Universitat Autònoma de Barcelona

DRONS I PRIVACITAT: ANÀLISI DEL MARC NORMATIU ESPANYOL

Memòria del Treball de Fi de Grau en Gestió Aeronàutica

realitzat per

Jordi Guinovart Martín

i dirigit per

Júlia Tutusaus Garcia

Escola d'Enginyeria

Sabadell, juny de 2026

La sotasignada, Júlia Tutusaus Garcia directora del Treball de Fi de Grau, professora de l'Escola d'Enginyeria de la UAB,

CERTIFICA:

Que el treball al que correspon la present memòria ha estat realitzat sota la seva direcció per

Jordi Guinovart Martín

I per a que consti firma la present.
Sabadell, ***juny*** de ***2026***

JÚLIA TUTUSAUS GARCIA - DNI 39476357P

Firmado digitalmente por JÚLIA TUTUSAUS GARCIA - DNI 39476357P
Fecha: 2026.06.25 11:12:43 +02'00'

Signat

RESUM

Aquest treball analitza fins a quin punt el marc normatiu espanyol és suficient per protegir el dret a la privacitat davant l'ús de drons amb finalitats de vigilància. En els darrers anys, els drons han experimentat un gran creixement en diferents àmbits civils com la seguretat i les emergències fet que ha generat nous reptes relacionats amb la protecció de dades i els drets fonamentals.

La recerca combina una anàlisi teòrica i jurídica amb una petita part pràctica basada en un qüestionari dirigit a professionals que utilitzen aquestes tecnologies habitualment. L'estudi es centra especialment en la regulació dels drons, la privacitat i dels riscos associats.

Els resultats mostren que, tot i que existeix una regulació cada vegada més desenvolupada, encara hi ha dubtes en la seva aplicació i preocupacions relacionades amb la captació d'imatges i la protecció de la privacitat. Per aquest motiu, el treball conclou que és necessari continuar adaptant la normativa als nous usos dels drons i reforçar algunes garanties jurídiques.

Paraules clau: drons, vigilància, privacitat, protecció de dades, normativa.

ABSTRACT

This study analyses whether the Spanish legal framework is enough to protect privacy in the use of drones for surveillance. In recent years, drones have become more common in civil sectors such as security, emergencies and audiovisual work, creating new challenges for data protection and fundamental rights.

The research combines a theoretical and legal analysis with a small practical study based on a questionnaire answered by professionals who regularly work with drones. It focuses on drone regulation; privacy and the risks linked to this technology.

The results show that, although the legal framework is more developed today, there are still doubts about how the rules are applied in practice and concerns about image capture and privacy protection. The study concludes that regulations should continue adapting to new uses of drones and that some legal safeguards should be strengthened.

Keywords: drones, surveillance, privacy, data protection, regulation.

ÍNDEX DE CONTINGUT

1. ÍNDEX DE FIGURES..... 5

2. ÍNDEX DE TAULES..... 6

3. INTRODUCCIÓ..... 7

4. MARC TEORIC..... 10

4.1. La societat de la vigilància..... 10

4.2. El dret a la privacitat..... 12

4.3. Tecnologia i drets fonamentals..... 14

5. CONTEXT DELS DRONS..... 16

5.1.Definició..... 16

5.1.1. Categoria oberta..... 17

5.1.2. Categoria específica..... 18

5.1.3. Categoria certificada..... 19

5.1.4. Normativa en les diferents categories..... 19

5.2. Relació entre les classes tècniques i les categories operatives..... 20

5.3. Usos dels drons en l'àmbit civil..... 21

5.4. Drons i vigilància..... 23

6. MARC NORMATIU ESPANYOL..... 25

6.1. Regulació dels drons..... 25

6.2. Protecció de dades i privacitat..... 28

6.3. Límits legals a la vigilància..... 32

7. ESTUDI PRÀCTIC: PERCEPCIONS PROFESSIONALS SOBRE LA NORMATIVA I LA PRIVACITAT EN L'ÚS DELS DRONS..... 35

7.1. Objectiu de l'estudi..... 35

7.2. Metodologia..... 36

7.3. Resultats..... 38

7.3.1. Perfil dels participants i coneixement de la normativa..... 38

7.3.2. Percepció sobre la normativa i la privacitat..... 40

7.3.3. Dubtes normatius, reptes legals i riscos associats..... 41

7.3.4. Resultats de les preguntes obertes..... 43

7.4. Discussió dels resultats i limitacions de l'estudi..... 45

8. CONCLUSIONS..... 46

8.1. Resolució de la hipòtesi de recerca..... 46

8.2. Propostes i línies futures de recerca..... 47

9. ANNEXES..... 48

10. BIBLIOGRAFIA..... 50

1. ÍNDEX DE FIGURES

Figura 1. Principals requisits de la categoria oberta 18
Figura 2. Relació entre classes tècniques i categories operatives 23
Figura 3. Resultats de la pregunta 1 38
Figura 4. Resultats de la pregunta 2 38
Figura 5. Resultats de la pregunta 3 39
Figura 6. Resultats de la pregunta 4 39
Figura 7. Resultats de la pregunta 5 40
Figura 8. Resultats de la pregunta 6 40
Figura 9. Resultats de la pregunta 7 41
Figura 10. Resultats de la pregunta 8 41
Figura 11. Resultats de la pregunta 9 42
Figura 12. Resultats de la pregunta 10 42
Figura 13. Annex 1. Captura del qüestionari 48
Figura 14. Annex 2. Captura del qüestionari 48
Figura 15. Annex 3. Captura del qüestionari 49
Figura 16. Annex 4. Captura del qüestionari 49

