività compiute e degli strumenti utilizzati, oltre all'eventuale elencazione delle ulteriori operazioni che sarebbero necessarie per completare l'analisi forense.

---

[83] Direttiva 2006/42/EC relativa alle macchine, recepita con D. Lgs. n. 17/2010.

[84] Il progetto CART era costituito da un gruppo di specialisti nell'indagine delle informazioni contenute negli elaboratori. Ulteriori informazioni sul team di lavoro sul progetto CART sono disponibili al seguente URL: http://www2.fbi.gov/hq/lab/org/cart.htm, e all'interno del volume *Handbook of Forensic Services*, 2007, disponibile al seguente URL: http://www.fbi.gov/about-us/lab/handbook-of-forensic-services-pdf.

[85] K. Zatiko, *Commentary: Defining digital forensics*, in Forensic Magazine, 2007, disponibile al seguente URL: . http://www.forensicmag.com/node/128.

[86] K. Kent, S. Chevalier, T. Grance, H. Dang, *Guide to integrating Forensic Techniques into Indente Response*, NIST publication, 2006, disponibile al seguente URL: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

La *digital forensics* richiede competenze specifiche che vanno al di là della mera raccolta e conservazione dei dati effettuate dall'utente finale, pretendendo, generalmente, il massimo rispetto della catena di custodia, ossia la certificazione delle varie attività di analisi della prova digitale, per assicurare la stessa non venga alterata.

Anche la dottrina italiana ha avviato un proprio filone di ricerca intorno alla definizione e ai contenuti della computer forensics, concentrandosi solo sulla parte relativa ai profili penali delle indagini telematiche. Si tratta di un lavoro ancora embrionale e soprattutto meno suffragato da una giurisprudenza consolidata, lavoro che, tuttavia, merita il massimo sostegno.

Cesare Maioli definisce la *computer forensics*[87] come "*la disciplina che studia l'insieme delle attività rivolte all'analisi e alla soluzione dei casi di criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer, o in cui il computer può rappresentare comunque un elemento di prova*".

Per quanto attiene alla ***cyber security***, merita di essere citato Eugene Spafford, docente di Computer Science della Purdue University, il quale, già nel 1989, sosteneva che "*l'unico sistema realmente sicuro è un sistema spento, affogato in un blocco di cemento, sigillato in una stanza dalle pareti schermate col piombo e protetto da guardie armate. E anche in questo caso è dubbio che possa essere sicuro*"[88].

Anche se una simile affermazione risuona di quell'enfasi molto cara agli esperti di sicurezza informatica, nella pratica si osserva un inevitabile e sempre crescente utilizzo delle rete – da parte dei robot e dei droni – al fine di condividere, in tempo reale, informazioni e istruzioni; ed il rischio a ciò collegato non può essere sottovalutato. Nel settore industriale, infatti, un attacco informatico può significare la completa distruzione di un'intera linea di prodotti o l'interruzione di una catena di montaggio, con il risultato di un danno enorme in termini economici e di produttività. Nel settore della robotica, addirittura, un attacco informatico può mettere in pericolo la vita delle persone, o anche fornire delle informazioni strategiche per la commissione di un illecito da parte di un *cyber* criminale.

Nel prossimo paragrafo, cercheremo di evidenziare come queste due materie debbano essere tenute in forte considerazione anche in assenza di una regolamentazione di settore chiara ed univoca.

Problematiche giuridiche rilevanti

Sulla scorta di quanto illustrato nella Sezione 2 della ricerca con riferimento all'esame delle tre macro-categorie di impiego (telepresenza mediante robot, robot courier e droni-multicotteri), la *cyber security* e la *digital forensics* possono e debbono rivestire un ruolo di grande rilevanza nella prevenzione e nella gestione di eventuali incidenti in grado di generare delle conseguenze giuridiche per i soggetti che, a vario titolo, hanno contribuito alla realizzazione del robot o del drone.

In caso di malfunzionamento di tali agenti artificiali, si porrà il problema di comprendere se tale comportamento anomalo sia dovuto ad un possibile attacco informatico connesso ad un aggiornamento o, più semplicemente, ad un problema di compatibilità del software. In tutti e due i casi, dovrà essere verificato se tale malfunzionamento del robot sia stato generato dalle successive implementazioni o a seguito di un "bug" di progettazione.

La *digital forensics* diventa quindi strategica per cercare di comprendere le ragioni di tale malfunzionamento, attraverso il recupero e la cristallizzazione della prova digitale.

Fino ad ora, tuttavia, la robotica si è rivolta al mondo della digital forensics come possibile opportunità di evoluzione di tale seconda disciplina, e non come oggetto di studio. Sono, infatti, numerosi i casi in cui vengono proposte soluzioni di robotica per migliorare e automatizzare i processi di *digital forensics*[89].

È sicuramente necessario un diverso approccio, in quanto la complessità e la imprevedibilità delle azioni dei robot impongono una diversa riflessione sia a livello tecnico che a livello giuridico in tema di *digital forensics*.

Sotto questo profilo, rilevano due aspetti di particolare rilievo: **da un lato, deve essere possibile ricostruire con esattezza i processi compiuti dal robot prima di un evento imprevisto, attraverso una corretta ed adeguata memorizzazione dei file di *log* di sistema; dall'altro, ogni attività di analisi successiva all'eventuale incidente deve essere certificata attraverso l'utilizzazione della funzione di *hash***. Tale funzione opera in un solo senso (ossia non può essere invertita) e consente la trasformazione di un documento di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata; tale stringa rappresenta una sorta di "impronta digitale" del testo in chiaro, ed è detta valore di *hash* o *Message Digest*. Se il dato digitale fosse alterato anche in minima parte, cambierebbe di conseguenza anche l'impronta. In altre parole, calcolando e registrando l'impronta, e successivamente ricalcolandola, è possibile dimostrare al di là di ogni dubbio se i contenuti del file, oppure del supporto, abbiano subito o meno modifiche, anche solo accidentali. Pertanto, la registrazione e la ripetizione costante del calcolo degli *hash* sui reperti sequestrati costituisce l'unico metodo scientificamente valido per garantire l'integrità e la

---

87 C. Maioli, *introduzione all'informatica forense, in la sicurezza preventiva della comunicazione,* a cura di P. Pozzi, F. Angeli, Torino, disponibile al seguente URL: http://www.jus.unitn.it/users/dinicola/criminologia-ca/topics/materiale/dispensa_4_1.PDF.

88 E. Spafford, citato in *Computer Recreations: Of Worms, Viruses and Core War*, a cura di A. K. Dewdney in *Scientific American*, March 1989.

89 I. Ray, *Remote Upload of Evidence over Mobile ad hoc Network*, in *Advances in Digital Forensics II*, a cura di M S. Olivier, S. Shenoi, Springer, 2006.

catena di custodia dei reperti.

Ove non fossero adottate le procedure per garantire una corretta "catena di custodia" nella fase successiva all'incidente, i dati informatici contenuti nel supporto non avranno più i requisiti di certezza, genuinità e paternità. È, quindi, necessario avere un'elevata conoscenza informatica e disporre di una strumentazione tecnica adeguata, e pianificare correttamente le attività di indagine da compiere, definendo in modo circostanziato gli obiettivi, il flusso di lavoro e le varie fasi.

Oltre al necessario rispetto delle procedure di *digital forensics*, **devono essere considerati i profili relativi alla *cyber security***, in quanto l'estrema rapidità con cui in questi ultimi anni la robotica si è sviluppata non ha consentito di valutare adeguatamente sia il fenomeno della criminalità informatica (che potrebbe sfruttare le vulnerabilità dei sistemi operativi dei robot per finalità illecite), sia quello dei movimenti hacker (che potrebbero opporsi alla robotica in quanto "colpevole" di rimpiazzare il "lavoro umano" in molti settori[90]).

Per portare alcuni esempi concreti, nel 2013 la DARPA (*Defense Advanced Research Projects Agency*) ha finanziato un progetto di due ricercatori – Charlie Miller e Chris Valasek, entrambi esperti in *cyber security* – che aveva l'obiettivo di dimostrare la vulnerabilità dei vari software che gestiscono da remoto un autoveicolo, al fine di sensibilizzare l'industria del settore *automotive* a sviluppare software più sicuri[91]. I due ricercatori hanno sfruttato il fatto che sempre più spesso i veicoli moderni siano connessi in rete così da aumentare la loro gamma di servizi. Tale scelta, ormai obbligata nel caso della robotica, rende sicuramente più semplice per un *cyber* criminale sferrare un attacco, che può avere effetti non particolarmente rilevanti – come, ad esempio, l'azionamento del clacson o il controllo del sistema di climatizzazione – oppure avere effetti decisamente più seri da un punto di vista di sicurezza – come quello di bloccare il funzionamento del freno o di acquisire il controllo del volante.

In ambito militare, i rischi sono già noti da tempo, soprattutto se si considerano gli investimenti in termini di robotica che molti governi stanno facendo in tutto il mondo. Il 4 dicembre del 2012, il Governo iraniano ha ufficialmente dichiarato di aver preso possesso di un drone militare statunitense (Sentinel RQ-170) al confine tra Iran e Afghanistan[92]. Le perfette condizioni del velivolo dopo la sua "cattura" hanno fatto supporre agli esperti del settore che fosse avvenuto un attacco informatico da parte del Governo iraniano. Attraverso questa operazione militare, l'Iran ha quindi potuto ottenere informazioni sensibili sulle altre missioni americane in corso e, soprattutto, comprendere il funzionamento del drone in modo da poter controllare i droni americani in caso di attacco.

Per tornare all'esame delle tre macro-categorie, si pensi, per quanto attiene il caso della **telepresenza mediante robot**, al caso in cui il sistema operativo dell'agente artificiale sia "aggiornato" con applicazioni informatiche che gli consentano di svolgere attività non ipotizzate al momento della sua progettazione. In caso di incidente, diventerà **importante comprendere se il malfunzionamento sia dovuto alla mancata compatibilità tra il sistema operativo e l'applicazione o se invece la stessa applicazione non nasconda in realtà un malware in grado di generare un comportamento anomalo del robot**.

Per quanto concerne, poi, i **robot courier**, si immagini il caso in cui uno di essi debba trasportare un determinato oggetto in un ambiente particolarmente impervio. Il robot, oltre a dover essere solido per resistere agli eventuali impatti, dovrà essere particolarmente adattivo per evitare gli ostacoli, e autonomo per poter gestire situazioni di pericolo senza bisogno di attendere istruzioni dall'esterno. Le caratteristiche di adattatività e autonomia, due delle tre citate nell'introduzione, contrastano con i principi di base di sicurezza informatica, in quanto rendono meno "controllabile" il robot e lo espongono a potenziali attacchi. È evidente, quindi, che **nella fase di progettazione debbano essere adeguatamente bilanciate le esigenze di funzionalità del robot con quelle di sicurezza e non attaccabilità del suo sistema operativo**[93].

Infine, per quanto attiene ai **droni**, Todd Humphrey, ricercatore dell'Università del Texas, ha dimostrato che, spendendo circa 1.000 dollari, si è in grado di effettuare un *"GPS spoofing"* di un drone civile, prendendo così il pieno controllo del velivolo[94]. Attraverso tale tecnica di attacco, è possibile generare un segnale GPS fasullo, in grado di far cadere in errore anche

---

[90] Per un approfondimento su tale teoria si veda: B. Sheppard and T. Thompson, *Cyber Security for Robots: Scenarios for 2030. Cyber-Enhanced Well-Being or Artificial Retardation*?, *Institute for Alternative Futures*, 2014, Report disponibile al seguente URL: http://www.roboticsbusinessreview.com/pdfs/Cyber_Security_for_Robots_Scenarios_IAF_5_Feb_2014_(1).pdf.

[91] C. Miller and C. Valasek, *Adventures in Automotive Networks and Control Units*, 2013. Report disponibile al seguente URL: http://illmatics.com/car_hacking.pdf.

