RSD
Rivista Semestrale di Diritto

RIVISTA SEMESTRALE DI DIRITTO

ISSN 2724-2862

Numero 2/2020

Dicembre 2020

ISSN 2724-2862

Direttore Scientifico

Dott.ssa Caterina Del Federico

Vicedirettori

Dott. Simone Cedrola
Dott. Pasquale La Selva
Dott.ssa Claudia Cantone

Direttore

Dott. Riccardo Guarino

Comitato di Direzione

Piera Di Guida, Claudia Calderini, Rossana Grauso, Gianluca Barbetti, Claudia Addona, Mario Nocera

Comitato di Redazione

Giulia Cavallari, Andrea Nicosia, Carlo Pezzullo, Michele D'Onofrio, Rossella Giuliano.

Comitato scientifico

Amedeo Arena (Università Federico II), Marco Bassini (Università Bocconi), Gianluca Bertolotti (Università Roma III), Federico Caporale (Università della Sapienza), Alfonso Maria Cecere (Università Federico II), Alfonso Celotto (Università Roma III), Nicoletta Corrocher (Università Bocconi), Giovanni Comazzetto (Università di Padova), Paolo Costa (Università Cattolica), Massimo Rubino De Ritis (Università Luigi Vanvitelli), Francesco De Santis (Università Federico II), Lorenzo Del Federico (Università di Chieti-Pescara), Massimiliano Delfino (Università Federico II), Gabriele Della Morte (Università Cattolica), Giusella Finocchiaro (Università di Bologna), Federico Girelli (Università Cusano), Lucio Imberti (Università di Milano), Marco Imperiale (Harvard University), Maria Beatrice Magro (Università Marconi), Maria Luisa Mancusi (Università Cattolica), Laurent Manderieux (Università Bocconi), Arturo Maresca (Università della Sapienza), Stefano Mele (Università di Foggia), Alessandro Milone (Università Parthenope), Lilla' Montagnani (Università Bocconi), Fulvio Palombino (Università Federico II), Nicoletta Parisi (Università Cattolica), Elisabetta Pederzini (Università di Torino), Giovanna Petrillo (Università Luigi Vanvitelli), Lucia Picardi (Università Federico II), Cinthia Pinotti (Corte dei Conti, Piemonte), Filippo Pizzolato (Università di Padova), Ludovica Poli (Università di Torino), Concetta Ricci (Università del Molise), Carlo Rossi Chauvenet (Università Bocconi), Andrea Saccucci (Università Luigi Vanvitelli), Adriana Salvati (Università Luigi Vanvitelli), Giovanni Sartor (Università di Bologna), Michele Tamponi (LUISS), Giovanni Terrano (Università Federico II), Roberto Virzo (Università del Sannio), Roberto Zannotti (Università LUMSA), Giovanni Zarra (Università Federico II), Giovanni Ziccardi (Università di Milano).

Sede

Ius in itinere Srls, Via Santa Lucia, 34 Napoli - Partita Iva 08593431219

Info e contatti

Sito web: www.rivistadidiritto.it

Per l'invio dei contributi scrivere a: redazione@iusinitinere.it

Per qualsiasi informazione scrivere a: info@iusinitinere.it

RSD
Rivista Semestrale di Diritto

Indice

Articoli

Dott. Raffaele Cantone – *La prevenzione della corruzione nelle società pubbliche* p. 7

Prof.ssa Nicoletta Parisi e Prof. Dino Rinoldi – *Misure di prevenzione personale e libertà di movimento* p. 67

Saggi

Prof. Alberto Artosi e Dott. Luigi Russi – *Dispositivi sessuali. Il diritto alla prova del sesso artificiale* p. 87

Dott.ssa Valeria Bilotto – *Comunicazione, conoscenza e pubblicazione del provvedimento amministrativo: la corretta individuazione del dies a quo dell'impugnazione nella specifica ipotesi dell'impugnazione dell'aggiudicazione dei contratti pubblici di lavori, servizi e forniture. Breve riflessione alla luce delle risultanze dell'Adunanza Plenaria n. 12/2020.* p. 103

Prof. Lorenzo Del Federico – *La tutela del contribuente nell'evoluzione del diritto tributario internazionale: dagli accordi amministrativi fra autorità fiscali alle procedure arbitrali* p. 130

Dott. Davide Gasparini – *Dai modelli legali al comodato "di terzo genere"* p. 153

Dott.ssa Federica Marconi – *Brevi riflessioni in tema di tutela della privacy durante la pandemia Covid-19. Il caso dell'impiego dei droni per la verifica del rispetto delle misure di contenimento e contrasto alla diffusione del virus* p. 168

Dott.ssa Emanuela Morotti – *Rilievi critici sulla possibilità di configurare l'abuso del promissario acquirente nella nuova disciplina degli immobili da costruire* p. 185

Dott. Andrea Nicosia – *Lo scioglimento degli Enti locali per infiltrazioni mafiose. Riflessioni alla luce della relazione della Commissione d'inchiesta e vigilanza sul fenomeno della mafia e della corruzione in Sicilia dell'Assemblea Regionale Siciliana* p. 198

Dott. Andrea Persichillo – *L'apertura della Corte Costituzionale alla società civile. Alcuni spunti di riflessione* p. 215

Dott. Giacomo Piersanti – *La riparazione pecuniaria ex art. 332 quater c.p.: tra visioni interne e proiezioni convenzionali* p. 235

Dott. Giulio Soana – *L'accesso transfrontaliero alla prova informatica. Oltre il principio di territorialità* p. 254

RSD
Rivista Semestrale di Diritto
ISSN 2724-2862
Articolo scientifico sottoposto a referaggio ai sensi dell'art. 3 del Regolamento della Rivista

Brevi riflessioni in tema di tutela della privacy durante la pandemia Covid-19. Il caso dell'impiego dei droni per la verifica del rispetto delle misure di contenimento e contrasto alla diffusione del virus.

A cura della **Dott.ssa Federica Marconi**[1]

ABSTRACT

La continua evoluzione del contesto emergenziale generato dalla crisi sanitaria da Covid-19, ha posto l'esigenza di adottare misure volte ad assicurare la verifica sul pieno rispetto delle disposizioni dettate in materia di contenimento e contrasto alla diffusione dell'epidemia. Il non sempre pieno rispetto di tali misure da parte dei cittadini dei diversi Stati colpiti dal virus ha spinto questi ultimi a ricorrere a strumenti di controllo e monitoraggio generalizzati, più o meno invasivi della sfera personale. Tra questi, si annovera l'utilizzo di sistemi di riconoscimento biometrico, di geolocalizzazione o di videosorveglianza. Sembra che le nuove tecnologie si stiano conquistando, sempre più, un ruolo da protagoniste nella lotta al virus, dimostrandosi particolarmente efficaci nel combatterne la diffusione. Ci si chiede allora: fino a che punto lo stato di emergenza – in una situazione di crisi senza precedenti come quella attuale – può giustificare la compressione del diritto alla riservatezza dei dati? Entro che limiti le democrazie occidentali possono ricorrere a strumenti che, come i droni, consentono di realizzare una sorveglianza sistematica e generalizzata nei confronti della totalità della popolazione? Entro quale perimetro le misure per verificare il rispetto degli obblighi di permanenza domiciliare e distanziamento sociale potrebbero dirsi realmente conformi al canone di proporzionalità? Fin dove l'enforcement pubblicistico può spingersi ad impiegare strumenti lesivi della libertà personale senza che questo sfoci in forme più o meno inedite di controllo sociale?