2. ÍNDEX DE TAULES

Taula 1. Relació entre classes tècniques i categories operatives.....20
Taula 2. Resultats de les preguntes obertes 44

3. INTRODUCCIÓ

Per començar, en els últims anys, l'ús de drons en l'àmbit civil ha crescut. Cada vegada són més presents en diverses activitats, com ara la seguretat, la vigilància d'espais públics, la gestió urbana, el control d'infraestructures o les emergències. Aquest augment respon, en gran part, als avantatges que ofereixen aquests dispositius, ja que són eines àgils i poden arribar amb facilitat a determinats espais, permetent captar imatges de manera ràpida i eficient.

Ara bé, aquest desenvolupament tecnològic també genera nous interrogants. El fet que els drons permetin observar, gravar i recopilar dades des de l'aire introdueix formes de control que poden passar desapercebudes per la ciutadania. A diferència d'altres mecanismes de vigilància més visibles, com poden ser les càmeres fixes, els drons tenen una gran mobilitat i poden operar de manera menys perceptible. Això fa que no només s'hagi de valorar la seva utilitat pràctica, sinó també les conseqüències que el seu ús pot tenir sobre els drets de les persones.

En aquest context, es parteix d'una idea central, **l'expansió dels drons en l'àmbit civil no és només una qüestió tècnica o operativa, sinó també jurídica i social.** El seu ús pot resultar útil en determinades situacions, però al mateix temps pot afectar drets fonamentals, com el dret a la privacitat. Quan aquests dispositius s'utilitzen per vigilar espais públics, apareix una tensió clara entre la recerca de seguretat i la necessitat de respectar els límits propis.

Aquest conflicte és especialment important perquè la capacitat dels drons per captar imatges, enregistrar situacions i recollir informació no sempre va acompanyada d'una percepció clara per part de les persones afectades. En molts casos, aquestes no saben exactament quan estan sent observades, quines dades es recullen ni amb quina finalitat es tractaran més tard. Per això, el debat no es centra únicament en si l'ús dels drons és legal o útil, sinó en si els controls existents són realment suficients per evitar observacions i anàlisis innecessaris o desproporcionats.

A partir de tot això, s'ha de tenir en compte l'anàlisi del marc normatiu aplicable. Tant la Unió Europea com l'Estat espanyol han anat desenvolupant normes destinades a regular l'ús dels drons i a protegir les dades personals. Entre aquestes, destaca especialment el Reglament General de Protecció de Dades, així com la normativa específica sobre operacions amb drons. Tot i això, el fet que existeixi regulació no significa necessàriament que la protecció sigui sempre efectiva. La rapidesa amb què evoluciona la tecnologia, la varietat d'usos possibles i la dificultat de controlar certes pràctiques fan pensar que poden existir limitacions, buits o problemes d'aplicació.

Per aquest motiu, la pregunta principal en la qual es basa aquesta recerca és la següent:

- **És suficient el marc normatiu espanyol per protegir el dret a la privacitat davant l'ús de drons amb finalitats de vigilància en l'àmbit civil?**

A partir d'aquesta pregunta, l'objectiu general del treball és analitzar de manera crítica si el marc normatiu vigent és suficient per prevenir usos dels drons que puguin comportar usos desproporcionats en la privacitat de les persones, especialment en espais públics. Per això, aquest treball no es limita a descriure la normativa existent, sinó que pretén valorar fins a quin punt aquesta respon de manera adequada als riscos reals que planteja aquesta tecnologia.

Per assolir aquest objectiu general, es plantegen **tres objectius específics.**

En primer lloc, examinar el context actual de la vigilància tecnològica i la seva relació amb la protecció dels drets fonamentals, amb especial atenció al dret a la privacitat. Aquest primer objectiu és important perquè l'ús de drons s'ha d'entendre dins d'un context més ampli en què les tecnologies de control i captació d'informació tenen cada vegada més presència en la vida quotidiana.

En segon lloc, analitzar la normativa espanyola aplicable a l'ús de drons i a la protecció de dades personals, per tal d'identificar quins límits, garanties i obligacions estableix. En aquest punt, convé precisar que, quan en aquest treball es parla de drons, es fa referència als vehicles aeris no tripulats utilitzats en l'àmbit civil, és a dir, aparells que poden volar sense portar una persona a bord i que, segons les seves característiques tècniques, poden incorporar càmeres, sensors o altres sistemes de captació d'informació. Aquesta precisió és rellevant perquè no tots els drons tenen el mateix ús ni el mateix nivell de risc. Alguns poden tenir funcions recreatives o tècniques, mentre que d'altres poden ser utilitzats per observar espais, gravar imatges o recopilar dades.

Finalment, identificar i valorar els principals riscos jurídics i socials derivats de l'ús de drons amb finalitats de vigilància, posant el focus en possibles situacions de control excessiu, manca de garanties o insuficiència reguladora. Aquest objectiu respon al fet que els drons no només són eines útils des d'un punt de vista tècnic, sinó també tecnologies que poden generar impactes importants sobre els drets fonamentals, especialment quan s'utilitzen en espais públics.