[92] Per un approfondimento si consiglia il seguente report dell'InfoSec Institute, *Hacking Drones … Overview of the Main Threats*, disponibile al seguente URL: http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/.

[93] W. M. Shen, *Robotics Research for Cybersecurity*, Polymorphic Robotics Laboratory, University of Southern California, 2012.

[94] T. Humphrey, *Statement on the vulnerability of Civil Unmanned Aerial Vehicles and other systems to civil GPS spoofing*, Submitted to

i sistemi di navigazione più evoluti, che utilizzano il segnale "malevolo" per le triangolazioni e vengono indirizzati verso la destinazione voluta dall'attaccante. Alle medesime conclusioni è arrivata anche Missy Cummings, professoressa di aeronautica e astronautica del MIT[95].

Nel 2014 tali speculazioni possono apparire esagerate, ma si consideri che alcuni studi prevedono che, entro il 2030, ogni famiglia sarà dotata di un robot, e che gli investimenti previsti nel settore della robotica entro il 2020 sono stimati in 100 miliardi di dollari[96]. Questi dati non possono non far riflettere sull'**importanza di prevedere sistemi adeguati per proteggere il robot o il drone da attacchi informatici**.

D'altro canto, però, **le rigide procedure previste dalla *digital forensics* e dalla cyber security corrono il rischio di violare i diritti fondamentali dell'individuo**. Le attività di memorizzazione, analisi e monitoraggio dei processi di funzionamento di un agente artificiale consentono di accumulare un volume di dati in grado di consentire il controllo, il tracciamento e la profilazione dell'utilizzatore. Per questa ragione, è di fondamentale importanza un **corretto bilanciamento di interessi tra le esigenze di sicurezza e funzionalità del robot e quelle, costituzionalmente protette, del rispetto della privacy e della tutela dei dati personali dei loro utilizzatori**. Sotto questo profilo va citata l'Opinione 01/2015 dell'*Article 29 Working Party* – relativa ai problemi di privacy legati all'utilizzo dei droni –, che insiste molto su un approccio orientato alla *"privacy by design"* e *"by default"*[97].

Normativa di riferimento applicabile

Come già anticipato nel precedente paragrafo, per quanto attiene alla *digital forensics* **non esiste, a livello nazionale, una chiara normativa di riferimento**, anche se la legge 48/2008 di ratifica della Convenzione di Budapest sul *cybercrime* ha modificato alcuni articoli del codice di procedura penale, includendo – all'interno del titolo relativo ai mezzi di ricerca delle prova – l'obbligo di rispettare i principi fondamentali della *digital forensics*.

Tuttavia, ai fini della presente ricerca, rivestono una fondamentale importanza le ***best practices* stilate a livello internazionale da varie organizzazioni**. Tra le molte redatte in questi anni, le più importanti sono indubbiamente le linee guida della *International Organization on Computer Evidence* (IOCE) del 1995, quelle della *Internet Engineering Task Force* (IETF) del 2002 – che hanno costituito lo standard RFC 3227 in tema di raccolta della prova digitale – e quelle del *Scientific Working Group on Digital Evidence* (SWGDE) del 2013[98]. Tali documenti contengono tutte le regole e le procedure che devono essere rispettate nell'acquisizione, catalogazione ed analisi della prova digitale.

Un capitolo a parte è costituito dalle **norme ISO 27037** in tema di identificazione, raccolta, acquisizione e conservazione della prova digitale[99]. Tale documento, pur non contenendo alcun specifico riferimento alla robotica, è uno standard di particolare rilevanza e garantisce, se correttamente applicato, la possibilità di ottenere una certificazione del rispetto delle procedure previste dalla *digital forensics*.

Come già evidenziato, le sopracitate procedure sono di fondamentale importanza per garantire la corretta acquisizione della prova digitale in caso di incidente o di altra contestazione di natura giudiziaria. Tuttavia, tali procedure non possono soltanto essere prese in considerazione dopo che l'evento si è verificato, perché alcune di esse, come ad esempio la conservazione dei file di *log*, impongono un'attività precedente di pianificazione, da effettuarsi nella fase di implementazione del sistema operativo e degli applicativi del robot o del drone.

---

the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security, 18 luglio 2012. Disponibile al seguente URL: http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Humphreys.pdf.

95 BBC News, *Why everyone may have a personal air vehicle*, articolo pubblicato il 31 ottobre 2013 e disponibile al seguente URL: http://www.bbc.com/future/story/20131031-a-flying-car-for-everyone.

96 New York Times, *German Maker of Robots Gains as Chinese Wages Rise*, articolo pubblicato il 13 aprile 2012 e disponibile al seguente URL: http://www.nytimes.com/2012/04/14/business/global/kuka-german-maker-of-robots-will-expand-in-china.html?_r=1&.

97 Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones del 16 giugno 2015, disponibile al seguente URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf.

98 Internet Engineering Task Force (IETF), *Guidelines for Evidence Collection and Archiving (RFC 3227)*, 2002, redatte da D. Brezinski e T. Killalea e disponibili al seguente URL: https://www.ietf.org/rfc/rfc3227.txt; Scientific Working Group on Digital Evidence (SWGDE), *Best Practices for Computer Forensics, Version 3.0, 2013*, disponibile al seguente URL: https://swgde.org/documents/Current%20Documents/2013-09-14%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20V3-0. Per ulteriori approfondimenti si vedano anche le *best practices* redatte dalla International Association of Chiefs of Police nel 2006, dal Department of Justice del Governo americano nel 2008 e quelle previste dal National Institute of Standards and Technology nel 2014.

99 ISO/IEC 27037:2012, *Guidelines for identification, collection, acquisition, and preservation of digital evidence*, 2012. Un estratto di tale norme è presente al seguente URL: http://www.iso27001security.com/html/27037.html.

Proprio sotto il profilo della conservazione dei dati, si osserva – dalla tabella presente nella Sezione 2 – che **molte componenti del robot adottato come modello non conservano i dati di sistema**. Tra queste rilevano in modo particolare il *laser scanner*, il *bumper* e i sensori per il rilevamento degli ostacoli, il GPS per la determinazione della posizione dell'apparato e il sensore inerziale per la determinazione dei movimenti del robot. **Se da un lato è condivisibile tale scelta, in quanto rispettosa della privacy dell'utilizzatore del robot, è altresì da considerare che in questo modo si perde l'opportunità di raccogliere delle informazioni particolarmente utili in caso di eventi patologici**.

Per quanto riguarda la sicurezza del sistema operativo e degli applicativi che gestiscono il robot o il drone, è possibile identificare una normativa di riferimento, anche se va detto che tale regolamentazione ha interessato maggiormente l'ambito della protezione delle infrastrutture critiche che la materia oggetto della presente ricerca.

Negli ultimi anni, il Parlamento Europeo e il Consiglio d'Europa, prima con la **decisione quadro 2005/222/GAI** e successivamente con la **direttiva 2013/40/UE** relativa agli attacchi contro i sistemi di informazione[100], hanno iniziato a delineare un quadro normativo di riferimento. Il 15 agosto 2015 è entrata in vigore la legge 114/2015 di delegazione europea 2014, che demanda al Governo il recepimento anche di tale Direttiva che avrebbe dovuto entrare in vigore entro il 4 settembre 2015.

Obiettivo della direttiva è proprio quello di uniformare il diritto penale degli Stati membri nel settore degli attacchi contro i sistemi di informazione, stabilendo norme minime relative alla definizione dei reati e delle sanzioni rilevanti, e migliorando la cooperazione fra le autorità competenti, tra cui la polizia e gli altri servizi specializzati degli Stati membri incaricati dell'applicazione della legge, nonché le competenti agenzie e gli organismi specializzati dell'Unione, come Eurojust, Europol e l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA).

Più specificamente, la direttiva 2013/40/UE introduce le fattispecie di reato di accesso illecito ai sistemi di informazione, di interferenza illecita relativamente ai sistemi, e di interferenza illecita relativamente ai dati. Le ultime due riguardano gli atti compiuti per ostacolare gravemente o interrompere il funzionamento di un sistema di informazione mediante l'immissione di dati informatici, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di tali dati. È stata introdotta, inoltre, una specifica disposizione normativa che vieta la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o la messa a disposizione di strumenti hardware o software in grado di compiere gli illeciti sopradescritti.

A livello nazionale, due sono le normative di interesse per quanto riguarda la *cyber security*. La prima è la **legge 547/1993, modificata con la legge 48/08 di ratifica della Convenzione Cybercrime**. Questa legge aveva da tempo previsto alcune delle fattispecie poi menzionate nella direttiva 2013/40/UE e, più specificamente, il reato di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, l'accesso abusivo a sistema telematico, e il danneggiamento informatico. Tali fattispecie hanno trovato una scarsa applicazione da parte della giurisprudenza, ma hanno sicuramente il pregio di aver fornito una pronta risposta sanzionatoria agli illeciti connessi all'utilizzo delle nuove tecnologie, che coinvolgono anche il settore della robotica.

La seconda normativa da prendere in considerazione è il **codice privacy**. Tale normativa individua preventivamente le misure di sicurezza che devono rispettare i parametri individuati nel codice privacy (articoli 33, 34, 35 e 36) e nel Disciplinare Tecnico (Allegato B del codice privacy). **L'utilizzo di sistemi di *cloud robotics* ha come possibile conseguenza che il fornitore del servizio assuma il ruolo di co-titolare del trattamento dei dati** e, conseguentemente, abbia l'obbligo di adottare tutte quelle misure organizzative, tecniche, informatiche, logistiche e procedurali volte a ridurre al minimo i rischi di distruzione o perdita dei dati, l'accesso non autorizzato, il trattamento non consentito o non conforme alle finalità della raccolta, la modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole. L'eventuale violazione delle misure di sicurezza può comportare una responsabilità penale (art. 169 del codice privacy) con arresto fino a due anni, in caso di violazione delle misure minime (assenza di sistemi di autorizzazione e autenticazione o di sistemi di protezione da malware), o una responsabilità civile (art. 15 del codice privacy) qualora non siano adottate misure idonee di protezione. Tali ultime misure non sono state tipizzate dal legislatore, ma rientrano nella scelta che il titolare deve compiere sulla base della natura dei dati trattati, delle caratteristiche del trattamento e dello stato dell'arte e della tecnica. Nel caso della responsabilità civile, è poi prevista una presunzione di colpa a carico del responsabile del danno: al titolare spetta l'onere della prova di aver adottato tutte le misure possibili per evitare il danno, mentre il danneggiato deve solo dimostrare l'esistenza del danno.

In definitiva, se è sicuramente importante la sicurezza "fisica" del robot attraverso il rispetto delle normative nazionali e comunitarie in materia (c.d. "direttiva macchine"), lo è altrettanto la sicurezza informatica del sistema operativo che gestisce il

[100] Direttiva 2013/40/UE del Parlamento Europeo e del Consiglio del 12 agosto 2013 relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio.

robot o il drone.

Per questa ragione, gli **standard ISO 27001**[101] in materia di sicurezza informatica costituiscono una certificazione quasi imprescindibile per chi voglia investire nel settore della robotica nel prossimo futuro.

Allocazione delle responsabilità tra i vari soggetti coinvolti

Come già evidenziato nella Sezione 4.1, i soggetti che possono essere, a vario titolo, responsabili in caso di incidente di un robot o di un drone sono i seguenti:

a) il produttore di una o più componenti del robot o del drone;
b) l'assemblatore di tali componenti;
c) il fornitore del servizio cloud cui il robot o il drone può connettersi per aggiornare e migliorare le proprie prestazioni;
d) lo sviluppatore di applicazioni per il robot o il drone;
e) l'utente stesso, in caso di un utilizzo improprio del robot o del drone.

Rimandando ai paragrafi precedenti le valutazioni in ordine ai profili generali di responsabilità civile e penale, è utile comprendere **quale possibile allocazione di responsabilità possa esserci nel caso in cui il robot o il drone subisca un cyber attacco da cui derivi un incidente, o anche solo un malfunzionamento**.