[1] Avvocato presso l'ordine degli avvocati di Roma e dottorando in "Teoria dei Contratti, dei Servizi e dei Mercati" presso la Facoltà di Economia dell'Università degli Studi di Roma Tor Vergata, dove è cultore della materia sulle cattedre di Diritto Pubblico dell'Economia; Istituzioni finanziarie europee; European Institutions, Law and Markets.

ABSTRACT

The Covid-19 outbreak is severely testing the democratic systems of most advanced countries. A lively debate has arisen with regard to the emergency measures adopted by several European countries to contain and fight the spread of the virus. Due to the outgoing health crisis and because of the consequent economic and social issues, most countries have been adopting measures to monitor the public compliance with lockdown regulations and to encourage or enforce social distancing. Some States have begun deploying generalized control and monitoring tools, more or less invasive in the personal sphere, to monitor individual activities such as whether or not people are complying with social distancing.

Technologies like biometric recognition, GIS and mapping, location technology or video surveillance systems are playing a growing key role in responding to Covid-19 pandemic, by helping authorities and people in different ways to prevent further spread of the coronavirus outbreak. Although, ongoing aerial surveillance and surveillance to track individual's health raise serious issues regarding to the erosion of citizen's constitutional rights, such as their privacy rights.

Several questions arise: can the state of emergency - in a crisis situation as unique as the current one - justify the compression of the right of personal data protection? How can the adoption of tools like drones – which may carry out systematic and generalized surveillance on the entire population – be considered justified within the legal framework of democratic countries? To what extent can measures to verify compliance with emergency regulations and to ensure social distancing really be considered compliant with the principle of proportionality? How far can public enforcement go in using instruments that infringe personal freedom? Beyond which limit must the surveillance capabilities of this technology be considered as unprecedented digital forms of social control?

PAROLE CHIAVE

misure emergenziali, Covid-19, Privacy, Droni, European Data Protection Board.

Sommario: 1. Il caso italiano: la nota ENAC sull'impiego dei droni. – 2. Contesto normativo di riferimento e dichiarazioni del European Data Protection Board: come garantire che l'enforcement pubblico sia privacy compliant*?* – 3. Prospettiva comparata: brevi cenni sulla pronuncia del Conseil d'État sulla inammissibilità della sorveglianza del rispetto delle norme Covid-19 per mezzo dei droni. 4 – Brevi riflessioni conclusive.

1. Il caso italiano: la nota ENAC sull'impiego dei droni

L'Organizzazione Mondiale della Sanità, dopo aver riconosciuto e dichiarato il carattere pandemico della diffusione del Covid-19, si è rivolta agli Stati consigliando di intensificare la sorveglianza attiva per rendere più facile e celere l'identificazione di individui infetti, al fine di attuare un rapido isolamento e/o eventuale quarantena. Cogliendo tali indicazioni, l'Italia, come molti altri Paesi europei, ha fatto ricorso all'impiego dei droni per attuare rigorosamente la sorveglianza durante e nella fase immediatamente successiva al lockdown generalizzato: ciò ha sollevato ovvie preoccupazioni in materia di protezione dei dati personali e di privacy, proprio in quanto i droni – se e quando utilizzati per la sorveglianza – risultano dotati di telecamere di bordo o di altri sensori capaci di raccogliere informazioni e monitorare gli spostamenti.

L'Ente Nazionale per l'Aviazione Civile - ENAC, con provvedimento del 23 marzo 2020[2] ha autorizzato in via generalizzata le forze dell'ordine ad impiegare i droni[3] per il contrasto alla diffusione del Covid-19[4] «[…] nell'ottica di garantire il contenimento dell'emergenza epidemiologica "coronavirus", al fine di consentire le operazioni di monitoraggio degli spostamenti dei cittadini sul territorio comunale», così come previsto dai DPCM dell'8 e del 9 marzo 2020.[5] In particolare, sono state dettate disposizioni derogatorie rispetto a quanto originariamente previsto dal Regolamento ENAC relativo a "Mezzi Aerei a Pilotaggio Remoto[6]", per le operazioni condotte con sistemi aeromobili a pilotaggio remoto con mezzi aerei di massa operativa inferiore a 25 kg nella disponibilità dei Comandi di Polizia Locale e impiegati nelle attività di monitoraggio. Tra queste, è stata ammessa la possibilità di effettuare operazioni critiche

[2] Nota ENAC, prot. 23/03/2020-0032363-P, relativa ai "Provvedimenti governativi emergenziali in vigore fino al 03/04/2020 – Utilizzo dei droni" e rivolta ai Ministeri dell'Interno, delle Infrastrutture e dei Trasporti, della Giustizia e al Dipartimento dell'Amministrazione penitenziaria. Hanno fatto seguito le ulteriori note di aggiornamento del 31/03/2020 prot. 34875-P; del 09/04/2020 prot. 36155-P; del 16/04/2020 prot. 39230-P; del 30/04/2020 prot. 43446-P.

[3] Con il termine droni si designano mezzi aerei a pilotaggio remoto che operano autonomamente o vengono pilotati a distanza. Per ricostruire una completa definizione è necessario fare riferimento al glossario dell'Organizzazione Internazionale dell'aviazione civile (CIR328, 2011); alla normativa europea (Reg. UE 2018/1139 del Parlamento europeo e del Consiglio del 04 luglio 2018, in vigore dal 11 settembre 2018 e recante "Norme comuni al settore dell'aviazione civile"); alla normativa nazionale, con particolare riferimento al Regolamento ENAC di cui di dirà infra.

[4] Ne costituisce un esempio quanto previsto dal Comune di Cagliari che ha impiegato i droni per verificare gli spostamenti delle persone e gli assembramenti in funzione anti contagio da coronavirus. Agli agenti della polizia locale, infatti, è stato assegnato il compito di pilotare tali velivoli a seguito del via libera da parte dell'ENAC. È stato previsto che, con cadenza quotidiana e fino al termine dell'emergenza, tali strumenti avrebbero dovuto sorvolare quartieri cittadini e zone "difficili da raggiungere". Veniva precisato, inoltre, che le riprese aeree sarebbero state effettuate inizialmente ad una quota tale da rendere impossibile il riconoscimento facciale, e solo in un secondo momento, laddove si fosse configurata una violazione ai decreti in vigore, la possibilità di abbassare la quota così da poter procedere ad una eventuale identificazione. Il drone – dotato di altoparlante, termocamera e camera – avrebbe inoltre potuto registrare eventuali richieste di soccorso.

[5] Art. 14, DL 9 marzo 2020, n. 14 "Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza COVID-19", in Gazzetta Ufficiale del 9 marzo 2020, n. 62 con cui, di fatto, si è consentito al sistema di prevenzione e contenimento del contagio di derogare alla disciplina della protezione dei dati personali dei cittadini sino al termine dello stato di emergenza. Si tenga conto che il Governo ha concesso alle Regioni la facoltà di adottare esercitare poteri straordinari in materia di privacy per far fronte all'emergenza Covid-19.