Pel que fa a la metodologia, el treball adopta un enfocament qualitatiu. Es basa, principalment, en la revisió de bibliografia acadèmica, l'estudi de la normativa vigent i l'anàlisi crític del seu contingut. També es tindran en compte documents institucionals i fonts jurídiques relacionades amb l'ús civil dels drons i amb la protecció de dades personals.

A més de la part teòrica, el treball inclou també una petita part pràctica amb l'objectiu de conèixer la percepció de diferents professionals que utilitzen drons en l'àmbit civil. Per fer-ho, es va elaborar un qüestionari en línia dirigit a operadors i persones vinculades a sectors com la seguretat, l'audiovisual, la inspecció d'infraestructures o la formació de pilots de drons. Les preguntes es van centrar en el coneixement de la normativa, la percepció sobre la protecció de la privacitat i els principals problemes que es troben en l'aplicació de la regulació.

Aquesta metodologia permet, d'una banda, entendre el paper que tenen actualment els drons dins la societat i els diferents usos que poden tenir en l'àmbit civil i, de l'altra, analitzar fins a quin punt el marc normatiu existent és capaç de donar resposta als riscos que aquesta tecnologia pot generar.

Pel que fa a l'estructura, el treball s'organitza en sis capítols principals. Després d'aquesta introducció, el segon capítol desenvolupa el marc teòric, centrat en la societat de la vigilància, el dret a la privacitat i la relació entre tecnologia i drets fonamentals. El tercer capítol presenta el context dels drons, explicant què són, com es classifiquen i quins usos tenen en l'àmbit civil, així com la seva relació amb la vigilància.

El quart capítol analitza el marc normatiu espanyol aplicable als drons, especialment en relació amb la protecció de dades, la privacitat i els límits legals de la vigilància. A continuació, el cinquè capítol desenvolupa l'estudi pràctic basat en els resultats del qüestionari realitzat a professionals del sector, amb l'objectiu d'analitzar la seva experiència i la seva percepció sobre la normativa actual. El treball es tanca amb les conclusions, on es recullen els principals resultats de la recerca, les limitacions detectades i les possibles.

4. MARC TEORIC

4.1. La societat de la vigilància

La vigilància no és un fenomen nou. Al llarg de la història, diferents formes de control han estat presents en la societat, especialment en àmbits com l'exèrcit, les institucions o els ajuntaments de les ciutats. No obstant això, en les darreres dècades, aquest fenomen ha adquirit una nova dimensió a causa del desenvolupament de les tecnologies digitals. Aquest canvi ha portat a parlar del que s'anomena "societat de la vigilància", és a dir, un context en què la recollida i el control d'informació sobre les persones esdevé una pràctica cada vegada més habitual.

El sociòleg David Lyon explica que la vigilància actual no pot entendre's només com un mecanisme puntual de control, sinó com una característica estructural de la societat contemporània. Segons Lyon, els avenços tecnològics, especialment en l'àmbit de la informàtica i les comunicacions, han fet possible una vigilància més extensa, més eficient i, sobretot, menys visible. Això implica que moltes de les formes de control actuals no es perceben directament, sinó que funcionen de manera integrada en la vida quotidiana.

Un dels aspectes més rellevants que destaca aquest autor és que la vigilància moderna no depèn únicament de la tecnologia, sinó també del context social en què s'aplica. És a dir, no es tracta només de la capacitat tècnica de controlar, sinó de com aquesta capacitat s'integra en les estructures socials, econòmiques i polítiques. Així, la vigilància es pot trobar en àmbits molt diversos, com l'administració pública, la seguretat, el treball o fins i tot el consum.

A més, Lyon assenyala que les noves tecnologies han transformat la manera com es recull i es gestiona la informació sobre les persones. Un element clau en aquest procés és el pas de la informació en paper a la informació digital. Aquest canvi ha facilitat que les dades es puguin emmagatzemar, creuar i analitzar amb molta més facilitat, generant el que ell anomena una *"dataimagen",* és a dir, un conjunt de dades que representen una persona en diferents sistemes. Aquesta idea és especialment important, ja que implica que el control ja no es basa només en l'observació directa, sinó també en el tractament d'informació.

Seguidament, les reflexions del filòsof Michel Foucault ajuden a entendre millor l'origen d'aquestes formes de vigilància. Foucault va desenvolupar el concepte de "panòptic" per descriure un model de control en què els individus poden ser observats en qualsevol moment sense saber exactament quan estan sent vigilats. Aquesta incertesa fa que les persones acabin regulant el seu propi comportament, ja que actuen com si estiguessin sempre sota observació.

Aquesta idea continua sent útil avui dia, tot i que el context ha canviat. Mentre que el model clàssic del panòptic es basava en una estructura física, com una presó, la vigilància actual es caracteritza per ser molt més difusa i descentralitzada. Tal com apunten diversos autors, el control ja no depèn d'un únic centre visible, sinó que es distribueix a través de múltiples tecnologies i sistemes que operen de manera simultània. Això fa que la vigilància sigui menys evident, però alhora més constant.

D'acord amb això, alguns textos assenyalen que la societat actual combina elements de control amb justificacions basades en la seguretat, l'eficiència o la millora dels serveis. Això genera una certa acceptació social de la vigilància, ja que sovint es percep com una eina necessària. No obstant això, aquesta acceptació pot dificultar la identificació dels seus límits i riscos, especialment quan les persones no són plenament conscients del grau de control al qual estan sotmeses.