Innazitutto, l'utilizzo di sistemi di *cloud robotics* potrebbe aumentare il rischio di una responsabilità a carico del gestore del servizio, il quale – in caso di mancata adozione delle misure di sicurezza previste dal codice privacy, descritte nel precedente paragrafo – potrebbe incorrere in una sanzione di natura penale o in una richiesta di risarcimento da parte del danneggiato.

Allo stesso modo, anche lo sviluppatore di applicazioni per il robot o per il drone dovrà sempre tenere in grande considerazione i profili di sicurezza, perché, qualora attraverso una sua applicazione fosse possibile perpetrare un attacco informatico, sarebbe possibile far ricadere su di lui la responsabilità dell'evento dannoso o del malfunzionamento.

Con un minor grado di rischio, anche gli altri soggetti sopra elencati (produttore, assemblatore e utente), possono essere responsabili a vario titolo in caso di malfunzionamento del robot o del drone. Si immagini il caso in cui l'utente decida di modificare alcune impostazioni di sicurezza del sistema operativo per poter installare determinati applicativi: in questo caso, non si può sicuramente escludere un suo contributo causale nell'eventuale incidente che potrebbe avere luogo a causa di tali modifiche.

Diverso è il discorso per quanto attiene la *digital forensics*, la quale, intervenendo dopo che l'evento dannoso si è verificato, non può comportare delle responsabilità per i soggetti che interagiscono con il robot o con il drone. Tuttavia, è interessante osservare come l'utilizzo di servizi cloud potrebbe rendere problematica l'attività di analisi forense del dato digitale, in quanto tale attività è stata tradizionalmente concepita per essere effettuata su di un supporto fisico, mentre nel caso della *cloud robotics* dovrà necessariamente essere compiuta su *cloud server* potenzialmente dislocati fuori dal territorio nazionale[102].

Infine, va considerato che, in caso di **incidente, l'utente potrebbe essere in grado di alterare significativamente la prova** digitale, qualora la stessa non sia residente nei cloud server. Per questa ragione, **sarebbe interessante ipotizzare, non solo per i droni, ma anche per i robot, una "black box" che permetta di registrare, cristallizzare e conservare in modo idoneo tutti gli eventi che precedano l'eventuale incidente**.

In conclusione, le discipline della digital forensics e della sicurezza informatica collegate alla robotica sono di grande importanza, ma non dovranno essere circoscritte solo all'aspetto tecnologico. Esse dovranno infatti aprirsi alla considerazione di tutti gli aspetti legali interconnessi. Tra questi sono prioritari:

- la formalizzazione di regole e procedure per l'acquisizione e l'utilizzo della prova informatica, nel rispetto delle *best practices* nazionali e internazionali;
- la formalizzazione di regole e procedure di *cyber* sicurezza idonee a proteggere il robot o il drone da eventuali attacchi informatici;
- il rispetto della privacy dell'utente, che dovrà essere costantemente bilanciato con le esigenze di conservazione e di sicurezza del dato proprie della *digital forensics* e della *cyber security*.

---

[101] ISO/TC 184/SC 2 - *Robots and robotic devices*, disponibili al seguente URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=54138&includesc=true&published=on&development=on.

[102] S. Simou, C. Kalloniatis, E. Kavakli, S. Gritzalis, *Cloud Forensics: Identifying the Major Issues and Challenges*, in *Lecture Notes in Computer Science Volume 8484*, 2014, 271-284, disponibile al seguente URL: https://www.academia.edu/7120726/Cloud_Forensics_Identifying_the_Major_Issues_and_Challenges.

4.5 Diritti su beni immateriali

(a cura di Marco Ciurcina)

Introduzione e principi generali

Con l'espressione **"diritti su beni immateriali"** si fa riferimento, innanzitutto, al diritto d'autore ed ai diritti connessi a questo, ai c.d. diritti di proprietà industriale (marchi ed altri segni distintivi, brevetti, modelli e disegni, etc.), ma anche ai diritti della personalità (nome, immagine, etc.) e ad altri diritti stabiliti dall'ordinamento che interferiscono con la creazione o con l'uso di beni immateriali (ad es.: riserva di produzione di beni culturali; segreto di stato). Il diritto alla privacy, per la speciale rilevanza nella materia della robotica di servizio, costituisce oggetto di trattazione specifica all'interno della Sezione 4.3.

In generale, i diritti su beni immateriali conferiscono ai loro titolari diritti esclusivi o di credito (il cui contenuto varia da diritto a diritto) nei confronti dei terzi che facciano un certo uso di tali beni.

Tali set normativi possono interferire con la robotica di servizio a diversi livelli. Innanzitutto, nella produzione di un robot o di un drone si possono creare od utilizzare elementi tutelati da diritti (l'aspetto esterno, i componenti hardware e software, etc.); ma anche nell'uso di un robot o di un drone possono entrare in gioco elementi tutelati da diritti su beni immateriali (ad es., i software e/o le banche di dati utilizzati dall'utente, le registrazioni realizzate dal robot/drone).

La fitta rete di esclusive che deriva dall'applicazione delle norme rende difficile – nella robotica di servizio – la collaborazione ed il riuso, così come avviene, del resto, in molti altri ambiti d'attività umana.

Anche per ovviare a questo problema, si sono diffusi diversi modelli di licenza che stabiliscono espressamente la facoltà di riuso da parte dei terzi, favorendo anche la collaborazione. In sostanza, grazie all'applicazione di un predefinito modello di licenza, si sono venuti organizzando dei veri e propri "beni comuni", come per esempio:

- software libero (ad es., il sistema operativo *GNU/Linux*[103] o il *Robot Operating System* – ROS[104]);
- open hardware (ad es., *Arduino*[105]);
- banche dati di contenuti (*Wikipedia*[106], *Open Street Map*[107], etc.).

Problematiche giuridiche rilevanti

Sulla base della descrizione delle casistiche fornita nella Sezione 2, **si possono individuare le seguenti evenienze:**

- commercializzazione di robot e/o droni assemblando componenti hardware interamente realizzati da terzi;
- realizzazione, riutilizzando e modificando software libero (ad es., ROS), di una piattaforma software, mediante la quale:
  i. fornire agli utenti di robot/droni servizi accessibili da remoto mediante API;
  ii. consentire a terzi di fornire applicazioni utilizzabili dagli utenti di robot/droni;
- realizzazione, riutilizzando e modificando software libero (ad es., ROS), di:
  i. un *software development kit* (SDK) che sarà utilizzato da terzi per realizzare applicazioni funzionanti su robot/droni;
  ii. componenti software che funzioneranno sui robot/droni commercializzati dallo stesso produttore di componenti software o da terzi, ed utilizzati dagli utenti.

Di conseguenza, risulta utile concentrare l'attenzione in particolar modo sulle componenti software del sistema, onde verificare la corretta gestione dei diritti ad esse applicabili.

In generale, **è necessario** affrontare i problemi tipici di questa specifica materia, e cioè:

a) **individuare una corretta policy di acquisizione degli elementi tutelati da diritti, che includa anche la verifica**

[103] Si veda: http://it.wikipedia.org/wiki/Linux#La_controversia_sulla_definizione_GNU.2FLinux.

[104] Si veda: http://en.wikipedia.org/wiki/Robot_Operating_System e http://www.ros.org/.

[105] Si veda: http://arduino.cc/.

[106] Si veda: http://www.wikipedia.org/.

[107] Si veda: http://www.openstreetmap.org/.

del fatto che non si violino diritti di terzi (tenendo conto dei vincoli imposti dalle licenze che si riferiscono agli artefatti acquisiti);

b) **individuare una corretta policy di licenza dei diritti sugli artefatti che sono messi a disposizione dei terzi**.

In generale, la realizzazione di artefatti software può essere frutto dell'opera di dipendenti, di terzi fornitori o può essere frutto del riuso di componenti disponibili al pubblico secondo i termini di una licenza di software libero.

Il **software realizzato internamente all'azienda** non pone problemi quando è creato – in conformità all'art. 12-bis della Legge 22 aprile 1941 n. 633, rubricato *"Protezione del diritto d'autore e di altri diritti connessi al suo esercizio"* – "*dal dipendente nell'esecuzione delle sue mansioni o su istruzioni impartite dallo stesso datore di lavoro*".

Per il **software realizzato da terzi fornitori**, si richiama la necessità di acquisire espressamente da tali terzi tutti i diritti necessari all'uso che si intende fare del software stesso.

Per quanto riguarda il **software disponibile con licenza di software libero**, si rende opportuna, già in fase di acquisizione, un'analisi preventiva, onde verificare se e come il software che – riutilizzando software libero – si va a realizzare possa essere utilizzato e distribuito, e se quindi sia compatibile con la policy d'uso e distribuzione che si intende adottare.

Infatti, **il riutilizzo di software libero implica la necessità di verificare se i termini di licenza del software riutilizzato, secondo le modalità di riutilizzo adottate**:

i. **impongano vincoli alla fornitura di servizi che incorporano il software riutilizzato**;

ii. **impongano vincoli nella distribuzione di pacchetti software** (SDK, componenti software).

In sostanza, si deve individuare il tipo di relazione tecnica esistente tra il software riutilizzato e quello creato per essere utilizzato e distribuito, al fine di verificare se la licenza del software riutilizzato imponga vincoli per quel particolare tipo di relazione. La verifica deve essere "bidirezionale", nel senso che si deve anche verificare se la licenza che si utilizza per il software distribuito a terzi sia compatibile con il riuso di componenti licenziati secondo i termini di licenza applicabili ai componenti riutilizzati.

Nel caso in cui **si decida di riutilizzare il software ROS**[108], si rileva che **detto software è licenziato, per lo più**[109], **con licenza BSD**[110]. La licenza BSD impone il solo vincolo di menzione della nota di copyright e delle condizioni della licenza nel software distribuito. Tuttavia, **vi sono specifiche librerie del sistema ROS che sono licenziate secondo i termini di altre licenze di software libero**. È pertanto opportuno verificare se nel sistema siano presenti librerie licenziate secondo termini di licenza che impongono vincoli all'uso del software come servizio (per esempio, la licenza AGPLv3[111]) e/o alla distribuzione del software (per esempio, una licenza *copyleft*[112]).

Normativa di riferimento applicabile

Con riguardo alle tre casistiche-tipo di cui alla Sezione 2, **i seguenti set normativi possono avere rilievo in relazione all'attività di produzione od uso di robot/droni**:

- l'aspetto dei robot/droni o di loro parti può costituire l'oggetto del diritto su disegni e modelli previsto dagli artt. 31-44 del D. Lgs. 10 febbraio 2005, n. 30 (codice della proprietà industriale – c.p.i.) o degli artt. 2 n. 10 e 12-19 della Legge 22 aprile 1941, n. 633 (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio – l.d.a.);
- specifici aspetti dei robot/droni potrebbero costituire l'oggetto del diritto di brevetto per invenzione previsto dagli artt. 45-81 c.p.i. o del diritto di brevetto per modello d'utilità previsto dagli artt. 82-86 c.p.i.;
- le parti elettroniche dei robot/droni possono costituire l'oggetto del diritto di topografie dei prodotti a semiconduttori previsto dagli artt. 87-97 c.p.i.;
- il know-how relativo ai robot/droni potrebbe costituire l'oggetto del diritto sulle informazioni segrete previsto dagli artt. 98-99 c.p.i.;
- il software che fa funzionare i robot/droni può costituire l'oggetto di diritto d'autore ai sensi degli artt. 2 n. 8, 12-19 e 64-bis-64-quater l.d.a.;
- i dati utilizzati per il funzionamento dei robot/droni possono costituire l'oggetto di diritto *sui generis* sulle banche

---

[108] Si veda: http://www.ros.org/.