[6] Edizione 3 dell'11/11/2019. L'art. 34 di tale Regolamento rinvia genericamente al rispetto di quanto previsto nel Codice privacy, nonché delle misure e degli accorgimenti a garanzia dell'interessato prescritti dal Garante per la protezione dei dati personali.

in *Visual Line of Sight*[7] anche su aree urbane «dove vi è scarsa popolazione esposta al rischio di impatto» senza dover preventivamente avvalersi di specifica autorizzazione dell'Ente, anche qualora le operazioni da compiersi non rispondano agli scenari standard pubblicati[8]. Per lo stesso motivo, è stata disposta la deroga anche con riferimento alle previsioni relative all'obbligo di registrazione e di identificazione dei droni, oltre alla concessione della possibilità di volare nelle no fly zone aeroportuali ad un massimo di 15 metri di altezza dal suolo.

In tale contesto, si è posta la necessità di delineare il perimetro nell'ambito del quale le Polizie Locali potessero essere chiamate a concorrere alle attività finalizzate a garantire l'esecuzione e l'osservanza delle limitazioni della libertà di circolazione e di iniziativa economica, al fine di prevenire e di contrastare la propagazione del virus.[9]

Il Dipartimento della Pubblica Sicurezza del Ministero dell'Interno[10], dopo aver sospeso il ricorso a tali velivoli radiocomandati, ha stabilito che i Corpi di polizia locale possono impiegare i droni nell'espletamento dei compiti di sorveglianza loro attribuiti nel contesto emergenziale, solo previo coinvolgimento dei Prefetti e nel rispetto delle indicazioni da questi fornite. Viene evidenziato, inoltre, come il concorso prestato dalle Polizie Locali in occasione dell'emergenza Covid19 «sia preordinato ad assicurare la salvaguardia del bene giuridico della "salute pubblica", nella sua dimensione collettiva», trovando il proprio riconoscimento e fondamento nell'art. 32 della Costituzione.

Stante il riconoscimento della possibilità di far ricorso a tali strumenti - al fine di attuare un monitoraggio della popolazione e dei relativi spostamenti, di tracciare i contatti e di accertare eventuali violazioni alle disposizioni dettate dai decreti emergenziali – si è posto un ulteriore problema, di ben più complessa risoluzione: come operare il necessario bilanciamento tra diritti di pari dignità costituzionale coinvolti? L'impiego di tali strumenti impone, infatti, la necessità di operare un contemperamento tra, da un lato, il diritto alla salute – in una dimensione non solo individuale, quanto e soprattutto pubblica; dall'altro, il diritto alla riservatezza dei soggetti coinvolti e incisi da siffatte forme di controllo generalizzato.

A tale nota ha fatto seguito una ulteriore nota di aggiornamento resa dall'Ente Nazionale dell'Aviazione Civile[11], mediante la quale è stato preso atto delle indicazioni rese dal Ministero dell'Interno con particolare riferimento ai poteri dei Comuni. È stato previsto che i comuni sono tenuti, preventivamente

---

[7] E cioè entro una distanza orizzontale e verticale tale da consentire il contatto visivo continuativo con il dispositivo.

[8] In particolare, in deroga all'art. 10, par. 8, del Regolamento citato è, in ogni caso, consentito il sorvolo di assembramenti di persone o delle aree in cui si verifichino concentrazioni inusuali e non autorizzate di persone.

[9] Si noti comunque come la nota Enac parli di "disponibilità" e non di "proprietà" dei droni da parte della polizia locale. L'utilizzo di servizi forniti da terzi impone la formalizzazione di un accordo sulla protezione dei dati ai sensi dell'articolo 28 del GDPR, così come previsto anche dall'articolo 7, comma 3 del Regolamento Enac.

[10] Nota prot. 555/O.P./0001054/2020/2 del 30/03/2020, recante "Prevenzione della diffusione del virus "Covid-19" – indirizzi tecnici dell'ENAC e dell'ENAV concernenti l'utilizzo di sistemi aeromobili a pilotaggio remoto (SAPR) da parte del personale dei Corpi e Servizi di polizia locale".

[11] Nota ENAC – prot. 31/03/2020 – 0034875, indirizzata a: Ministero dell'Interno, Ministero delle Infrastrutture e Trasporti, Dipartimento della Protezione Civile, Stato Maggiore dell'Aeronautica, Ministero della Giustizia – Dipartimento Amministrazione Penitenziaria, ENAV S.p.A., Associazione Nazionale dei Comuni Italiani, Comandi Polizie locali.

all'utilizzo dei SAPR[12] da parte delle polizie locali, a informare e a coordinarsi con i Prefetti delle città di riferimento, indicando le aree urbane dove si intendono concentrare prevalentemente i controlli con l'utilizzo dei droni.

La nota, fornendo indicazioni di carattere tecnico – per quanto qui di interesse – evidenzia che per gli aeromobili a pilotaggio remoto con massa operativa inferiore a 25 kg, a prescindere dalle operazioni effettuate, è necessario procedere alla registrazione dell'operatore nel portale *d-flight,* alla identificazione del mezzo tramite apposizione del QR code e al rispetto delle regole di circolazione e utilizzo dello spazio aereo.[13] Le operazioni di volo in ambiente urbano sono classificate come "operazioni critiche"[14] e risultano assoggettate ai stringenti requisiti alternativi quali una autorizzazione richiesta dall'operatore ed emessa dell'ENAC[15], una dichiarazione dell'operazione in caso di volo in "scenari standard"[16], ovvero l'utilizzo di mezzi di peso minore o uguale a 2 kg con caratteristiche di inoffensività accertata dall'ENAC[17], di peso minore o uguale a 300 g con parti rotanti protette da impatto accidentale e con velocità massima minore o uguale a 60 km/h.[18]

Circa gli aeromobili a pilotaggio remoto delle Polizie locali, non essendo questi classificabili come *"aeromobili di Stato"*[19] e risultando, dunque, assoggettati al Regolamento ENAC e alla Circolare ATM 09, l'ENAC ha deciso di derogare l'applicazione delle disposizioni sopra elencate nel caso di operazioni condotte dalle amministrazioni di Polizia locale con propri mezzi e piloti. Per tali operazioni, infatti, l'Amministrazione locale assume gli obblighi e le responsabilità dell'operatore privato di cui all'art. 11 del Regolamento citato. In aggiunta, è stato previsto che – in assenza di droni nella diretta disponibilità delle Polizie locali – queste possano avvalersi di mezzi e piloti appartenenti all'organizzazione di operatori terzi, purché già registrati e noti all'ENAC, al fine di affiancare l'amministrazione di Polizia locale, e operando sotto le indicazioni e la responsabilità di quest'ultima.

---

[12] Acronimo di "sistemi aeromobili a pilotaggio remoto", e cioè un sistema costituito da un mezzo aereo (aeromobile a pilotaggio remoto, c.d. "APR") senza persone a bordo, utilizzato per fini diversi da quelli ricreativi e sportivi, e dai relativi componenti necessari per il controllo e comando (stazione di controllo) da parte di un pilota remoto. La nota precisa che «[…] secondo le previsioni contenute nell'articolo 743 del Codice della Navigazione, i mezzi aerei a pilotaggio remoto sono degli aeromobili e, al fine di dare attuazione alle previsioni codicistiche, l'ENAC, con il Regolamento "Mezzi aerei a Pilotaggio Remoto" e con la Circolare ATM 09, ha definito le disposizioni per il loro utilizzo nello spazio aereo nazionale».

[13] Rispettivamente: art. 8, comma 1 e art. 24 del Regolamento citato.

[14] Cfr. art. 10 del Regolamento citato. In particolare, al comma 3, si precisa che «Le operazioni critiche possono essere condotte ove sia assicurato un livello di sicurezza coerente con l'esposizione al rischio». 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.