Un altre aspecte rellevant és que la vigilància no afecta totes les persones de la mateixa manera. Tal com es destaca en l'anàlisi de Lyon, determinats sistemes de control poden tenir un impacte més gran en alguns col·lectius, especialment aquells que es troben en situacions de major vulnerabilitat. Això posa de manifest que la vigilància no és només una qüestió tècnica, sinó també social i política.

En conjunt, es pot afirmar que la vigilància contemporània es caracteritza per tres elements principals. Per començar, és més extensa, ja que abasta cada vegada més àmbits de la vida. A més, és més invisible, perquè sovint no es percep de manera directa. Per últim, és més constant, ja que el control no es limita a moments concrets, sinó que pot ser continu.

Aquest marc teòric és fonamental per entendre el paper dels drons dins de la societat actual. Aquests dispositius s'insereixen precisament en aquest context de vigilància tecnològica, ja que permeten captar informació de manera mòbil, flexible i, en molts casos, poc visible. Per això, l'anàlisi de la societat de la vigilància resulta imprescindible per comprendre els riscos que poden derivar del seu ús i per valorar fins a quin punt el dret és capaç de respondre-hi adequadament.

4.2. El dret a la privacitat

El dret a la privacitat és un dels drets fonamentals que protegeixen l'àmbit personal de les persones davant possibles intromissions externes. Jurídicament, aquest dret no es limita només a evitar que altres persones accedeixin a informació privada, sinó que implica també el control sobre les pròpies dades i sobre com aquestes poden ser utilitzades. Això és especialment rellevant en un context en què les tecnologies com els drons permeten captar i tractar informació de manera constant.

A l'Estat espanyol, aquest dret es troba reconegut a l'article 18 de la Constitució, que estableix el dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge. Aquest mateix article també introdueix una idea clau per al context actual: la necessitat de limitar l'ús de la informàtica per garantir aquests drets. Aquesta previsió és especialment significativa, ja que anticipa el problema que avui es planteja amb les noves tecnologies, com ara els sistemes de vigilància o els drons.

A partir d'aquí, la privacitat no es pot entendre com un concepte limitat a l'àmbit domèstic. En l'actualitat, la seva protecció s'estén també a l'espai públic, en la mesura que les persones continuen tenint dret a no ser sotmeses a un control desproporcionat. Això implica que el fet de trobar-se en un espai obert no elimina automàticament la protecció de la privacitat, sinó que obliga a analitzar en quines condicions es poden captar imatges o dades.

La protecció de la privacitat està estretament vinculada al dret a la protecció de dades personals. Aquest dret es desenvolupa principalment a través del Reglamento General de Protección de Datos i de la Llei orgànica 3/2018 de protecció de dades personals i garantia dels drets digitals.

Una de les idees més importants del RGPD és que no n'hi ha prou amb evitar l'accés a dades, sinó que cal regular tot el seu tractament. Això inclou aspectes com la recollida, l'emmagatzematge, l'ús i la possible comunicació a tercers. En aquest context, el reglament estableix principis bàsics com el de limitació de la finalitat, la minimització de dades o la necessitat que existeixi una base jurídica que justifiqui el tractament.

Això és clau: el problema no és només que es captin dades o imatges, sinó **com es fa, amb quina finalitat i fins a quin punt és necessari**. Per exemple, no és el mateix captar una imatge de manera puntual per una finalitat concreta que fer una vigilància continuada sense que les persones afectades en siguin conscients.

A més, el RGPD posa especial èmfasi en la transparència i en el dret de les persones a saber què es fa amb les seves dades. Això inclou el dret a ser informades, a accedir a les dades, a rectificar-les o a demanar-ne la supressió. Aquest conjunt de drets reforça la idea que la privacitat no és només un espai a protegir, sinó també un àmbit sobre el qual les persones han de tenir control.

La Llei orgànica 3/2018 adapta aquests principis al context espanyol i incorpora també els anomenats drets digitals. Aquesta norma reconeix que la protecció de dades no és només una qüestió tècnica, sinó una part essencial dels drets fonamentals en l'entorn digital. Això és especialment rellevant en situacions en què les tecnologies permeten un seguiment constant de l'activitat de les persones, com pot passar en l'àmbit laboral o en espais públics.

Per exemple, les guies de l'Agència Espanyola de Protecció de Dades posen de manifest que, fins i tot en contextos en què existeix una relació de subordinació o una finalitat legítima, com la seguretat, el tractament de dades ha de respectar criteris de proporcionalitat i necessitat. És a dir, no tot és acceptable encara que hi hagi una justificació general.

A partir d'aquí, és important entendre que el dret a la privacitat no és un dret absolut. Això vol dir que pot entrar en conflicte amb altres interessos, com la seguretat pública, la prevenció de delictes o l'eficiència en la gestió de determinats serveis. Però, qualsevol limitació ha de complir determinades condicions. En primer lloc, ha d'estar prevista per una norma. En segon lloc, ha de perseguir una finalitat legítima. I, en tercer lloc, ha de ser proporcional, és a dir, adequada i necessària per aconseguir l'objectiu perseguit sense anar més enllà del que és imprescindible. Aquest criteri de proporcionalitat és fonamental, ja que permet valorar si una determinada pràctica de vigilància és acceptable o si per contra, suposa una ingerència excessiva en la privacitat.