[109] Si veda: http://en.wikipedia.org/wiki/Robot_Operating_System dove si legge: "*Both the language-independent tools and the main client libraries (C++, Python, and LISP) are released under the terms of the BSD license, and as such are open source software and free for both commercial and research use. The majority of other packages are licensed under a variety of open source licenses*".

[110] Si veda: http://en.wikipedia.org/wiki/BSD_licenses.

[111] Si veda: http://it.wikipedia.org/wiki/GNU_Affero_General_Public_License e http://www.gnu.org/licenses/agpl-3.0.html.

[112] Si veda: http://en.wikipedia.org/wiki/Copyleft.

di dati ai sensi dell'art. 102-bis e 102-ter, e/o di diritto d'autore ai sensi degli artt. 2 n. 9, 12-19 e 61-64 l.d.a.;

- altri elementi dei robot/droni (immagini, audio, video, etc.) possono costituire l'oggetto di diritto d'autore – ai sensi dell'art. 2 nn. 1, 2, 4, 6 e 7 e degli artt. 12-19 l.d.a. – o di diritti connessi, previsti nella stessa Legge;
- i dati trattati nel funzionamento dei robot/droni che consistono in dati personali costituiscono l'oggetto di diritto alla protezione dei dati personali ai sensi del codice privacy;
- le registrazioni foto, video o audio realizzate dai robot/droni e l'aspetto esterno dei robot/droni possono interferire con diritti della personalità – quali il diritto al nome (art. 6-9 codice civile), il diritto all'immagine (art. 10 codice civile) ed il diritto all'identità personale (riconosciuto dalla giurisprudenza in applicazione dell'art. 2 della Costituzione Italiana) –, ma anche con la riserva di riproduzione dei beni culturali (art. 106 D. Lgs. 42/2004) e con le norme sul segreto di stato.

Allocazione delle responsabilità tra i vari soggetti coinvolti

Con riferimento specifico alla materia trattata nella presente sezione, è utile sottolineare che **la distribuzione delle responsabilità tra i diversi soggetti coinvolti** (fornitori di soluzioni software/hardware per la connessione di robot di servizio attraverso reti a banda larga; produttori hardware; creatori delle applicazioni software) **si può modulare secondo le modalità di licenza degli artefatti (software e banche di dati) utilizzati dall'utente per il funzionamento del robot/drone**.

Si parte da un assunto che si ritiene a presupposto del ragionamento che segue: nei confronti dei consumatori è più complesso far valere clausole d'esclusione e/o limitazione della responsabilità e, quindi, potrebbe essere utile **evitare di configurarsi come fornitore di servizi ai consumatori** (fornendo piuttosto servizi agli integratori di robot).

Il modello descritto nella Sezione 2 prevede che le funzionalità di una soluzione software/hardware per la *cloud robotics* e l'utente entrino in contatto perlomeno in due momenti:

i. uso di servizi da parte dei robot/droni nella disponibilità degli utenti;
ii. uso di componenti software da parte dei robot/droni nella disponibilità degli utenti.

Qualora si forniscano tali servizi e/o software ai consumatori, si potrebbe rispondere dei danni che eventualmente conseguano al loro uso.

Si possono, in astratto, adottare due diverse strategie per limitare questo rischio:

i. **licenziare tali servizi e software ai propri partner commerciali** (produttori hardware e sviluppatori delle applicazioni software)**, affinché questi, a loro volta, possano licenziarli ai loro clienti** (possibili consumatori)**, assumendo su di sé le responsabilità** che ne conseguano;
ii. **partecipare alla creazione di "beni comuni" (software libero e/o banche dati aperte), eventualmente resi disponibili da enti terzi *no profit*** che forniscano funzionalità (software o servizi) da far usare ai partner commerciali e/o agli utenti.

La seconda di queste due strategie risulta interessante anche perché, **in certi casi** (quelli in cui sia possibile configurare un accesso diretto del consumatore al "bene comune"), potrebbe evitare anche al produttore hardware e/o allo sviluppatore software di assumere il rischio conseguente all'uso del servizio/software. Tale ultima strategia si potrebbe conciliare con le necessità di business mediante diverse tecniche, come quella del *dual licensing* (e cioè la licenza di un artefatto secondo condizioni diverse e alternative, alcune delle quali a pagamento), oppure attraverso la predisposizione di servizi aggiuntivi a pagamento di diverso tipo.

4.6 Regolamento ENAC

(a cura di Mauro Alovisio, Giovanni B. Gallus e Paolo Zampella)

L'Italia è il primo paese in Europa a dotarsi, in un'ottica di semplificazione, di un regolamento in materia di aeromobili a pilotaggio remoto senza pilota ed equipaggio a bordo (c.d. "droni").

Il sopra citato regolamento[113] – che definisce le regole, i requisiti tecnici e di sicurezza per l'impiego dei mezzi aerei a pilotaggio remoto (APR) – è stato emanato dall'Ente Nazionale per l'Aviazione Civile (ENAC) – in attuazione del regolamento (CE) n. 216/2008 e dell'art. 743 del codice della navigazione – in data 16 dicembre 2013, al termine di una consultazione pubblica avviata nel 2012, alla quale hanno partecipato molteplici *stakeholders* (imprese, costruttori, associazioni). In data 16 luglio 2015, il regolamento è stato aggiornato alla sua seconda edizione, ed è naturalmente su di essa che si basa la presente disamina della disciplina applicabile ai droni in Italia.

L'adozione di una normativa specifica costituisce un presupposto imprescindibile per lo sviluppo del mercato dei droni, anche alla luce della Convenzione di Chicago del 1944, la quale prevede che "*[n]o aircraft capable of being flown without a pilot shall be flown over the territory of a contracting State without special authorisation by that State and in accordance with the terms of such authorisation*".

Il regolamento ENAC costituisce, in assenza di definizione di standard a livello internazionale, un **prezioso punto di riferimento a livello mondiale ed europeo, in quanto fornisce un primo inquadramento giuridico del fenomeno dei droni**, settore in forte crescita e con importanti ricadute in termini di ricerca.

Prima della sua emanazione, non erano previste regole certe per i progettisti e piloti di droni (i droni rientravano nella disciplina del codice della navigazione, che richiedeva agli operatori del settore requisiti rigorosi: ad es., le licenze di tipo aeronautico).

Esso sarebbe dovuto entrare in vigore a decorrere dal sessantesimo giorno successivo al 17 dicembre 2013, data di pubblicazione dello stesso sul sito internet istituzionale dell'ENAC (www.enac.gov.it), e quindi entro il 17 febbraio 2014, termine successivamente posticipato – con disposizione del 14 febbraio 2014 – al 30 aprile 2014. La seconda edizione del regolamento – che apporta modifiche di particolare rilievo, volte a trovare un migliore equilibrio tra esigenze di sicurezza ed esigenze di sviluppo del mercato –, pubblicata sul sito ENAC il 17 luglio 2015, è entrata in vigore il 15 settembre 2015.

Composto da 37 articoli e strutturato in otto sezioni, il regolamento ha il pregio di individuare un set di regole finalizzate a garantire, da un lato, la sicurezza dei cittadini sorvolati dai droni e, dall'altro, certezze e uniformità nell'utilizzo di tali mezzi per gli operatori economici che intendano farne uso.

Tale atto normativo specifica che cosa sia un drone, illustra la classificazione dei droni a seconda della loro massa operativa al decollo (peso minore o uguale a due chilogrammi; maggiore di due, ma minore di 25 chilogrammi; maggiore o uguale a 25, e non superiore a 150 chilogrammi), prevede (in determinati casi) un sistema semplificato di autocertificazioni, distingue – al fine di prevenire rischi e pericoli – tra operazioni critiche e non critiche, introduce l'obbligo di assicurazione e definisce regole di sicurezza e privacy.

Costituisce un pregevole sforzo di dare risposte agli operatori e – come si evince dalla relativa relazione introduttiva – propone *"un approccio bilanciato ai temi della sicurezza che tenga conto delle caratteristiche tecniche e operative dei sistemi a pilotaggio remoto, delle modalità di occupazione dello spazio aereo, del contributo conferito dalla capacità di gestione dell'operatore e dalla qualificazione dei piloti di tali mezzi"*.

Il regolamento introduce, a tal fine, come vedremo, due importanti differenziazioni: il peso degli APR; la capacità del pilota di avere o meno in vista l'APR (operazioni VLOS e BLOS: *Visual Line Of Sight* indica che le operazioni sono svolte in condizioni nelle quali il pilota remoto rimane in contatto visivo con il mezzo aereo, senza aiuto di dispositivi ottici e/o elettronici; *Beyond Line Of Sight* indica operazioni condotte ad una distanza tale da non consentire al pilota remoto di rimanere in contatto visivo diretto e costante con il mezzo aereo, o di rispettare le regole dell'aria applicabili al volume di spazio aereo interessato interessato).

Il Sistema Aeromobile a Pilotaggio Remoto (SAPR) è un sistema costituito da un **mezzo aereo a pilotaggio remoto senza persone a bordo** – non utilizzato per fini ricreativi e sportivi (a differenza degli aeromodelli) e che può essere impiegato per operazioni specializzate o per attività di ricerca e sviluppo – e dai relativi componenti necessari per il controllo ed il comando da parte di un pilota remoto.

La prima grande distinzione operata dal regolamento è quella tra due tipologie di Mezzi Aerei a Pilotaggio Remoto (APR):

- i *Sistemi Aeromobili a Pilotaggio Remoto (SAPR)*, mezzi impiegati o destinati all'impiego in operazioni specializzate o in attività sperimentali;
- gli *Aeromodelli*, mezzi impiegati esclusivamente per scopi ricreazionali e sportivi, e che non sono considerati aeromobili ai fini del loro assoggettamento alle previsioni del codice della navigazione.

Ci si occuperà in primo luogo dell'analisi delle norme concernenti i SAPR, per poi trattare brevemente la materia relativa agli aeromodelli.

L'impiego dei droni è soggetto al rispetto delle singole sezioni, come applicabili, di cui si compone il regolamento (cfr. art. 7).

[113] Si veda: http://www.enac.gov.it/la_normativa/normativa_enac/regolamenti/regolamenti_ad_hoc/info-122671512.html. Versione inglese: http://www.enac.gov.it/Servizio/Info_in_English/Courtesy_translations/info-1220929004.html

È importante sottolineare come restino fuori dall'ambito di applicazione del regolamento, come specificato dall'art. 2, comma 3[114], i *"sistemi autonomi",* che sono peraltro espressamente oggetto di una definizione, all'art. 5, quali SAPR per cui il pilota non ha possibilità di controllare il volo del mezzo, intervenendo in diretta. Tale esclusione è coerente con l'art. 743 del codice della navigazione, che include tra gli aeromobili i *"mezzi aerei a pilotaggio remoto"*, rendendo quindi necessaria, ai fini della loro inclusione nella categoria, l'attività di pilotaggio, ancorché da remoto.

Ne consegue, dunque, che **al momento appare difficilmente prospettabile la liceità dell'utilizzo di sistemi (completamente) autonomi**.

La necessità di un controllo remoto (addirittura visuale) appare chiara dalla lettura delle norme, le quali verranno esaminate più in dettaglio nel prosieguo: i sistemi devono sempre operare all'interno delle aree VLOS, e solo per brevi fasi di volo (e previa espressa autorizzazione dell'ENAC) in aree EVLOS (*Extended Visual Line Of Sight*: aree le cui dimensioni superano i limiti delle condizioni VLOS, e per le quali il requisito del mantenimento del contatto visivo con il drone è soddisfatto con l'uso di mezzi alternativi).

Il controllo remoto, di norma accompagnato dal controllo visuale, è dunque, al momento, un elemento sostanzialmente imprescindibile per per l'impiego dei droni a uso civile. Nella seconda edizione si introduce comunque la possibilità di effettuare operazioni BLOS, ma adottando sistemi e procedure per il mantenimento della separazione e per evitare le collisioni che richiedono l'approvazione da parte dell'ENAC, esclusivamente in spazi aerei segregati, e sulla base della tipologia delle operazioni e delle risultanze della valutazione del rischio effettuata dall'operatore SAPR (art. 26).