[15] Art. 11, comma 6, Reg. cit.

[16] Artt. 11, comma 1, e art. 10, comma 2, Reg. cit.

[17] Art. 12, comma 1, Reg. cit.

[18] Art. 12, comma 5, Reg. cit.

[19] Ai sensi del Codice della navigazione sono tali «[…] gli aeromobili militari e quelli, di proprietà dello Stato, impiegati in servizi istituzionali delle Forze di polizia dello Stato, della Dogana, del Corpo nazionale dei vigili del fuoco, del Dipartimento della protezione civile o in altro servizio di Stato». Al contrario, tutti gli altri aeromobili sono da considerarsi privati. Tuttavia, il quarto comma precisa che «sono equiparati agli aeromobili di Stato gli aeromobili utilizzati da soggetti pubblici o privati, anche occasionalmente, per attività dirette alla tutela della sicurezza nazionale».

Da ultimo, la nota ribadisce la deroga espressa alle disposizioni in materia di circolazione e di utilizzo dello spazio aereo, evidenziando che è consentito alle Forze di Polizia, della Dogana, dei Vigili del Fuoco e del Dipartimento della Protezione civile, nonché alla Forze di Polizia locale, operare anche in prossimità degli aeroporti e fino ad una altezza massima di 15 metri, pur di far fronte alla grave situazione attuale.

2. Contesto normativo di riferimento e dichiarazioni del European Data Protection Board: come garantire che l'enforcement pubblico sia privacy compliant?

Il graduale inserimento dei droni nello spazio aereo civile è stato realizzato a partire dalla Comunicazione COM (2014) 207 della Commissione europea.[20] Ha fatto seguito una serie di interventi volti ad adeguare il quadro regolamentare di riferimento, al fine di garantire un appropriato contemperamento tra la possibilità di impiegare i droni – tanto più se dotati sensori audio/video, sia da parte di soggetti privati che da parte di soggetti pubblici – e la necessità di assicurare il rispetto dei diritti fondamentali nel contesto europeo, senza comportare l'introduzione di forme "atipiche" di sorveglianza.

La sfida più grande affrontata dal legislatore – europeo e dei singoli Stati membri – è stata dunque quella di assicurare il bilanciamento tra il libero impiego dei droni e il rispetto della disciplina sulla privacy, tanto in una dimensione di utilizzo privato, quanto e soprattutto con riferimento al potenziale uso che degli stessi può essere fatto da parte dell'apparato pubblicistico con finalità di monitoraggio generalizzato.

In particolare, la legittimità dell'impiego di tali strumenti veniva subordinata al rispetto delle disposizioni vigenti in materia di protezione dei dati, e soprattutto di quanto stabilito dalle misure nazionali istituite a norma della Direttiva 95/46/CE sulla protezione dei dati e della Decisione Quadro 2008/977.[21] Specificava, inoltre, che qualsiasi trattamento dei dati avrebbe dovuto trovare la proprio base in un motivo legittimo, tenuto conto che il diritto alla riservatezza si estende non solo agli spazi privati ma anche a quelli pubblici.[22]

---

[20] Bruxelles, 08/04/2014, COM (2014) 207, recante "Comunicazione della Commissione al Parlamento Europeo e al Consiglio – 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". Al paragrafo 3.4. ("Tutelare i diritti fondamentali dei cittadini") veniva ribadito che le operazioni dei sistemi RPAS non devono portare alla violazione di diritti fondamentali – quali il diritto alla vita privata e familiare e la tutela dei dati personali. Riconosceva, altresì, che nella vasta gamma delle potenziali applicazioni civili dei sistemi RPAS 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.

[21] Rispettivamente: Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati; GU L 281, del 23 novembre 1995, pp. 31-50. Ora abrogata dal Reg. UE/2016/679, cd. *GDPR* e Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale.

[22] Corte eu. Dir. uomo, 7 febbraio 2012, Sentenza Von Hannover v. Germania, che ha evidenziato come «[…] il concetto di vita privata si estende agli aspetti relativi all'identità personale, come il nome, la foto o l'integrità fisica e morale di una persona; la garanzia offerta dall'articolo 8 della Convenzione mira principalmente a garantire lo sviluppo, senza interferenze esterne, della personalità di ciascun individuo nelle sue relazioni con altri esseri umani. Esiste quindi una zona di interazione di una persona con gli altri, anche in un contesto pubblico, che può rientrare nell'ambito della vita privata».

A completamento di ciò, doveva necessariamente tenersi conto di quanto previsto – a tutela della vita privata e dei dati di carattere personale – dalla CEDU[23] e dalla Carta dei Diritti dell'Unione Europea.[24]
L'anno successivo, viene redatta l'Opinion n. 1/2015 dal Working Party 29[25] nella quale si ribadiva che eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti e tutelati dalla Carta di Nizza e dalla Convenzione Europea, devono necessariamente trovare il proprio fondamento in una previsione legislativa (testualmente, "in accordance with law") e che potevano dirsi ammissibili nella misura in cui ciò fosse necessario per il soddisfacimento dell'interesse generale come garantito dall'Unione Europea, ovvero per il perseguimento di una o più delle finalità legittime previste all'art. 8, comma 2, della CEDU.
La stessa Opinion, con riferimento all'impiego dei droni, chiariva che il loro utilizzo non presenta di per sé rilevanti problematiche: le questioni sorgono, d'altra parte, quando si rivolge l'attenzione agli effetti invasivi che possono derivare dai dispositivi installati sui droni stessi e in grado di catturare immagini.
Il Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, ha successivamente istituito l'Agenzia dell'Unione europea per la sicurezza aerea al fine di dettare regole comuni a livello europeo nel settore dell'aviazione civile. Si è così provveduto a sostituire il previgente quadro legislativo risalente al 2008 (c.d. "Basic Regulation") e a ricondurre nel perimetro delle competenze UE anche la regolamentazione degli aeromobili senza equipaggio con un peso inferiore a 150 kg, prima riservata ai singoli Stati membri.
Da ultimo, la cornice normativa di cui sopra è stata completata dal Regolamento UE 945/2019 – che stabilisce i requisiti di conformità in fase di progettazione e fabbricazione, in vigore dal primo luglio 2019 – e dal Regolamento UE 947/2019 – che detta disposizioni per l'utilizzo dei droni, in vigore dal primo luglio 2019, con efficacia a decorrere dal primo luglio 2020 – termine rinviato di sei mesi proprio a causa dell'emergenza Covid-19.

---

[23] Art. 8 della Convenzione Europea dei diritti dell'uomo e del cittadino, che sancisce il diritto di ogni persona al rispetto della propria vita privata e familiare, nonché del proprio domicilio e della corrispondenza. Al comma 2 è specificato che non può esservi ingerenza da parte di una autorità pubblica nell'esercizio di tale diritto, salvo che «tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».
[24] Artt. 7 e 8 della Carta di Nizza, rispettivamente a tutela del diritto al rispetto della propria vita e familiare, del domicilio e delle comunicazioni e a protezione dei dati di carattere personale. Tali articoli specificano che i dati di carattere personale devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Il comma 1 dell'art. 52 stabilisce che eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta «devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».
[25] Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilization of Drones, adottata il 16 giugno 2015 dal Article 29 Data Protection working party. Si segnalava, in particolare, la possibilità di ricorrere all'impiego dei droni quali strumenti utilizzabili in chiave di law enforcement da parte di autorità pubbliche e il conseguente rischio elevato per la libertà degli individui, tenuto contro della interferenza diretta «[…] with the rights to respect for prvate life and to the protection of personal data protected under Article 8 of the European Convention of Human Rights ("ECHR") and Article 7 and 8 of the Europea Charter of Fundamental Rights ("Charter")».