Aquest punt és especialment important en relació amb l'ús de tecnologies com els drons. Aquests dispositius permeten captar imatges i informació des de diferents angles i amb una gran mobilitat, cosa que pot incrementar el risc d'una vigilància més intensa i menys controlada. Per això, la clau no és només determinar si l'ús dels drons està permès, sinó analitzar en quines condicions es duu a terme i si aquestes respecten els límits establerts pel dret.

En definitiva, el dret a la privacitat en l'actualitat no es pot entendre només com una protecció davant intromissions puntuals, sinó com un conjunt de garanties que busquen limitar el poder de captació i tractament d'informació. En un context de vigilància tecnològica creixent, el repte principal no és evitar qualsevol recollida de dades, sinó assegurar que aquesta es realitza de manera justificada, limitada i respectuosa amb els drets de les persones.

4.3. Tecnologia i drets fonamentals

El desenvolupament de les tecnologies digitals ha transformat profundament la manera en què es relacionen les persones, les institucions i el poder. En aquest context, la tecnologia no només facilita noves formes de comunicació o d'accés a la informació, sinó que també amplia de manera significativa la capacitat de control sobre la societat. Aquest fet planteja un repte important per als drets fonamentals, especialment per aquells vinculats a la privacitat i a la llibertat individual.

En primer lloc, cal tenir en compte que les noves tecnologies permeten una recollida i tractament de dades molt més extensos que en etapes anteriors. Sistemes digitals, sensors, càmeres o dispositius connectats fan possible obtenir informació de manera contínua, sovint sense que les persones en siguin plenament conscients. Això implica que la vigilància ja no es limita a situacions concretes, sinó que pot formar part del funcionament habitual de la societat.

Diversos estudis assenyalen que aquest augment de la capacitat tecnològica ha intensificat el conflicte entre seguretat i privacitat. En particular, la utilització de tecnologies de vigilància massiva ha ampliat la capacitat dels poders públics i privats per monitoritzar comportaments i recopilar informació a gran escala. Això no només afecta la privacitat, sinó també altres drets fonamentals, com la llibertat d'expressió o la llibertat de reunió.

A més, aquestes tecnologies no només permeten observar, sinó també analitzar i combinar dades de diferents fonts. Això incrementa el nivell de control, ja que es poden generar perfils, prediccions o sistemes de seguiment més complexos. En aquest sentit, la vigilància actual no es basa únicament en la presència física, sinó en la capacitat de gestionar informació de manera automatitzada.

Davant d'aquest escenari, el dret intenta establir límits i garanties per protegir les persones. Normes com el *Reglamento General de Protección de Datos* tenen com a objectiu regular l'ús de la informació personal i evitar abusos. Aquestes normes introdueixen principis com la necessitat de justificació del tractament, la limitació de la finalitat o la protecció des del disseny.

No obstant això, un dels principals problemes és que la tecnologia evoluciona molt més ràpid que el dret. Aquest desfasament fa que, sovint, les lleis no siguin suficients per respondre als nous riscos que apareixen. Tal com s'ha assenyalat en diversos estudis, la manca de regulacions clares o actualitzades pot augmentar el risc de vulneracions dels drets fonamentals.

Aquest desajust entre tecnologia i normativa genera una situació complexa. D'una banda, existeixen normes que estableixen límits. Però, de l'altra, la rapidesa amb què apareixen noves tecnologies dificulta la seva aplicació efectiva. Això es tradueix en una certa inseguretat jurídica i en la possibilitat que determinades pràctiques es desenvolupin en zones grises.

Un altre aspecte important és la dificultat de control real. Encara que hi hagi regulació, no sempre és fàcil garantir que es compleixi en la pràctica. Les tecnologies actuals permeten operar de manera distribuïda, automatitzada i, en molts casos, poc visible. Això fa que el control sobre el seu ús sigui limitat i que les possibles infraccions siguin difícils de detectar o de provar.

A més, tal com assenyalen organismes internacionals, les tecnologies digitals poden ser alhora una eina de progrés i un risc per als drets humans. Això implica que el debat no és simplement si la tecnologia és positiva o negativa, sinó com s'utilitza i quines garanties existeixen per evitar abusos.

En aquest context, el dret no només ha de regular, sinó també adaptar-se. Això implica desenvolupar mecanismes més flexibles i anticipar possibles riscos abans que es materialitzin. No obstant això, aquesta adaptació no sempre és fàcil, ja que requereix equilibrar interessos diferents, com la seguretat, la innovació o la protecció dels drets fonamentals.

Aquestes tensions es fan especialment visibles en tecnologies que permeten la vigilància en espais públics, com és el cas dels drons. Aquests dispositius exemplifiquen clarament aquest problema, ja que combinen mobilitat, capacitat de captació d'imatges i dificultat de control. Això fa que el marc jurídic hagi d'afrontar situacions noves que no sempre estan completament previstes.

En definitiva, la relació entre tecnologia i drets fonamentals es caracteritza per una tensió constant. D'una banda, la tecnologia incrementa les possibilitats de control i de recollida d'informació. De l'altra, el dret intenta establir límits per protegir les persones. No obstant això, el desfasament entre ambdós i la dificultat d'aplicació efectiva de les normes fan que aquesta protecció no sempre sigui suficient.