Resta fuori dal regolamento in esame anche l'utilizzo dei SAPR in ambienti in spazio chiuso (spazio *indoor*), fatta eccezione per la previsione di cui all'art. 10, comma 7[115], sulla cui opportunità, per difetto di competenza dell'Ente, è legittimo sollevare qualche dubbio.

Gli APR devono essere identificati attraverso l'apposizione sul mezzo aereo di una targhetta riportante i dati identificativi del sistema e dell'operatore. La targhetta deve essere installata anche sulla stazione di terra.

Tra le novità più interessanti del nuovo regolamento vi è l'obbligo di dotare i SAPR – a partire dal 1 luglio 2016 –, oltre che della sopra citata targhetta, anche di un dispositivo elettronico di identificazione, che consenta la trasmissione in tempo reale dei dati inerenti l'APR ed il proprietario/operatore e dei dati essenziali di volo, nonché la registrazione degli stessi. Le caratteristiche del sistema saranno fissate dall'ENAC.

I SAPR possono essere utilizzati, ai sensi dell'art. 7 del regolamento, per operazioni specializzate e per attività di ricerca e sviluppo.

Nel caso di operazioni specializzate per conto terzi, il regolamento prevede l'obbligo di stipulare un accordo tra l'operatore del SAPR e il committente, nel quale le parti definiscono le rispettive responsabilità per la specifica operazione di volo, nonché le eventuali limitazioni e condizioni connesse, anche con riguardo ai profili del trattamento dei dati personali.

La nuova versione del regolamento amplia i precedenti limiti in materia di distanze: i SAPR potranno ora volare nelle operazioni in VLOS **fino ad una distanza massima di 500 metri sul piano orizzontale ed in altezza massima fino a 150 metri AGL** (*Above Ground Level*, al di sopra del livello del suolo). Il regolamento prevede, all'art. 24, perfino la possibilità dell'ENAC di autorizzare anche distanze e altezze superiori, a seguito della presentazione di adeguata valutazione del rischio da parte dell'operatore.

Il regolamento specifica, inoltre, che – in caso di perdita del contatto visivo del SAPR entro i limiti orizzontali e verticali consentiti – il pilota deve terminare il volo il prima possibile.

---

[114] L'art. 2, terzo comma, del regolamento prevede infatti quanto segue:
"Non sono assoggettati alle previsioni del presente Regolamento:
a) i SAPR di Stato di cui agli articoli 744, 746 e 748 del Codice della Navigazione;
b) i sistemi autonomi;
c) i SAPR che svolgono attività in spazio chiuso (spazio indoor), a meno di quanto previsto al comma 7 dell'art. 10;
d) i SAPR costituiti da palloni utilizzati per osservazioni scientifiche o da palloni frenati."

[115] Il quale specifica che trova comunque applicazione, anche nel caso di utilizzo di SAPR in ambienti chiusi, il divieto di sorvolo di assembramenti di persone per cortei, manifestazioni sportive o inerenti forme di spettacolo, o comunque di aree dove si verifichino concentrazioni inusuali di persone.

Il regolamento conferma altresì, nella sua seconda edizione, il divieto di utilizzo dei SAPR: all'interno dell'ATZ (*Aerodrome Traffic Zone*) di un aeroporto e nelle aree sottostanti le traiettorie di decollo ed atterraggio; ad una distanza inferiore a cinque chilometri dall'aeroporto (*Aerodrome Reference Point* o coordinate geografiche pubblicate), laddove non sia istituita una ATZ a protezione delle operazioni di volo; all'interno delle zone regolamentate attive e delle zone proibite, riportate in AIP (*Aeronautical Information Publication*).

Il regolamento, nella sua nuova versione, definisce (art. 5) anche i profili dell'attività di ricerca e sviluppo che consentono lo svolgimento di attività di ricerca pura o finalizzata alla verifica di determinate concezioni di progetto del SAPR stesso, di nuovi equipaggiamenti, nuove installazioni, tecniche di impiego od usi.

L'effettuazione dell'attività per lo scopo *"ricerca e sviluppo"* è soggetta, ai sensi dell'art. 9, comma 10, ad autorizzazione da parte dell'ENAC.

Inoltre l''aggiornamento del regolamento prevede la possibilità di utilizzare i droni anche per il trasporto di merci pericolose, previa autorizzazione da parte dell'ENAC (art. 7, comma 4).

Il regolamento **distingue la disciplina applicabile ai sopra citati SAPR in due macro-categorie,** in relazione alla loro massa operativa al decollo :

- inferiore a 25 chilogrammi (Sezione II del Regolamento); una disciplina parzialmente specifica è prevista per i SAPR di massa inferiore od uguale ai due chilogrammi (Sezione II, art. 12);
- uguale o maggiore a 25 chilogrammi (Sezione III, artt. 14-19).

La regolamentazione dei SAPR che superano i 150 chilogrammi è di competenza dell'Agenzia Europea per la Sicurezza Aerea (EASA).

Uno dei principi cardine del regolamento per i SAPR di peso inferiore ai 25 chilogrammi è costituito dal concetto di valutazione del rischio. Il regolamento, infatti, distingue due tipologie di situazioni: le operazioni aeree in ambienti non a rischio e le operazioni aeree in ambienti a rischio.

Per **operazioni specializzate non critiche** si intendono quelle operazioni condotte in VLOS che non prevedono il sorvolo, anche in caso di avarie e malfunzionamenti, di aree congestionate, assembramenti di persone, agglomerati urbani, infrastrutture sensibili. Nelle operazioni non critiche la possibilità di arrecare danni a terra a persone e cose, nel caso di avarie e malfunzionamenti del drone, è più difficile e remota.

Si osservi come la versione precedente del regolamento prevedesse *"infrastrutture"* in genere e *"linee e stazioni ferroviarie, autostrade e impianti industriali"*, ora sostituite con l'espressione *"infrastrutture sensibili"*.

Nel caso di operazioni specializzate non critiche, non occorre un'autorizzazione da parte dell'ENAC: l'operatore è tenuto a presentare all'ENAC, attraverso la procedura riportata sul sito web istituzionale, una semplice dichiarazione – con conseguente meccanismo di silenzio-assenso – che attesti la rispondenza alle applicabili sezioni del Regolamento e indichi le condizioni e i limiti applicabili alle operazioni di volo previste, inclusa, eventualmente, la necessità di operare in spazi aerei segregati. Restano in capo all'operatore la responsabilità di valutare il rischio associato alle operazioni ed il permanere delle condizioni che fanno ritenere non critiche le operazioni, nonché gli obblighi di possedere e mantenere aggiornata la documentazione tecnica prevista dall'art. 11, comma 8, come applicabile .

Il sopra citato articolo 11, comma 8 prevede la seguente documentazione:

a) i dati della targhetta identificativa del SAPR, la descrizione e la configurazione del sistema da impiegare, nonché le caratteristiche e le prestazioni tali da garantirne un impiego sicuro ovvero la dichiarazione di conformità rilasciata dal costruttore, nel caso di SAPR in possesso di certificato di tipo;

b) i risultati delle prove dell'attività sperimentale iniziale;

c) la tipologia delle operazioni specializzate che si intende svolgere;

d) i termini temporali per i quali è richiesta l'autorizzazione;

e) i risultati dell'analisi del livello di rischio associato alle operazioni previste, eseguita al fine di sostanziare la sicurezza delle stesse;

f) il manuale di volo dell'APR o documento equivalente;

g) il programma di manutenzione del SAPR;

h) il manuale delle operazioni, inclusa la descrizione delle modalità di valutazione e gestione del rischio.

Il regolamento specifica che la dichiarazione rimane valida, purché le operazioni siano condotte nell'ambito delle condizioni e limiti dell'autorizzazione o della dichiarazione. Nel caso in cui siano apportate modifiche al sistema o effettuate operazioni al di fuori delle previsioni della dichiarazione, la dichiarazione medesima perde efficacia.

Pertanto, a titolo esemplificativo, nel caso di utilizzo di droni per riprese video e/o fotografiche in zone non a rischio, non è richiesto il rilascio di una specifica autorizzazione, in quanto l'ENAC riconosce l'autocertificazione dell'operatore secondo lo standard del regolamento (con dichiarazione di *compliance* al regolamento stesso, documentazione, prove di volo).

Per operazioni specializzate critiche si intendono tutte le operazioni che presentano particolari rischi per la sicurezza, perché prevedono il sorvolo di aree congestionate, assembramenti di persone, agglomerati urbani, infrastrutture sensibili. L'eventualità di una avaria o di un guasto del drone offre, in tali situazioni, elevati rischi di danni a terra a persone e cose.

In questi casi l'attività di verifica dell'ENAC è molto più approfondita e puntuale in relazione all'operatore, all'*assessment* del rischio ed al pilota.

Nel caso di operazioni critiche occorre, infatti, fare domanda all'ENAC ed ottenere una specifica autorizzazione prima dell'inizio delle operazioni.

Le operazioni specializzate critiche possono essere condotte ove sia assicurato un livello di sicurezza coerente con l'esposizione al rischio, con riferimento alle operazioni dell'aviazione generale. Il livello di sicurezza di tali operazioni è determinato dall'insieme dei contributi forniti dal SAPR, dal pilota, dalle procedure operative e di gestione delle attività di volo, dalle condizioni ambientali e dagli altri elementi essenziali per determinare un impiego sicuro di tali mezzi, inclusa la corretta attuazione del programma di manutenzione.

La domanda di autorizzazione o la dichiarazione per l'effettuazione di operazioni specializzate possono essere presentate all'ENAC solo dopo che l'operatore abbia completato con esito positivo la relativa attività di volo sperimentale in accordo alle previsioni del regolamento.

Nel caso di operazioni critiche, l'operatore presenta all'ENAC la domanda di autorizzazione, nella quale attesta la rispondenza al Regolamento e indica le condizioni e i limiti applicabili alle operazioni di volo previste, inclusa, eventualmente, la necessità di operare in spazi aerei segregati. Alla domanda va allegata la seguente documentazione (la medesima prevista per la presentazione della dichiarazione di operatore nel caso di operazioni non critiche):

a) i dati della targhetta identificativa del SAPR, la descrizione e la configurazione del sistema da impiegare, nonché le caratteristiche e le prestazioni tali da garantirne un impiego sicuro ovvero la dichiarazione di conformità rilasciata dal costruttore, nel caso di SAPR in possesso di certificato di tipo;

b) i risultati delle prove dell'attività sperimentale iniziale;

c) la tipologia delle operazioni specializzate che intende svolgere;

d) i termini temporali per i quali è richiesta l'autorizzazione;

e) i risultati dell'analisi del livello di rischio associato alle operazioni previste, eseguita al fine di sostanziare la sicurezza delle stesse;

f) il manuale di volo dell'APR o documento equivalente;

g) il programma di manutenzione del SAPR;

h) il manuale delle operazioni, inclusa la descrizione delle modalità di valutazione e gestione del rischio.

Ricevuta la domanda, l'ENAC rilascia l'autorizzazione al completamento – con esito positivo – della valutazione della documentazione prodotta da parte dell'operatore per sostanziare la capacità di effettuare l'attività in sicurezza. Nell'ambito delle valutazioni, l'ENAC si riserva di richiedere l'effettuazione di ulteriori analisi e prove, come pure di condurre eventuali ispezioni.

Come già osservato, l'autorizzazione o la dichiarazione rimangono valide, purché le operazioni siano condotte nell'ambito delle condizioni e dei limiti dell'autorizzazione o della dichiarazione, e decadono nel caso in cui siano apportate modifiche al sistema o siano effettuate operazioni al di fuori delle previsioni dell'autorizzazione/dichiarazione. L'ENAC si riserva la facoltà di effettuare verifiche sulle effettive modalità con cui sono condotte le operazioni.