A conferma della strettissima correlazione che intercorre tra utilizzo dei droni e tutela delle istanze connesse al tema della privacy, il Regolamento 2018/1139 contiene un espresso riferimento alla necessità che le norme riguardanti gli aeromobili senza equipaggio contribuiscano al rispetto di quanto previsto dal Regolamento UE 2016/679 in materia di protezione dei dati personali.[26]

L'art. 72, relativo a "Raccolta, scambio e analisi di informazioni", specifica che la Commissione, l'Agenzia e le autorità nazionali competenti, nonché le persone fisiche e giuridiche possono adottare, conformemente al diritto nazionale e a quello dell'Unione, le misure necessarie per garantire l'opportuna riservatezza delle informazioni da essi ricevute e che in alcun modo risultano pregiudicati eventuali obblighi più rigorosi di riservatezza previsti dai regolamenti (UE) n. 996/2010 e (UE) n. 376/2014, oppure da altra legislazione dell'Unione.

Alla tutela della riservatezza dei dati personali si fa altresì riferimento nell'Allegato IX del Regolamento, laddove è individuato quale requisito essenziale degli aeromobili senza equipaggio quello di «[…] possedere le relative caratteristiche e funzionalità specifiche che tengono conto dei principi della tutela della riservatezza e della protezione dei dati personali fin dalla progettazione e per impostazione predefinita».[27]

Ai sensi del GDPR, dunque, tutti gli strumenti e le attività che comportano la raccolta e il trattamento dei dati personali – salvo specifiche eccezioni – devono rispettare le disposizioni ivi contenute.

L'art. 5, comma 1, del Regolamento citato, nell'elencare i principi relativi al trattamento dei dati personali, alla lett. c), prevede la c.d. "minimizzazione dei dati", e cioè che gli stessi siano "adeguati, pertinenti e limitati" a quanto necessario rispetto alle finalità per le quali sono trattati.[28] Ciò, evidentemente, non sembra di per sé escludere la possibilità per lo Stato di continuare ad impiegare mezzi tecnologici – quali i droni – che consentano di catturare e registrare immagini.

---

[26] Si veda il Considerando 28, secondo cui le norme riguardanti gli aeromobili senza equipaggio dovrebbero contribuire al rispetto dei diritti garantiti dal diritto dell'Unione: in particolare, al rispetto della riservatezza e della vita familiare, così come sancito dall'articolo 7 della Carta dei diritti fondamentali dell'Unione europea, e alla protezione dei dati di carattere personale, sancita dall'articolo 8 della Carta e dall'articolo 16 TFUE, e disciplinato dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio. Il Considerando 33 prevede che dovrebbe essere possibile vietare, limitare o subordinare a determinate condizioni le attività di cui al capo III del Regolamento, se necessario nell'interesse della sicurezza dell'aviazione civile. Tale possibilità dovrebbe essere esercitata in conformità degli atti delegati e di esecuzione adottati dalla Commissione a tal fine. Gli Stati membri hanno la possibilità di adottare misure, conformemente al diritto dell'Unione, che non rientrano nell'ambito di applicazione del Regolamento, per motivi quali la pubblica sicurezza e la protezione del diritto alla riservatezza e la protezione dei dati di carattere personale.

[27] L'Allegato IX – "Requisiti essenziali degli aeromobili senza equipaggio – 1. Requisiti essenziali per la progettazione, la produzione, la manutenzione e l'esercizio di aeromobili senza equipaggio" prevede che se necessario al fine di attenuare i rischi inerenti alla sicurezza, alla tutela della riservatezza, alla protezione dei dati personali, alla sicurezza o all'ambiente derivanti dal loro esercizio, «gli aeromobili senza equipaggio devono possedere le relative caratteristiche e funzionalità specifiche che tengono conto dei principi della tutela della riservatezza e della protezione dei dati personali fin dalla progettazione e per impostazione predefinita». In base alle necessità, infatti, tali caratteristiche e funzionalità devono garantire una facile identificazione dell'aeromobile, come pure della natura e della finalità del suo impiego; esse devono inoltre garantire che siano rispettati le limitazioni, i divieti o le condizioni applicabili, in particolare per quanto riguarda l'esercizio in particolari zone geografiche, al di là di una certa distanza dagli operatori o a determinate altitudini.

[28] Il rispetto del principio di minimizzazione implica che nel trattare i dati raccolti si favorisca, tra quelle astrattamente disponibili per il raggiungimento dello scopo immediato, la modalità con minore impatto sui diritti degli individui.

Allo stesso tempo però, l'art. 6, comma 1, lett. e) stabilisce che il trattamento di dati personali possa considerarsi lecito solo se e nella misura in cui, tra le altre, ricorra la circostanza che lo stesso sia necessario «[…] per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento».[29] Quest'ultimo, tuttavia, deve trovare la propria base giuridica nel diritto dell'Unione, ovvero nel diritto di uno Stato membro a cui è soggetto il titolare del trattamento, dovendosi al contrario ammettere il trattamento dei dati personali a seguito del rilascio del consenso informato, in ragione dell'esecuzione di un contratto, per la salvaguardia di interessi vitali dell'interessato o di altra persona fisica, per il perseguimento del prevalente legittimo interesse del titolare del trattamento o di terzi che risulti prevalente rispetto all'interesse dei soggetti interessati a non essere ripresi.

La compatibilità delle misure adottate con le previsioni di cui all'art. 34 del Regolamento sulla Protezione dei dati personali – relativo alle comunicazioni di violazioni dei dati personali all'interessato – è stata confermata, da ultimo, dalla Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di Covid-19, adottata il 19 marzo 2020 dal European Data Protection Board.

Viene precisato che le norme in materia di protezione dei dati non ostacolano l'adozione di misure per il contrasto della pandemia da Coronavirus, ciò nonostante, anche in questi momenti eccezionali, i titolari e i responsabili del trattamento dei dati devono garantire la protezione dei dati personali dei soggetti interessati: l'emergenza è una condizione giuridica che può legittimare limitazioni delle libertà, a condizione che tali limitazioni siano proporzionate e confinate esclusivamente al periodo di emergenza.

Nella dichiarazione resa dal European Data Protection Board si evidenzia l'interesse condiviso da tutti i Paesi flagellati dal virus ad arginarne la diffusione, anche mediante il ricorso a tecniche e strumenti moderni. I dati personali che tali strumenti sono in grado di raccogliere devono comunque essere quelli strettamente necessari per conseguire gli obiettivi prefissati e possono essere trattati solo per finalità predeterminate ed esplicite. A ciò deve aggiungersi che gli interessati dovrebbero ricevere informazioni trasparenti circa le attività di trattamento dei dati da svolgere, sulle loro caratteristiche principali, sul periodo di conservazione dei dati e sulle finalità del trattamento.

Ne consegue che, nel caso di specie, i dati raccolti non potranno essere impiegati per finalità diverse da quelle del monitoraggio, né tantomeno conservati per un tempo superiore allo strettamente necessario.