Així, el repte principal no és només regular la tecnologia, sinó garantir que aquesta regulació sigui realment efectiva en la pràctica. En aquest sentit, la qüestió no és només si existeixen normes, sinó si aquestes són capaces de limitar de manera real i efectiva l'ús de tecnologies que poden afectar els drets fonamentals.

5. CONTEXT DELS DRONS

5.1.Definició

Els drons, també coneguts com a UAS (Unmanned Aircraft Systems) o aeronaus no tripulades, són aparells capaços de volar sense portar una persona a bord. Aquests dispositius poden ser controlats a distància per un pilot o funcionar de manera automatitzada mitjançant sistemes programats. En els darrers anys, el seu ús s'ha expandit considerablement en l'àmbit civil, especialment en activitats relacionades amb la seguretat, la vigilància, la captació d'imatges, les emergències o la gestió d'infraestructures.

Una de les característiques principals dels drons és la seva capacitat per incorporar tecnologies com càmeres, sensors, o GPS. Això els permet captar informació de manera ràpida i des de diferents perspectives, fins i tot en espais de difícil accés. Aquesta capacitat de recollida de dades és el que converteix els drons en una tecnologia especialment rellevant des del punt de vista de la privacitat i la vigilància.

A nivell normatiu, la regulació europea estableix dues formes complementàries de classificació dels drons. D'una banda, existeix una classificació tècnica basada en les característiques de l'aeronau. D'altra banda, existeix una classificació operativa basada en el risc de l'operació que es pretén realitzar. Aquesta distinció és important perquè la normativa no regula únicament el tipus de dron utilitzat, sinó també la manera com es desenvolupa l'activitat.

- **Estructura tècnica: les classes c0-c6**

La classificació tècnica dels drons es basa en els anomenats marcatges de classe, identificats mitjançant les categories C0, C1, C2, C3, C4, C5 i C6.

Aquests marcatges són etiquetes oficials establertes per la Unió Europea que indiquen les característiques tècniques de l'aeronau i els requisits que compleix. El marcatge de classe permet identificar ràpidament el pes del dron, els sistemes de seguretat incorporats i les operacions que podrà realitzar dins del marc normatiu europeu.

Les classes C0, C1, C2, C3 i C4 estan principalment associades a la categoria oberta, mentre que les classes C5 i C6 estan vinculades a la categoria específica.

- **Estructura operativa: categories oberta, específica i certificada**

Paral·lelament a la classificació tècnica, la normativa europea diferencia tres categories operatives: oberta, específica i certificada. Aquesta divisió es basa en el nivell de risc de l'operació i no en la finalitat del vol.

Això significa que els requisits normatius no depenen de si el dron s'utilitza de manera recreativa o professional, sinó de les característiques i riscos de l'activitat desenvolupada.

La categoria oberta engloba les operacions de risc baix, mentre que, la categoria específica inclou operacions de risc mitjà que superen algun dels límits establerts per a la categoria oberta. Finalment, la categoria certificada està reservada per a operacions de risc elevat i amb requisits similars als de l'aviació tripulada.

5.1.1. Categoria oberta

La categoria oberta és la categoria més habitual dins de les operacions en l'àmbit civil i engloba les operacions de menor risc. Les activitats realitzades dins d'aquesta categoria no requereixen autorització operacional ni declaració prèvia davant AESA, ja que sempre es compleixen totes les limitacions establertes per la normativa. Entre aquestes limitacions destaquen el manteniment del dron dins del camp visual del pilot, una altura màxima de 120 metres i el respecte de les distàncies de seguretat respecte de persones no participants.

La categoria oberta es divideix en tres subcategories: A1, A2 i A3.

A1: La subcategoria A1 permet operar drons a prop de persones no participants, encara que no es poden sobrevolar aglomeracions de persones. Aquesta subcategoria està associada principalment als drons de classe C0 i C1.