Per l'effettuazione di operazioni critiche, il regolamento richiede, all'art. 10, che il SAPR sia dotato di un mezzo di terminazione del volo la cui funzionalità sia indipendente dal sistema primario di comando e controllo del mezzo. La quota minima di volo da tenere deve essere determinata per ogni sistema di terminazione del volo in modo tale da garantirne l'efficacia.

La nuova versione del regolamento prevede la possibilità di svolgere operazioni specializzate critiche in condizioni VLOS, in aree urbane, in scenari che non prevedono il sorvolo di persone nell'area delle operazioni e nel buffer, a meno che tali persone non siano indispensabili alle operazioni ed addestrate allo scopo. In tali circostanze un adeguato livello di sicurezza può essere dimostrato tramite l'utilizzo di due sistemi indipendenti e dissimilari, di comando e controllo e di terminazione del volo. Il sistema di terminazione del volo deve consentire, quando attivato, la terminazione del volo all'interno dell'area di buffer.

Viene pertanto consentito il sorvolo delle aree urbane in condizioni VLOS ai SAPR che dimostrino un accettabile livello di

sicurezza. La conformità a tale requisito è ritenuta soddisfatta ove il SAPR sia dotato di specifici requisiti (paragonabili a quelli richiesti per l'aviazione generale)[116].

Il regolamento prevede, infine, all'art. 10, comma 7, il generale divieto di sorvolo di assembramenti di persone, per cortei, manifestazioni sportive o inerenti forme di spettacolo, o comunque di aree dove si verifichino concentrazioni inusuali di persone.

Una delle più significative innovazioni introdotte nella seconda edizione del regolamento è quella legata agli APR con massa operativa al decollo minore o uguale a 2 chilogrammi (c.d. **minidroni**). Per questi, infatti, le operazioni specializzate sono sempre considerate non critiche (e dunque soggette a mera dichiarazione e non ad autorizzazione), sempre che si tratti di droni che abbiano caratteristiche di inoffensività, accertate dall'ENAC o da altro soggetto autorizzato. In altre parole, i droni "inoffensivi" sotto i 2 chilogrammi possono operare anche in agglomerati urbani, senza bisogno di specifica autorizzazione.

Permane però il divieto assoluto di sorvolo di assembramenti di persone, per cortei, manifestazioni sportive o inerenti forme di spettacolo, o comunque di aree dove si verifichino concentrazioni inusuali di persone. Per condurre questi droni, è sufficiente che vi sia un pilota dotato di attestato, che assume anche le funzioni (e le responsabilità) dell'operatore, pur non essendo obbligatori i relativi requisiti organizzativi.

Ancor maggiore libertà è concessa ai c.d. "**microdroni**", di massa al decollo minore o uguale a 0,3 chilogrammi, e con una velocità massima minore o uguale a 60 chilometri all'ora: fermo restando il divieto di sorvolo di assembramenti, le operazioni sono considerate non critiche in tutti gli scenari, e non è neanche richiesto l'attestato di pilota, anche se, naturalmente, devono essere rispettate le regole di navigazione. Anche in questi casi occorre sempre far precedere le operazioni dalla dichiarazione all'ENAC.

Si aprono quindi interessantissimi scenari per l'uso in aree urbane (ad esempio per scopi giornalistici): bisogna però ricordare che anche se le operazioni sono lecite sotto il profilo della sicurezza della navigazione, rimangono fermi tutti i limiti in materia di trattamento di dati personali e di interferenze illecite nella vita privata.

Gli APR con massa al decollo uguale o maggiore ai 25 chilogrammi, che effettuano attività all'interno dello spazio aereo italiano, sono registrati dall'ENAC mediante iscrizione nel Registro degli Aeromobili a Pilotaggio Remoto, con l'apposizione di marche di registrazione dedicate; le medesime marche devono essere altresì apposte sulla stazione di controllo a terra. Deve inoltre essere apposta una targhetta di identificazione sul mezzo aereo e sulla stazione di terra (art. 14). La richiesta di registrazione deve essere effettuata dal proprietario del SAPR (art. 14) in accordo alle procedure stabilite dall'ENAC.

Nel caso di utilizzo di SAPR con mezzi aerei di massa massima al decollo maggiore o uguale a 25 chilogrammi, il regolamento richiede **specifiche condizioni di aeronavigabilità**: in particolare, viene prevista una specifica abilitazione alla navigazione, attestata dal rilascio di un Permesso di Volo al SAPR o – nel caso di SAPR in possesso di un Certificato di Tipo Ristretto – da un Certificato di Navigabilità Ristretto (art. 15).

Il **Permesso di Volo** può essere rilasciato:

- per effettuare la sperimentazione allo scopo di ricerca e sviluppo, o – nel caso di SAPR per i quali è stato richiesto un certificato di tipo ristretto – di dimostrazione di rispondenza alla base di certificazione;
- per operazioni specializzate, nel caso di SAPR non costruiti in serie e quindi non in possesso di certificazione di tipo ristretto.

Il Permesso di Volo specifica le condizioni e/o limitazioni nell'ambito delle quali devono essere condotte le operazioni; esse includono anche le applicabili limitazioni riguardanti le tipologie delle aree di operazione.

Il regolamento richiede per tali SAPR **ulteriori condizioni più rigorose, previste nella sua Sezione III.**

Nel caso di veicoli superiori ai 25 chilogrammi, il regolamento prevede, all'art. 19, **precisi obblighi di manutenzione**: l'operatore del SAPR deve cioè stabilire, sulla base delle istruzioni del costruttore, ed integrandole come necessario in base alla tipologia delle operazioni, un programma di manutenzione adeguato, per assicurare il mantenimento dell'aeronavigabilità del sistema.

L'operatore si deve inoltre dotare di un **sistema di registrazione dei dati** inerenti alle ore di volo, agli eventi significativi per la sicurezza, alle manutenzioni ed alla sostituzione componenti.

Il costruttore, o altra organizzazione da questi riconosciuta, è autorizzato ad effettuare le operazioni di manutenzione dei propri SAPR. La manutenzione ordinaria può essere effettuata anche dall'operatore, dopo aver frequentato idoneo corso per la

---

[116] I SAPR per le operazioni critiche devono essere dotati ai sensi dell'art. 10, sesto comma, di:
- un sistema primario di comando e controllo il cui software sia conforme agli standard aeronautici di cui alla specifica EUROCAE ED-12 almeno al livello di affidabilità progettuale D; standard alternativi possono essere accettati dall'ENAC ove soddisfino gli stessi obiettivi di affidabilità,
- sistemi idonei a mantenere il controllo delle operazioni in caso di perdita del data link o a mitigarne gli effetti, e
- un sistema di terminazione del volo il cui comando sia indipendente e dissimilare dal sistema di comando e controllo e che, ove attivato, consenta una moderata esposizione a potenziali danni da impatto.

manutenzione presso il costruttore o altre organizzazioni da questi autorizzate (cfr. art. 19).

Il regolamento prevede, all'art. 29, uno specifico obbligo di comunicazione di eventi, e specifica che l'operatore, il costruttore, l'organizzazione di progetto, il pilota e il manutentore, secondo le rispettive responsabilità, sono tenuti a **comunicare all'ENAC, entro 72 ore, ogni incidente ed inconveniente grave**.

Vengono poi approfonditi – in relazione a SAPR di qualunque massa – **il ruolo, i requisiti e le responsabilità dei piloti** che devono essere designati dall'operatore: avere un'età minima di 18 anni, conoscere le regole dell'aria applicabili, avere effettuato un programma di addestramento per lo specifico SAPR ed essere in possesso di un certificato medico in corso di validità (art. 20).

La seconda edizione contiene, inoltre, significative novità anche per i piloti: si distingue infatti tra *"attestato di pilota"* e *"licenza di pilota"*, entrambi con validità di 5 anni.

L'attestato di pilota consente di condurre gli APR di massa inferiore a 25 chilogrammi, ed è rilasciato *"per categorie di APR"*: non è quindi più collegato ad un sistema specifico. Per il rilascio dell'attestato, occorre una certificazione medica, la frequenza ad un corso di formazione, un programma di addestramento e un esame pratico presso un centro di Addestramento APR approvato dall'ENAC.

La licenza di pilota, rilasciata in applicazione delle procedure in uso per il rilascio delle altre licenze per il personale di volo, è invece necessaria per le operazioni BLOS, o per gli APR di massa uguale o superiore a 25 chilogrammi.

I centri di addestramento, oltre all'approvazione ENAC, devono essere dotati di idonea organizzazione e procedure, avere uno o più istruttori, ed almeno un esaminatore riconosciuto da ENAC. I centri hanno l'onere di notificare all'ENAC, entro 3 giorni, l'emissione dell'attestato di pilota (e tali dati sono resi accessibili alle Autorità di Pubblica Sicurezza).

Vi è poi un'altra innovazione, relativa alle modalità operative. Il pilota, difatti, dovrà essere immediatamente identificabile: il Regolamento prevede espressamente l'obbligo di utilizzare giubbetti ad alta visibilità con la scritta "pilota di APR".

Il regolamento specifica altresì che non è consentito ad un SAPR di operare in assenza di un'assicurazione per la responsabilità verso terzi, adeguata allo scopo e non inferiore ai massimali minimi di cui alla tabella dell'articolo 7 del Regolamento (CE) n. 785/2004 (art. 32).

Sotto il profilo della protezione dei dati personali, il regolamento richiama la normativa nazionale e specifica, all'art. 34, che – **nel caso in cui le operazioni svolte attraverso un SAPR possano comportare un trattamento di dati personali – tale circostanza dovrà essere menzionata nella documentazione** sottoposta ai fini del rilascio della pertinente autorizzazione.

Il trattamento dei dati personali deve essere effettuato in ogni caso nel rispetto del codice privacy – con particolare riguardo all'utilizzo di modalità che permettano di identificare l'interessato solo in caso di necessità ai sensi dell'art. 3 del codice –, nonché delle misure e degli accorgimenti a garanzia dell'interessato prescritti dal Garante per la protezione dei dati personali (informativa privacy**). La redazione del sopra citato articolo 34 del Regolamento ENAC in materia di privacy è il frutto della preziosa sinergia instaurata dall'ENAC con il Garante per la protezione dei dati personali, e costituisce una preziosa *best practice* a livello comunitario**. Il profilo della protezione dei dati deve inoltre essere previsto nei contratti e accordi fra operatori del SAPR e committenti (cfr. art. 7, comma 3 del Regolamento ENAC).

Si noti che il Garante per la protezione dei dati personali ha adottato, nel recente passato, un provvedimento generale in materia di videosorveglianza (in data 8 aprile 2010), ma non ha approfondito – in esso – né i profili dei droni, né quelli dello *street control*; pertanto, si renderà probabilmente necessario integrare e aggiornare tale provvedimento, anche in considerazione del fatto che alcuni enti locali hanno annunciato l'intenzione di utilizzare i droni per finalità di sicurezza urbana (così, ad es., il Comune di Jesolo per contrastare il fenomeno degli ambulanti), e altri li hanno già impiegati per usi di protezione civile (ad esempio il Comune di Olbia, per monitorare i corsi d'acqua soggetti a esondazione), con connesse criticità circa il bilanciamento di interesse fra privacy dei cittadini e sicurezza, nonché inerenti al rispetto dei principi di necessità e proporzionalità del trattamento di dati.

La relativa modulistica sui droni e le relative autorizzazioni sono pubblicate online sul sito dell'ENAC, a beneficio della certezza rispetto al traffico giuridico ed ai relativi contratti.

L'ENAC ha in passato pubblicato una bozza di circolare[117] che è stata oggetto di consultazione pubblica fino al 30 giugno 2014, al fine offrire agli operatori ulteriori chiarimenti in materia, e sta organizzando degli specifici *workshop* rivolti agli *stakeholders* (istituzioni, costruttori, piloti), al fine di illustrare l'impatto del regolamento sugli operatori e fornire ad essi

[117] Si veda: http://www.enac.gov.it/La_Normativa/Normativa_Enac/Consultazione_Normativa/info-1311250085.html.

specifici contesti per l'approfondimento ed il chiarimento di quesiti.