La misura descritta, riconducibile alla categoria relativa al "trattamento dei dati relativi all'ubicazione di soggetti" deve, dunque, rispondere a principi di necessità, adeguatezza e proporzionalità, rappresentando

[29] Si precisa che per "trattamento" dei dati deve intendersi qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. Per "titolare del trattamento", invece, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

una forma di controllo meno invasiva, rispetto – ad esempio – a quelle che prevedono il tracciamento dei dati attraverso i sistemi di localizzazione dei telefoni cellulare.[30]

Si segnala che, con riferimento alla disciplina nazionale, ai sensi dell'art. 126 del Codice della privacy[31] i dati relativi all'ubicazione geografica dei cittadini – diversi dai dati relativi al traffico – e riferiti agli utenti o agli abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, possono essere trattati solo se anonimi o se l'utente o l'abbonato abbiano preventivamente prestato il proprio consenso, revocabile in ogni momento, nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto. In questo ultimo caso, a svolgere le attività di tracciamento devono essere solo soggetti pubblici per le finalità di tutela della salute e sicurezza sociale.[32]

L'art. 23 del GDPR consente agli Stati membri di limitare con norme di diritto interno, per finalità e categorie di dati specifici, la portata degli obblighi e dei diritti che costituiscono il *core* del diritto alla privacy, al fine di salvaguardare interessi superiori tra cui la sicurezza pubblica o un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale.

Si comprende allora come il provvedimento ENAC, di cui sopra, giunga ad ammettere la raccolta di immagini e dati relativi alla localizzazione di cittadini sul territorio nazionale, purché l'uso dei droni sia limitato al solo periodo di emergenza da Covid-19 e al fine esclusivo di impedire la diffusione del virus. Ne consegue che tali dati non potranno essere impiegati per finalità differenti e ulteriori rispetto al monitoraggio, né tantomeno potranno essere conservati per un tempo superiore a quello necessario, rispondendo la loro conservazione esclusivamente alla necessità di irrogare la sanzione prevista in caso di inottemperanza alle misure di contenimento del contagio.

---

[30] In particolare, con riferimento a tali ulteriori e più invasive forme di controllo, l'attuale Presidente del Garante per la protezione dei dati personali ha evidenziato che in una situazione di emergenza sanitaria, economica e finanziaria come quella in corso è ammissibile qualche limitazione alle libertà personali, ma che mai tali circostanze possono costituire "scorciatoie pericolose" che consentano l'adozione di misure vicine al modello del sistema cinese, con la sua sorveglianza totale, o di quello della Corea del Sud. Al riguardo si veda l'intervista del 19 marzo 2020 reperibile sul sito del Garante per la protezione dei dati personali, sezione "Stampa e comunicazioni" – "Interviste e interventi".

[31] Decreto legislativo 30 giugno 2003, n. 196, integrato con le modifiche introdotto dal D.lgs. 10 agosto 2018, n. 101, art. 126, "Dati relativi all'ubicazione".

[32] Nel sistema delineato dal GDPR il consenso dell'interessato è una delle possibili condizioni di liceità del trattamento di dati personali. Tuttavia, quando viene in rilievo il trattamento di dati personali biometrici, dati relativi alla salute e dati relativi all'ubicazione – limitatamente, però, a quelli a disposizione dei fornitori di reti e servizi di telecomunicazione – la regola è quella del previo consenso dell'interessato (cfr. art. 9 GDPR e art. 126 D. Lgs. 196/2003, c.d. Codice della privacy). Per quanto riguarda i dati di ubicazione diversi da quelli delle telecomunicazioni – quali quelli desumibili, ad esempio, dai GPS del cellulare – vale dunque la regola generale di cui all'art. 6 GDPR.

3. Prospettiva comparata: brevi cenni sulla pronuncia del Conseil d'État sulla inammissibilità della sorveglianza del rispetto delle norme Covid-19 per mezzo dei droni.

Medesime questioni si sono poste in Francia, dove il Conseil d'État è stato chiamato a pronunciarsi sulla legittimità della sorveglianza a mezzo di droni per verificare e monitorare il rispetto delle norme sanitarie di contrasto alla diffusione del Covid-19.

Con *ordonnances* n. 440442 – 440445, del 18 maggio 2020 il Giudice adito ha ordinato di cessare immediatamente e senza indugio l'esecuzione delle misure di sorveglianza mediante droni, per controllare il rispetto delle norme sanitarie in vigore, applicabili durante il periodo di *déconfinement*. Ciò fino alla data dell'adozione di un testo regolamentare che avesse autorizzato il trattamento dei dati personali, nel rispetto delle disposizioni della legge del 6 gennaio 1978 e previo parere della Commissione nazionale sull'informatica e sulle libertà.

L'Associazione "La Quadrature du Net" e la "Ligue des droits de l'homme" avevano chiesto, infatti, al giudice dei *référés*[33] del Tribunale Amministrativo di Parigi di sospendere l'esecuzione della decisione del Prefetto di Polizia che aveva istituito, a far data dal 18 marzo 2020, un dispositivo finalizzato alla cattura di immagini da parte di droni, alla loro conservazione e al loro sfruttamento al fine di far rispettare le misure di confinamento. Chiedevano inoltre, l'immediata ingiunzione affinché tutte le immagini già catturate e raccolte fossero distrutte, sotto la pena della corresponsione di 1.024 euro per ogni giorno di ritardo. Con *ordonnance* del 5 maggio 2020, il giudice aveva respinto la richiesta avanzata, ritenendo non sussistente alcuna violazione manifestamente illegittima delle libertà fondamentali invocate: i dati per mezzo della telecamera dei droni non sarebbero stati utilizzati per l'identificazione dei soggetti, ma solo per consentire alle autorità di avere informazioni generali circa il numero delle persone riunite per strada o in altri spazi pubblici, così da pianificare eventuali interventi ove le misure di distanziamento non risultassero rispettate. Veniva così respinta la tesi dei ricorrenti secondo cui l'uso dei droni per tali finalità costituisce una ingerenza grave e illegittima nella vita privata degli individui, con un illecito trattamento e mancata protezione dei dati personali.

A fronte di tale pronuncia, i ricorrenti hanno adito il Consiglio di Stato per chiederne l'annullamento. Con una articolata pronuncia il Giudice Amministrativo ha, innanzitutto, ritenuto sussistere la condizione d'urgenza alla base della proposizione del ricorso per mezzo dello strumento del *référé*, in ragione dell'uso ripetuto – da due a tre ore al giorno – dei droni da parte della Prefettura di Parigi, dell'elevato numero di

[33] Tale procedura è prevista dall'ordinamento francese all'art. L. 512-2 del Codice di giustizia amministrativa a cui può essere fatto ricorso in caso di grave violazione delle libertà fondamentali Il giudice del *référé* può ordinare tutte le misure che ritenga necessarie a salvaguardare la libertà fondamentale che abbia subito una violazione grave e manifestamente illecita da parte di una persona giuridica di diritto pubblico o da un ente di diritto privato incaricato della gestione di un servizio pubblico, nell'esercizio dei suoi poteri. Trattasi di una procedura d'urgenza, in ragione della quale il giudice adito è tenuto a pronunciarsi entro 48 ore.

persone suscettibili di essere sottoposte a tale sorveglianza e dei correlati effetti, con conseguente rischio di instaurazione di numerosi contenziosi.