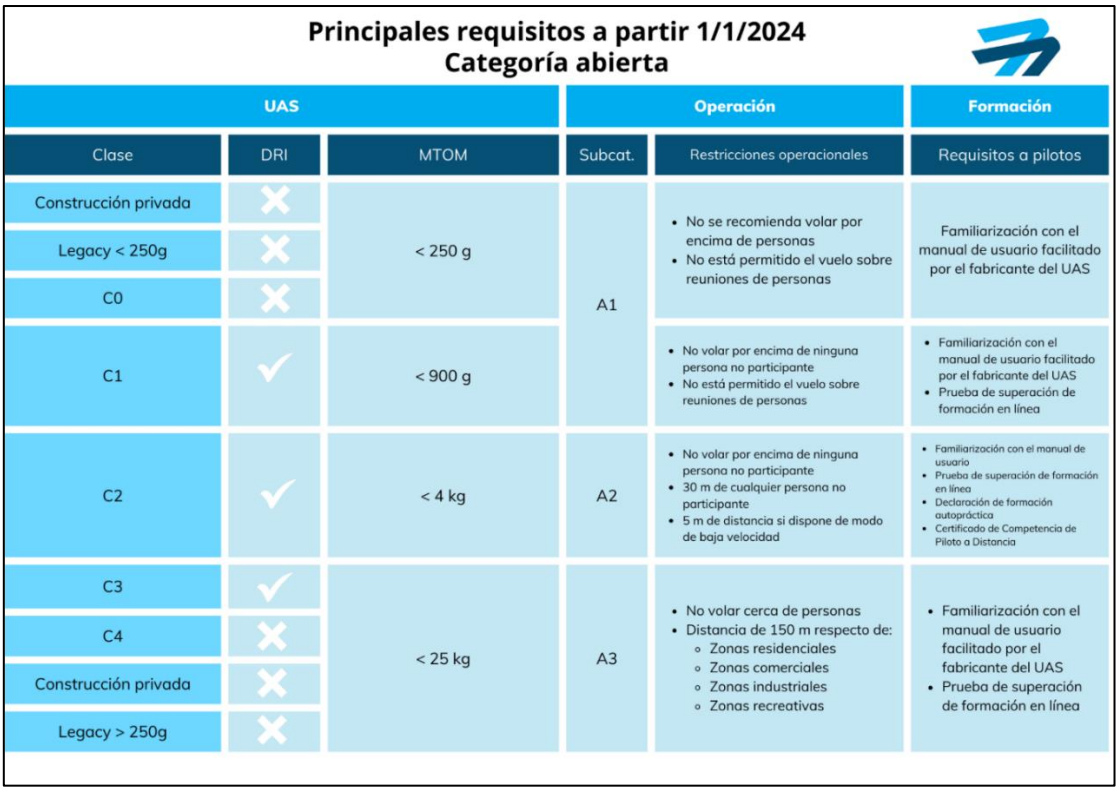
Els drons C0 tenen una massa inferior a 250 grams i representen el nivell de risc més baix previst per la normativa. Els drons C1 poden arribar fins als 900 grams i han d'incorporar determinats sistemes tècnics, com ara la identificació remota. Tot i que es permet volar prop de persones, el pilot ha d'evitar sempre que sigui possible el sobrevol directe de persones no participants.

A2: La subcategoria A2 està pensada per a operacions properes a persones, però amb majors limitacions de seguretat. En aquest cas s'utilitzen principalment drons de classe C2, amb una massa màxima inferior a 4 kg.

La normativa estableix una distància mínima de seguretat de 30 metres respecte de persones no participants. Aquesta distància es pot reduir fins a 5 metres quan el dron disposa d'un mode específic de baixa velocitat. A més, els pilots han d'acreditar una formació addicional respecte de la requerida per a les operacions A1 i A3.

A3: La subcategoria A3 permet fer operacions lluny de persones i en zones on el risc per a tercers sigui mínim. Inclou principalment drons de classe C3 i C4, que poden arribar fins als 25 kg de massa màxima.

Aquestes operacions s'han de desenvolupar en espais allunyats de persones no participants i a una distància mínima de 150 metres de zones residencials, comercials, industrials o recreatives. Per aquest motiu, aquesta subcategoria és habitual en treballs tècnics, activitats agrícoles, inspeccions d'infraestructures o operacions desenvolupades en entorns controlats.



Principales requisitos a partir 1/1/2024
Categoría abierta

UAS			Operación		Formación
Clase	DRI	MTOM	Subcat.	Restricciones operacionales	Requisitos a pilotos
Construcción privada	✗	< 250 g	A1	• No se recomienda volar por encima de personas • No está permitido el vuelo sobre reuniones de personas	Familiarización con el manual de usuario facilitado por el fabricante del UAS
Legacy < 250g	✗				
C0	✗				
C1	✓	< 900 g		• No volar por encima de ninguna persona no participante • No está permitido el vuelo sobre reuniones de personas	• Familiarización con el manual de usuario facilitado por el fabricante del UAS • Prueba de superación de formación en línea
C2	✓	< 4 kg	A2	• No volar por encima de ninguna persona no participante • 30 m de cualquier persona no participante • 5 m de distancia si dispone de modo de baja velocidad	• Familiarización con el manual de usuario • Prueba de superación de formación en línea • Declaración de formación autopráctica • Certificado de Competencia de Piloto a Distancia
C3	✓	< 25 kg	A3	• No volar cerca de personas • Distancia de 150 m respecto de: ◦ Zonas residenciales ◦ Zonas comerciales ◦ Zonas industriales ◦ Zonas recreativas	• Familiarización con el manual de usuario facilitado por el fabricante del UAS • Prueba de superación de formación en línea
C4	✗				
Construcción privada	✗				
Legacy > 250g	✗				

Figura 1. Principals requisits de la categoria oberta segons la normativa europea.

Font: Agència Estatal de Seguretat Aèria (AESA), 2024.

5.1.2. Categoria específica

La categoria específica inclou operacions que no poden desenvolupar-se dins dels límits establerts per a la categoria oberta. En aquest cas, es tracten d'activitats que presenten un nivell de risc superior i que, per tant, exigeixen mesures addicionals de seguretat. Aquesta categoria ocupa una posició intermèdia entre la categoria oberta i la categoria certificada.

Els drons associats a aquesta categoria solen correspondre a les classes C5 i C6, i. a diferència de la categoria oberta, les operacions de la categoria específica requereixen una intervenció administrativa prèvia per part d'AESA.

Una de les vies per la normativa és la declaració operacional que compleixi els requisits dels *Standard Scenarios* (STS) o Pre-Defined Risk Assesment (PDRA), mitjançant aquest procediment, l'operador comunica a AESA que compleix tots els requisits exigits per desenvolupar una determinada operació. La responsabilitat principal recau sobre l'operador, que ha de garantir que l'activitat es desenvoluparà de manera segura i conforme a la normativa vigent.