Come specificato nella bozza della Circolare NAV *"Mezzi Aerei a Pilotaggio Remoto"*, l'ENAC **sta sviluppando delle Linee Guida** allo scopo di fornire chiarimenti sull'applicazione del Regolamento e della Circolare ed ha pubblicato – in data 22 maggio 2014 – la bozza delle Linee Guida 2014/1 (*"Qualificazione del personale di volo APR"*[118]) e – in data 8 luglio 2014 – la bozza delle Linee Guida 2014/2 (*"SAPR Organizzazioni riconosciute"* che hanno la capacità di condurre accertamenti per supportare il richiedente nella dimostrazione di rispondenza al Regolamento[119]).

L'ENAC ha inoltre pubblicato una nota esplicativa sull'attuazione del regolamento[120] ed è in procinto di istituire una **specifica sezione di FAQ** (Frequently Asked Questions) sul proprio sito per dare risposte ai quesiti da parte di imprese e cittadini e al fine di accompagnare al meglio gli operatori nei relativi adempimenti in materia.

Il regolamento definisce, nella Sezione VII, anche le regole sulla gestione degli Aeromodelli, un settore che registra una forte crescita di fatturato. L'Aeromodello è un dispositivo aereo a pilotaggio remoto, senza persone a bordo, impiegato esclusivamente per scopi ricreativi e sportivi, non dotato di equipaggiamenti che ne permettano un volo autonomo, e che vola sotto il controllo visivo diretto e costante dell'aeromodellista, senza l'ausilio di aiuti visivi.

L'aeromodellista ai comandi dell'aeromodello ha la responsabilità di utilizzare il mezzo in modo da rispettare le regole dell'aria, non arrecare rischi a persone o beni a terra e ad altri utilizzatori dello spazio aereo, mantenere la separazione da ostacoli, evitare collisioni in volo e dare precedenza a tutti (art. 35).

Il regolamento sottolinea poi la responsabilità di ottemperare agli obblighi relativi e ad ottenere le eventuali autorizzazioni per l'utilizzo dello spettro elettromagnetico impegnato dal radiocomando.

Il regolamento ribadisce che l'aeromodellista deve rispettate le eventuali disposizioni emesse dalle amministrazioni locali competenti, e che manifestazioni aeromodellistiche e l'esercizio degli aeromodelli nel corso delle manifestazioni aeromodellistiche debbano essere effettuati in ottemperanza alle disposizioni emesse dall'Aero Club d'Italia.

Il regolamento prevede regole e requisiti declinati a seconda della massa dell'aeromodello: gli aeromodelli con massa al decollo minore di 25 chilogrammi, in particolare, possono volare nelle ore di luce diurna purché l'aeromodellista mantenga un continuo contatto visivo con l'aeromodello, senza aiuto di dispositivi ottici e/o elettronici, nonché a condizione che l'attività non presenti alcun rischio a persone e cose. Tali attività possono essere effettuate in aree non popolate opportunamente selezionate dall'aeromodellista, di raggio massimo di 200 metri e di altezza non superiore a 70 metri, e per le quali può assicurarne il controllo al fine di non causare rischio a persone e cose e fuori dalle ATZ e comunque ad una distanza di almeno 8 km dal perimetro di un aeroporto e dai relativi sentieri di avvicinamento/decollo. Devono inoltre essere rispettate le regole dell'aria applicabili inclusa la capacità di *"see and avoid"*. Le attività di volo possono essere effettuate anche in aree di altezza non superiore a 150 metri, purché l'aeromodellista sia titolare di una abilitazione al pilotaggio di aeromodelli radiocomandati rilasciata da una scuola certificata dall'Aero Club d'Italia e siano rispettate le regole dell'aria applicabili inclusa la capacità di "*see and avoid*" per l'aeromodellista e il rispetto del concetto di *"to be seen"* dell'aeromodello da parte degli altri aeromobili.

Nel caso non siano soddisfatte una o più delle limitazioni di cui sopra, l'attività di volo deve essere effettuata in spazi aerei regolamentati (permanenti) o segregati (temporanei).

Sugli aeromodelli utilizzati in un luogo aperto al pubblico non possono essere installati dispositivi o strumenti che ne configurino l'uso in operazioni specializzate.

L'attività con aeromodelli con massa al decollo massima uguale o maggiore a 25 chilogrammi, o con un sistema di propulsione che non rientra nei limiti previsti, è consentita ad aeromodellisti con un'età minima di 18 anni; l'attività deve essere svolta nelle ore di luce diurna, ad un'altezza massima dal terreno tale da consentire all'aeromodellista di mantenere un continuo contatto visivo con l'aeromodello senza aiuto di dispositivi ottici e/o elettronici, in aree istituite da ENAC e riservate alle attività aeromodellistiche. Tali aree sono caratterizzate da spazi aerei regolamentati o segregati.

È responsabilità dell'aeromodellista assicurare che durante l'attività in tali aree non siano presenti persone ad esclusione di quelle necessarie per lo svolgimento dell'attività.

Per le operazioni di aeromodelli spaziali (razzo modelli) non dotati di sistemi che ne permettano il controllo da parte dell'aeromodellista deve essere richiesto l'utilizzo dello spazio aereo all'ENAC.

Il regolamento prevede la possibilità dell'ENAC di adottare, nel rispetto della Legge n. 241/1990 e successive modifiche e integrazioni, **provvedimenti di sospensione totale o parziale delle autorizzazioni o delle certificazioni rilasciate** o annullare i privilegi ottenuti, nei casi per i quali è prevista una dichiarazione, in caso di inadempienza ai requisiti del Regolamento o quando l'operatore non si dimostra in grado di assicurarne la rispondenza (art. 30).

---

[118] Si veda: http://www.enac.gov.it/La_Regolazione_per_la_Sicurezza/Navigabilit-13-/Sistemi_Aeromobili_a_Pilotaggio_Remoto_%28SAPR%29/Documenti_correlati/info550418526.html.

[119] Si veda: http://www.enac.gov.it/La_Regolazione_per_la_Sicurezza/Navigabilit-13-/Sistemi_Aeromobili_a_Pilotaggio_Remoto_(SAPR)/Documenti_correlati/info232786887.html.

[120] Si veda: http://www.enac.gov.it/La_Regolazione_per_la_Sicurezza/Navigabilit-13-/Sistemi_Aeromobili_a_Pilotaggio_Remoto_%28SAPR%29/Documenti_correlati/info550418526.html.

Se l'operatore non consente all'ENAC l'effettuazione degli accertamenti di competenza, le autorizzazioni, le certificazioni e i privilegi ottenuti a seguito di dichiarazione possono essere altresì sospesi. Detto periodo di sospensione non può superare i 6 mesi e l'ENAC è tenuta a notificare all'operatore l'atto di sospensione, le motivazioni ed il tempo concesso per il rientro e il ripristino dei requisiti interessati. L'autorizzazione, la certificazione o i privilegi ottenuti a seguito di dichiarazione vengono revocati nel caso in cui l'operatore non provveda a ripristinare nei tempi previsti la rispondenza ai requisiti.

Una delle criticità dell'applicazione è costituita dall'effettività dei controlli: l'ENAC sarà effettivamente in grado di effettuare i controlli sopra citati o si troverà invece, in considerazione delle scarse risorse, a dover delegare tali funzioni ad altri enti? Nel caso, ad esempio, di voli di droni presso aree a rischio o voli notturni, quale autorità interverrà a tutela dei cittadini?

Per quanto concerne le **sanzioni** previste dalla normativa, la seconda edizione richiama espressamente l'art. 1174 del Codice della navigazione (sanzione amministrativa da 1.032 a 6.197 euro), per le ipotesi di effettuazione di operazioni specializzate con l'uso di SAPR in carenza dell'autorizzazione dell'ENAC per operazioni critiche o della dichiarazione da parte dell'operatore per operazioni non critiche, ovvero per l'inosservanza delle norme di sicurezza nel corso delle operazioni.

In realtà, le sanzioni applicabili non si limitano al solo art. 1174 del Codice della navigazione, ma riguardano anche altre fattispecie, sia attinenti alla navigazione aerea, che al codice della privacy e al codice penale.

Il pilota che sorvoli centri abitati, assembramenti o aeroporti, fuori dai casi specificamente autorizzati, è sanzionato con l'arresto fino a sei mesi o con l'ammenda fino a 516 €. Elevate sanzioni (sia penali che amministrative) sono previste per il pilota che sia sprovvisto di attestazione, di certificato medico, o operi al di fuori dei limiti previsti. Sono sanzionati penalmente anche l'operatore (ed il pilota) che utilizzino droni non equipaggiati con i dispositivi previsti: la sanzione per il primo è dell'arresto da un mese ad un anno ovvero ammenda da 516 a 1032,00 euro, mentre per il secondo è dell'arresto fino a sei mesi o ammenda da € 51,00 a € 516,00.

Vi è poi una norma che si applica tutte le volte che si violino le norme ENAC in tema di sicurezza della navigazione: difatti, ogni altra violazione del Regolamento (salvo che costituisca più grave reato) è sanzionata con l'arresto fino a tre mesi o la multa fino a 206 €. Tra l'altro, la condanna importa, in molti casi, la sospensione dei titoli abilitativi, e quindi, se si è pilota di drone, si rischia di non poter più lecitamente lavorare.

Per operare con un drone, come si è visto, è obbligatorio stipulare un'assicurazione e, laddove non si adempia a tale obbligo, le sanzioni sono elevatissime: l'operatore rischia una sanzione amministrativa fino a 100.000 €, e sanzioni comunque pesanti sono previste per il mancato rispetto dei minimi assicurativi. Sanzioni più modeste sono previste per l'uso del drone privo della targhetta di identificazione, e per l'operatore che impieghi un pilota non in regola.

Con riguardo al tema delle sanzioni, vi è poi da aggiungere che il Dipartimento della Pubblica Sicurezza ha emanato un prontuario, del 30 aprile 2015 (distribuito alle forze dell'ordine), che contiene uno schema delle condotte sanzionabili, non scevro da dubbi in ordine all'effettiva applicabilità di alcuni dei reati indicati alle fattispecie relative all'uso dei droni[121].

Nel prontuario non si fa menzione delle sanzioni relative alla privacy, né alle interferenze illecite nella vita privata, che sono comunque applicabili, e sono ancor più pesanti: l'omessa o inidonea informativa privacy è punita con la sanzione amministrativa da 6.000 a 36.000 €, il delitto di trattamento illecito di dati personali (art. 167 codice privacy) è punito con la reclusione fino a 3 anni, e il delitto di interferenze illecite nella vita privata (si pensi ad esempio alle riprese effettuate attraverso un drone, in un privato domicilio, superando un muro di recinzione) prevede la sanzione della reclusione da sei mesi a quattro anni.

Non bisogna dimenticare, infine, il regime di **responsabilità civile** previsto più in generale per gli esercenti/operatori di aeromobili, senz'altro applicabile al caso dei SAPR. Si tratta della responsabilità per danni a terzi sulla superficie, disciplinata dalla Convenzione di Roma del 1952, di cui l'Italia è parte e a cui è fatto espresso rinvio dall'art. 965 del codice della navigazione. Questi gli elementi che, in breve, caratterizzano l'istituto: si tratta, *in primis*, di una forma di responsabilità extracontrattuale e pressoché oggettiva in capo all'operatore (vale a dire indipendente dalla presenza di colpa); la prova liberatoria della responsabilità dell'operatore può essere costituita solo da specifiche circostanze espressamente indicate nella Convenzione (quali il concorso di colpa del danneggiato per propria negligenza, atto illecito od omissione); la previsione di

[121] Si veda, ad esempio, l'asserita qualificazione in termini di contravvenzione di cui all'art. 650 c.p. (punita con con l'arresto fino a tre mesi o con l'ammenda fino a duecentosei euro) per il caso di uso dell'aeromodello in maniera non conforme al regolamento. Tale conclusione è discutibile, dal momento che la Cassazione ha ritenuto la sopra citata norma incriminatrice non applicabile ai provvedimenti di carattere generale, come appunto il Regolamento (eppure ciò non esclude che le forze dell'ordine seguano le indicazioni del prontuario).

una limitazione del debito, istituto caratteristico del diritto della navigazione, che circoscrive l'esposizione risarcitoria dell'operatore entro una determinata soglia (in questo caso risponde solo fino all'ammontare delle somme previste come copertura assicurativa minima fissate dalla normativa comunitaria per la responsabilità verso i terzi, somme individuate dal Regolamento CE 785/2004, cui è altresì fatto riferimento per la definizione dell'assicurazione obbligatoria per i SAPR).