Nel merito, la Prefettura della Polizia di Parigi aveva sostenuto che i droni non erano utilizzati per identificare le persone, ma solo per rilevare eventuali assembramenti a Parigi in contrasto con le misure sanitarie in vigore e poter così disperdere il raduno, evacuare i locali e informare in tempo reale la prefettura. Nello specifico, i droni erano autorizzati a sorvolare la città ad un'altezza compresa tra gli 80 e i 100 metri, utilizzando un grandangolo e privi della capacità di catturare immagini in assenza di una scheda di memoria. Il Conseil d'Etat, condividendo la prima parte di tali argomentazioni, ha evidenziato come l'uso dei droni abbia l'obiettivo di far cessare e/o prevenire la violazione dell'ordine pubblico come conseguenza della violazione delle regole di sicurezza sanitaria. Ha sottolineato, inoltre, che l'uso dei droni, come definito dalla nota ministeriale del 14 maggio 2020, non è di natura tale da violare ex se in maniera grave e manifestamente illegittima le libertà fondamentali degli individui.

Tuttavia, il Giudice ha attribuito rilievo alle circostanze per cui i droni utilizzati sono dotati di uno zoom ottico e che, pur volando ad un'altezza compresa tra gli 80 e i 100 metri, sono in grado di scattare immagini precise che consentono l'identificazione di persone. Valorizzando tale dato fattuale essi risultano, quindi, capaci di raccogliere dati identificativi e di rendere perfettamente identificabili le persone a cui si riferiscono, in quanto non dotati di alcun dispositivo tecnico che impedisca l'utilizzo delle informazioni raccolte per scopi diversi da quelli attualmente perseguiti.

La suddetta possibilità di identificazione è stato il criterio sulla base del quale il Giudice ha qualificato i dati raccolti da tali strumenti come "dati personali", il cui trattamento deve conseguentemente essere autorizzato e controllato. L'eventualità stessa che una persona possa essere identificata determina la presenza di dati qualificabili come personali anche se la polizia non ha utilizzato la telecamera a fini di identificazione. Più semplicemente: la pura cattura di immagini da parte di una telecamera di bordo con zoom ottico costituisce un trattamento di dati personali, indipendentemente dal fatto che il responsabile del trattamento li abbia o meno utilizzati a fini di identificazione.

In ragione di ciò, tali dati sono stati considerati suscettibili di essere ricondotti entro il perimetro di applicabilità della direttiva del 27 aprile 2016 in materia di "protezione delle persone fisiche nei confronti del trattamento dei dati personali da parte delle autorità competenti con fini di prevenzione e di repressione dei reati".[34] In considerazione dei rischi connessi ad un uso contrario alle disposizioni in

[34] In questa situazione, l'articolo 31 della legge francese sulla protezione dei dati, che ha recepito la direttiva UE 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, (relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio), prevede che il trattamento dei dati personali debba essere autorizzato da un decreto ministeriale previa consultazione della CNIL, l'Autorità francese per la protezione dei dati. L'autorizzazione preventiva fornisce anche una certa trasparenza, che consente un dibattito pubblico. La mancanza del suddetto requisito costituisce una indebita ingerenza nella vita privata degli individui, tale da giustificare l'ordine provvisorio di bloccare immediatamente l'uso dei droni da parte della Polizia di Parigi. I pareri della CNIL sono resi pubblici. Si segnala che dal 25 maggio 2018 la CNIL ha predisposto un archivio aperto su questi trattamenti autorizzati, come previsto dall'art. 23. 36 della legge francese sui dati.

materia di protezione dei dati personali, il Conseil d'Etat ha stabilito che l'attuazione di un loro trattamento senza la presenza di un testo regolamentare ad hoc, che ne autorizzi la creazione e ne definisca le modalità di utilizzo, costituisce una violazione grave e manifestamente illegittima del diritto al rispetto della vita privata. Le misure che possono limitare l'esercizio dei diritti e delle libertà fondamentali devono essere necessarie, appropriate a proporzionate all'obiettivo di tutela della salute pubblica che perseguono, cosa che, secondo il Conseil d'Etat, non è avvenuta nel caso di specie.

Il Conseil d'Etat, in conclusione, non rifiuta l'uso dei droni di sorveglianza in quanto tale che, anzi, ritiene necessario per la sicurezza pubblica nelle circostanze attuali e quindi astrattamente legittimo, ma ne ha censurato l'uso improprio, illegale e arbitrario, in quanto non sufficientemente regolamentato. A tal fine, due sono gli strumenti presi in considerazione per porvi rimedio.

In primo luogo, è ordinato all'autorità prefettizia di Parigi di far cessare le misure di sorveglianza mediante droni fino alla data dell'adozione di un testo regolamentare che autorizzi tale trattamento dei dati personali nel rispetto delle disposizioni della legge del 6 gennaio 1978, c.d. Loi informatique et libertés, e previo parere della Commissione nazionale sull'informatica e sulle libertà.

In secondo luogo, e in alternativa, si prevede una soluzione di carattere più marcatamente tecnico: la sorveglianza per mezzo di droni dovrà cessare finché non verranno impiegati dispositivi tecnici tali da rendere impossibile, qualunque ne sia l'uso, l'identificazione delle persone filmate.

4. Brevi riflessioni conclusive

È indubbio che la necessità di ridurre i contatti sociali al fine di spezzare la catena dei contagi da Covid-19 abbia favorito il ricorso a strumenti versatili ed efficaci, le cui potenzialità hanno spesso subito limitazioni a causa di una non completamente sviluppata regolamentazione. L'indiscutibile utilità dei droni nell'attuale crisi sanitaria potrebbe, infatti, favorire un loro impiego sempre più diffuso e una loro emancipazione dall'impiego circoscritto ad una sfera prettamente privata: si pensi, in via esemplificativa, al loro impiego per consegnare materiale e forniture mediche, per raccogliere campioni di laboratorio e per organizzare le correlate spedizioni, per fare annunci di pubblico rilievo, per consegnare generi di prima necessità o per assicurare la disinfezione di spazi pubblici[35].

Alla luce di quanto ricostruito sinora, sembra potersi affermare che misure di sorveglianza come quelle realizzatesi con l'impiego dei droni, possano dirsi ammissibili in un contesto emergenziale purché le

[35] Si pensi al caso cinese, dove i droni sono stati impiegati a supporto della lotta alla diffusione del virus già da febbraio 2020, quando hanno trasportato campioni di test e forniture mediche da un ospedale nella provincia di Zhejang a un vicino centro di controllo delle malattie. O ancora, il caso irlandese, quando a partire da aprile 2020, l'Autorità di Aviazione ha consentito la consegna di beni essenziali a famiglie confinate presso la città di Moneygall. Per altri esempi di impiego dei droni durante la pandemia si veda: Covid-19 Transport brief – Drones in the Era of Coronavirus, in International Transport Forum, reperibile al seguente link: www.itf-oecd.org.

disposizioni abbiano, innanzitutto, una portata limitata nel tempo e strettamente connessa al perdurare dell'emergenza.

Vari ordinamenti di natura democratica hanno giustificato il ricorso a tali strumenti invocando la necessità di tutelare il bene preminente della salute dei cittadini, non tanto in una prospettiva individuale, quanto più nella sua dimensione collettiva.[36] Ammettendo la validità di tali argomentazioni, l'utilizzo dei dati sulla mobilità dei soggetti contagiati per ricostruire la catena epidemiologica, dovrebbe essere riletto alla luce della natura solidaristica del fine perseguito. Lungi dal voler introdurre forme atipiche di sorveglianza a fini repressivi, tali strumenti risponderebbero, quindi, all'esigenza di sottoporre ad accertamenti quanti siano potenzialmente entrati in contatto con l'interessato o comunque di adottare le misure utili a prevenire una ulteriore diffusione del contagio.

Non sfuggono ovviamente le implicazioni che una tale impostazione, per quanto astrattamente ammissibile, determina sui diritti e sulle libertà fondamentali dei soggetti coinvolti.

L'uso di tecnologie di sorveglianza di massa nell'ambito dell'esercizio di poteri emergenziali ha fatto sorgere dubbi circa la possibilità che i dati raccolti ed elaborati – si ribadisce, in un contesto e per finalità emergenziali – possano indebitamente sopravvivere all'emergenza stessa che ne ha reso legittimo l'impiego. Si pone, dunque, la necessità di interrogarsi sulle modalità a cui è concretamente possibile fare riferimento per conseguire le finalità sopra evidenziate, dovendosi sempre garantire il rispetto dei principi di proporzionalità, necessità e di adeguatezza.

Entro che limiti strumenti che, come i droni, consentono di realizzare una sorveglianza sistematica e generalizzata nei confronti della totalità della popolazione e misure volte a verificare il rispetto degli obblighi di permanenza domiciliare e distanziamento sociale potrebbero dirsi realmente conformi al canone di proporzionalità? Come assicurare un equilibrio tra costi e benefici dell'uso dei droni?

La sorveglianza da parte dello Stato è sempre stato un argomento controverso a livello globale e – oggi più che mai – il tema della sorveglianza per scopi sanitari globali è al centro dell'attenzione a causa della pandemia. Ogni Paese ha il proprio metodo. Il quadro e l'estensione del monitoraggio da parte dei Governi variano notevolmente a seconda della giurisdizione interessata: l'equilibrio tra la sorveglianza necessaria per sconfiggere questo virus e la protezione del nostro diritto fondamentale alla privacy sembra, tuttavia, difficile da raggiungere.

In tale ottica le autorità di regolamentazione e le organizzazioni di tutela della privacy hanno più e più volte esortato i Governi ad attuare regole che garantiscano che le politiche di sorveglianza e monitoraggio

[36] In una intervista rilasciata dal Presidente del Garante per la Protezione dei dati personali, quest'ultimo ha evidenziato come una delle maggiori sfide poste dalla pandemia sia proprio quella di «garantire che i diritti individuali siano limitati nella sola misura necessaria ad impedire il dilagare di un virus che è paritario nel contagio, ma cinicamente selettivo negli effetti». Le limitazioni di libertà cui si deve soggiacere sono, quindi, il prezzo da pagare, doverosamente, per tutelare soprattutto le fasce più vulnerabili della popolazione, ma devono essere limitazioni strettamente indispensabili, proporzionali all'efficacia attesa e soprattutto temporanee». Si veda: Privacy e democrazia ai tempi della pandemia – Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali (Di Niccolò Serri, www.fondazioneleonardo-cdm.com - 24 marzo 2020).

sanitario siano rigorosamente prescritte dalla legge, proporzionate alle esigenze di salute pubblica, trasparenti, controllate da autorità di regolamentazione indipendenti, soggette a una costante riflessione etica, non discriminatorie e rispettose dei diritti fondamentali. Tali autorità sono chiaramente chiamate ad offrire soluzioni innovative e lungimiranti, in particolare quando si tratta di questioni importanti come la cancellazione e la conservazione dei dati personali, la reversibilità dei nuovi controlli governativi e l'esercizio dei connessi poteri di verifica e di indagine

Nonostante la portata delle sfide economiche e di salute pubblica poste dalla pandemia COVID-19, è fondamentale che i Governi e gli attori del settore privato, infatti, non si allontanino dai principi fondamentali della governance dei dati e della privacy.

Con riferimento ai droni, stante l'urgenza che la situazione attuale comporta, qualsiasi responsabile del trattamento dovrebbe assicurare la conformità del trattamento da porre in essere, al fine di garantire la sicurezza del trattamento dei dati personali. Oltre all'adozione di misure di sicurezza e di riservatezza adeguate, è necessario garantire che i rapporti con gli eventuali responsabili del trattamento (quali fra tutti, i fornitori di droni, delle tecnologie di sorveglianza e di tracciamento e qualsiasi fornitore di stoccaggio come un cloud o un server integrato) siano ben protetti contrattualmente al fine di formalizzare gli obblighi e le responsabilità di ciascuna parte, in conformità con le disposizioni dell'articolo 28 del GDPR.

Le seguenti considerazioni, basate sui principi elaborati dall'OCSE in materia di governance dei dati e di privacy, dovrebbero guidare tali pratiche di raccolta e condivisione dei dati, e i Governi sono chiamati a promuovere un uso sempre più pienamente responsabile dei dati personali.[37]

L'utilizzo dei dati, infatti, deve muoversi entro un quadro normativo che ne delimiti con certezza i confini e che assicuri che gli stessi siano impiegati esclusivamente per il monitoraggio degli spostamenti, e non per diverse (e incompatibili) finalità. In aggiunta, i cittadini dovrebbero essere informati di trovarsi in zone interessate da monitoraggio a mezzo drone, la risoluzione delle videocamere dovrebbe essere regolata in modo da limitarsi alla ripresa di quanto strettamente necessario e le riprese dovrebbero essere effettuate, per quanto possibile, evitando luoghi di privata dimora o aree non rilevanti, tenuto conto del fine dichiarato per cui il monitoraggio è effettuato.

Per quanto concerne la conservazione dei dati raccolti si pone l'esigenza ulteriore di stabilire anticipatamente la policy di conservazione delle registrazioni, dei flussi dei dati e dei metadati. Immagini e video vanno conservati per il tempo strettamente necessario ad adempiere alle finalità di monitoraggio. Da ultimo occorre evidenziare come questi adempimenti vadano, per quanto possibile, formalizzati in modo da rispettare anche il principio di accountability e vadano, poi, resi conoscibili per tutti i soggetti

[37] OECD Policy Responses to Coronavirus (COVID-19) – Ensuring data privacy as we battle Covid-19, versione del 14 aprile 2020, reperibile al seguente link: http://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/.

coinvolti, mediante la messa a disposizione di adeguate istruzioni sulle modalità di trattamento dei dati e soprattutto sulle correlate misure sicurezza.

L'attuale situazione di crisi scaturita dal diffondersi della pandemia ha reso necessario il ricorso a misure di carattere eccezionale. Ciò, tuttavia, non può e non deve comportare una rinunzia totale e incondizionata ad altri diritti costituzionalmente riconosciuti e tutelati. Ne consegue che i vantaggi e benefici che un uso corretto e consapevole di questi strumenti può comportare possono essere completamente apprezzati – compatibilmente con una cultura democratica – solo nella misura in cui si assicuri il rispetto dei diritti e delle libertà fondamentali. A conferma di tale impostazione, ribadita da più e più voci, si può concludere condividendo l'affermazione secondo cui le norme a tutela dei dati personali non devono ostacolare l'adozione di misure di lotta e contrasto al coronavirus, ma che, tuttavia, queste ultime non possono prescindere dal rispetto dei diritti fondamentali della persona.[38]

[38] «Data protection rules (such as GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. However, I would like to underline that, even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects. Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data». Dichiarazione del presidente del Comitato europeo per la protezione dei dati (EDPB) A. Jelinek sul trattamento dei dati personali nel contesto dell'emergenza Covid, reperibile al seguente link: https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_it.