Da ultimo, la seconda edizione del Regolamento prevede, opportunamente, anche una **normativa transitoria**. In particolare, l'utilizzo del sito web dell'ENAC per deposito di dichiarazioni e notifica di attestati partirà dal 1° gennaio 2016.

L'obbligo dell'attestato per i piloti (secondo la nuova formulazione) partirà dalla stessa data, ma le qualificazioni già rilasciate saranno valide fino al primo ottobre 2016, e potranno anche essere convertite, a partire dal primo aprile 2016. Allo stesso modo, anche le autorizzazioni dei centri di addestramento APR già conseguite saranno valide fino al 1° aprile 2016.

Infine, per quanto riguarda le autorizzazioni e dichiarazioni per l'impiego di SAPR, è espressamente previsto che esse decadranno il primo luglio 2016. Le autorizzazioni (ma non le dichiarazioni) devono essere convertite entro la stessa data, mentre le dichiarazioni devono essere "confermate" mediante inserimento nel database ENAC.

In conclusione, il regolamento in esame costituisce comunque un prezioso punto di riferimento normativo, fornendo indicazioni e risposte agli utenti, operatori e imprese. La difficoltà più grande che si è presentata all'ENAC è stata quella di condensare a livello tecnico ed in un unico atto molteplici profili disciplinari relativi al mezzo, all'operatore, ai piloti, alle varie tipologie di droni.

Nonostante i lodevoli sforzi, si deve osservare tuttavia come **il regolamento non rappresenti lo strumento più adatto per disciplinare un fenomeno tanto complesso e dinamico come quello in oggetto (forse, data la materia, sarebbe stata preferibile l'adozione di linee guida**; soluzione adottata in altri paesi europei come Francia, Svizzera e Gran Bretagna). Si deve cioè rilevare come il diritto, anche in questo campo, si trovi costretto ad inseguire la velocità dell'innovazione tecnologica.

Da ultimo, va osservato che **la definizione di regole certe sui droni contribuirà verosimilmente allo sviluppo di attività economiche, di impresa e di ricerca, coinvolgendo inoltre attività di consulenza – da parte di giuristi e tecnici – rispetto ai profili di sicurezza, assicurazione e contrattualistica coinvolti**: come, ad esempio, nel caso frequente di operazioni specializzate per conto terzi (ad es., riprese di una manifestazione sportiva), lo svolgimento delle quali richiede che venga stipulato un accordo – tra l'operatore del SAPR e il committente – all'interno del quale le parti definiscano le rispettive responsabilità e concordino sull'idoneità del SAPR alla specifica operazione di volo e sulle eventuali limitazioni e condizioni connesse, anche con riguardo alle disposizioni in materia di protezione dati (cfr. art. 7, comma 3, e art. 34).

BIBLIOGRAFIA

ALLEN, C., VARNER, G., ZINSER J., (2000). *Prolegomena to Any Future Artificial Moral Agent*, in *Journal of Experimental and Theoretical Artificial Intelligence*, 12, 251-261.

ALOVISIO, M., (2011). *La videosorveglianza in ambito pubblico*, in M. Alovisio, D. Burroni, A. Frosini, E. O. Policella, *Videosorveglianza e privacy*, Experta.

ARTICLE 29 DATA PROTECTION WORKING PARTY, (2012). *Opinion 03/2012 on Developments in Biometric Technologies*, 27-04-2012. Disponibile al seguente URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY, (2013). *Remotely Piloted Aircraft Systems (RPAS) – Response to the Questionnaire*, 16-12-2013.

ARTICLE 29 DATA PROTECTION WORKING PARTY, (2015). *Opinion 01/2015 on Privacy and Data Protection Issues Relating to the Utilisation of Drones*, 16-06-2015. Disponibile al seguente URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf.

BEKEY, G. A., (2005). *Autonomous Robots: From Biological Inspiration to Implementation and Control*. The Mit Press, Cambridge, Mass., London, England.

CALO, R., (2014). *Robotics and the new Cyberlaw* in *California Law Review, Vol. 103, 2015*. Disponibile al seguente URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2402972

CALO, R., (2011). *Robots and privacy*, in *Robot Ethics: The Ethical and Social Implications of Robotics*, a cura di P. Lin, K. Abney, G.A. Bekey, Cambridge, 2011, 187. Disponibile al seguente URL: ssrn.com/abstract=1599189.

CAVOIKIAN, A., TAYLOR, S., ABRAMS, M. E., (2010). *Privacy by Design: essential for organizational accountability and strong business practices*, 4-6-2010, Springerlink.com, 409.

CHANG, J. B., SUBRAMANIAN, V., (2008). *Electronic Noses Sniff Success*, in *IEEE Spectrum*, marzo 2008. Disponibile al seguente URL: http://spectrum.ieee.org/biomedical/devices/electronic-noses-sniff-success/.

DAUTENHAHN, K., (2007). *Socially Intelligent Robots: Dimensions of Human-Robot Interaction*, in *Philosophical Transactions of the Royal Society B: Biological Sciences*, 362(1480): 679-704.

DENNING T., *ET AL.*, (2010). *A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and* Lessons, Proceedings of the 11th International Conference on Ubiquitous Computing, 30-9/3-10-2009, New York, 2010.

EASTBROOK, F.H., (1996). *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207.

FOGG, V. B. J., (2003). *Persuasive Technologies: Using Computers to Change What We Think and Do*, San Francisco, 2003, 313.

GARANTE PROTEZIONE DATI PERSONALI, (2013). *Doc. web n. 2574977 sulle "Linee guida redatte dall'Agenzia per l'Italia*

Digitale ai sensi dell'art. 58, comma 2, del D. Lgs. 7 marzo 2005, n. 82 (CAD)".

GATES, B., (2007). *A Robot in Every Home*, in *Scientific American*, gennaio 2007, 58.

GOZZANO, S., (1990). *I cinque sensi dei robot. Percezioni artificiali: l'informatica non imita solo l'intelligenza ma anche le capacità sensoriali*, in *Sapere*, 1990, IV, 9.

KENT, K., CHEVALIER, S., GRANCE, T. E DANG, H., (2006). *Guide to integrating Forensic Techniques into Indente Response*, NIST publication. Disponibile al seguente URL: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

KERR, O.S., (2004). *The Fourth Amendment and New Technologies. Constitutional Myths and the Case for Caution*, in *Michigan Law Review*, 2004, 801.

HUMPHREY, T., (2012). *Statement on the vulnerability of Civil Unmanned Aerial Vehicles and other systems to civil GPS spoofing*, Submitted to the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security, 18 luglio 2012. Disponibile al seguente URL: http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Humphreys.pdf.

EUROPEAN DATA PROTECTION SUPERVISOR, (2014). *Opinion on the Communication from the Commission to the European Parliament and the Council on "A New Era for Aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner"*, 26-11-2014.

INFORMATION COMMISSIONER'S OFFICE, (2015). *In the picture: A data protection code of practice for surveillance cameras and personal information*, v. 1.1. Disponibile al seguente URL: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf.

MAIOLI, C., (2004). *Introduzione all'informatica forense,* in *la sicurezza preventiva della comunicazione*, a cura di P. Pozzi, F. Angeli, Torino. Disponibile al seguente URL: http://www.jus.unitn.it/users/dinicola/criminologia-ca/topics/materiale/dispensa_4_1.PDF.

MCNALLY, P., INAYATULLAH, S., (1987). *The rights of robots: Technology, culture and law in the 21st century*, in *L. & Tech.*, 1987, IV, 20.

MILLER, C., VALASEK, C., (2013). *Adventures in Automotive Networks and Control Units*. Report disponibile al seguente URL: http://illmatics.com/car_hacking.pdf.

MORI, M., (1970). *Bukimi no tani - The uncanny valley*, in *Energy*, 1970, IV, 33.

NOTO LA DIEGA, G., (2014). Cloud computing *e protezione dei dati nel* web *3.0*, in *Giustiziacivile.com*, 5-4-2014.

PAGALLO, U., (2013). *The Laws of Robots: Crimes, Contracts, and Torts*. Springer, Dordrecht.

PUTNAM, H., (1987). *Mente, linguaggio e realtà*, Milano 1987.

RAY, I., (2006). *Remote Upload of Evidence over Mobile ad hoc Network*, in *Advances in Digital Forensics II*, a cura di M S. Olivier, S. Shenoi, Springer.

RUBINSTEIN, I. S., GOOD, N., (2012). *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, Public Law & Legal Theory Research Paper Series Working Paper n. 12-43, 2012, 1333.

SARZANA DI S. IPPOLITO, C., (1994). *I riflessi giuridici delle nuove tecnologie informatiche*, in *Dir. inf.*, 1994, III, 505.

SCHACTMAN, N., (2003). *Drones See, Smell Evil from Above*, in *Wired.com*, 24-3-2003.

SHARKEY, N., (2011). *Automated Warfare: Lessons Learned from the Drones*, in *Journal of Law, Information and Science*, 21(2): 10.5778/JLIS.2011.21.

SHARKEY, N., (2008). *2084: Big Robot is Watching You. Report on the Future of Robots for policing, surveillance and security*,

2008. Disponibile al seguente URL: www.scribd.com/mobile/doc/139971746.

SHEN, W. M., (2012). *Robotics Research for Cybersecurity*, Polymorphic Robotics Laboratory, University of Southern California.

SHEPPARD, B., THOMPSON, T., (2014). *Cyber Security for Robots: Scenarios for 2030. Cyber-Enhanced Well-Being or Artificial Retardation*?, *Institute for Alternative Futures*. Report disponibile al seguente URL: http://www.roboticsbusinessreview.com/pdfs/Cyber_Security_for_Robots_Scenarios_IAF_5_Feb_2014_(1).pdf.

SIMOU, S., KALLONIATIS, C., KAVAKLI, E., GRITZALIS, S., (2014). *Cloud Forensics: Identifying the Major Issues and Challenges*, in *Lecture Notes in Computer Science Volume 8484*, 271-284. Disponibile al seguente URL: https://www.academia.edu/7120726/Cloud_Forensics_Identifying_the_Major_Issues_and_Challenges.

SINGER, P.W., (2009). *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. London, Penguin.

SOLOVE, D., (2004). *The Digital Person: Technology and Privacy in the Digital Age*, New York, 2004, 36.

SPAFFORD, E., (1989). Citato in *Computer Recreations: Of Worms, Viruses and Core War*, a cura di A. K. DEWDNEY in *Scientific American*, March 1989.

UN WORLD ROBOTICS (2005). *Statistics, Market Analysis, Forecasts, Case Studies and Profitability of Robot Investment*, edited by the UN Economic Commission for Europe and co-authored by the International Federation of Robotics, UN Publication, Geneva (Switzerland).

ZATIKO, K., (2007). *Commentary: Defining digital forensics*, in *Forensic Magazine*. Disponibile al seguente URL: http://www.forensicmag.com/node/128.

ZITTRAIN, J., (2008). *The Future of the Internet: And How to Stop It*, New Haven, 2008, 110.