Quan l'operació presenta un nivell de complexitat superior, l'operador ha d'obtenir una autorització operacional emesa per AESA. En aquest cas, l'autoritat aeronàutica analitza les característiques concretes de l'activitat abans d'autoritzar-ne l'execució.

Aquest procediment implica un major control administratiu i una avaluació específica dels riscos associats a l'operació.

5.1.3. Categoria certificada

La categoria certificada correspon a les operacions amb un nivell de risc més elevat. Es tracta d'activitats que, per les seves característiques, poden equiparar-se a determinades operacions de l'aviació tripulada. Per aquest motiu, els requisits exigits són considerablement més estrictes i poden afectar tant l'aeronau com l'operador i el pilot. Aquesta categoria està reservada per a situacions específiques en què les conseqüències d'un possible incident podrien ser especialment greus.

5.1.4. Normativa en les diferents categories

Un altre element important és que la normativa no diferencia entre ús recreatiu i ús professional, sinó que el criteri principal és el nivell de risc de l'operació. Això significa que qualsevol persona que utilitzi un dron ha de respectar les limitacions establertes segons la categoria corresponent, independentment de la finalitat concreta del vol.

En relació amb les característiques bàsiques dels drons, cal destacar especialment tres aspectes. En primer lloc, la seva mobilitat, ja que poden desplaçar-se amb facilitat i accedir a espais on altres sistemes de vigilància no arriben. En segon lloc, la seva capacitat de captació d'informació, gràcies a càmeres i sensors cada vegada més avançats. I, finalment, la seva relativa invisibilitat o baixa perceptibilitat, especialment en drons petits, cosa que dificulta que les persones siguin plenament conscients de quan estan sent observades. Aquests tres elements són els que converteixen els drons en una tecnologia especialment sensible des del punt de vista de la privacitat.

5.2. Relació entre les classes tècniques i les categories operatives

Classe	Pes màxim	Categoria operativa	Subcategoria	Característiques principals
C0	< 250 g	Oberta	A1	Operacions prop de persones. Risc baix.
C1	< 900 g	Oberta	A1	Identificació remota obligatòria. No es poden sobrevolar aglomeracions.
C2	< 4 kg	Oberta	A2	Distància mínima de 30 m respecte de persones no participants.
C3	< 25 kg	Oberta	A3	Operacions allunyades de persones i zones urbanes.
C4	< 25 kg	Oberta	A3	Operacions en entorns controlats i lluny de tercers.
C5	Variable	Específica	-	Operacions de risc mitjà subjectes a autorització operacional.
C6	Variable	Específica	-	Operacions complexes amb requisits tècnics addicionals.

Taula 1. Relació entre classes tècniques i categories operatives dels drons.

Font: elaboració pròpia.

Com es pot observar a la taula anterior, la normativa europea estableix una relació directa entre les característiques tècniques dels drons i les condicions en què es poden utilitzar.

A mesura que augmenta el pes de l'aeronau i la complexitat de les seves operacions, també augmenten les limitacions i els requisits exigits als operadors per garantir la seguretat de les persones i de l'espai aeri.

Aquesta classificació permet adaptar les mesures de control al nivell de risc de cada operació, diferenciant entre activitats de baix risc, incloses dins de la categoria oberta, i operacions més complexes, que passen a formar part de la categoria específica o certificada. D'aquesta manera, la normativa intenta mantenir un equilibri entre les possibilitats que ofereix aquesta tecnologia i la necessitat de protegir la seguretat.

5.3. Usos dels drons en l'àmbit civil

En els darrers anys, l'ús dels drons en l'àmbit civil ha experimentat un creixement molt important, permeten obtenir informació de manera ràpida, accedir a zones difícils i captar imatges. Aquests dispositius ja no s'utilitzen amb finalitats recreatives, sinó també en activitats relacionades amb la seguretat, la vigilància i les emergències. Aquest augment respon principalment als avantatges que ofereixen, ja que des de perspectives d'altres sistemes no poden assolir amb la mateixa facilitat.

Un dels àmbits en què els drons tenen una presència més destacada és el de la seguretat. Diversos estudis assenyalen que aquests aparells s'utilitzen cada vegada més en tasques de vigilància i control, especialment en operacions policials, control de fronteres o supervisió d'espais públics. La seva capacitat de desplaçament i de captació d'imatges en temps real permet ampliar la capacitat d'observació de les autoritats i facilitar el seguiment de determinades situacions.

Algunes experiències desenvolupades per la Guardia Civil han mostrat l'ús de drons en operacions de vigilància marítima i control fronterer. Segons els informes analitzats, aquests dispositius permeten detectar embarcacions petites, seguir moviments i ampliar la capacitat de supervisió més enllà del territori visible des de terra. Aquesta utilització posa de manifest que els drons poden actuar com una eina de suport molt útil per a les forces de seguretat, especialment en espais amplis o de difícil accés.

Relacionat amb això, els drons també tenen un paper destacat en activitats de vigilància. La seva incorporació de càmeres, sensors i sistemes de geolocalització fa possible captar imatges i dades de manera constant i des de diferents angles. Aquesta capacitat, permet realitzar controls aeris, monitoritzar espais públics o supervisar esdeveniments multitudinaris amb més facilitat que altres sistemes tradicionals.

Ara bé, aquest ús també planteja interrogants importants des del punt de vista de la privacitat ja que a diferència de les càmeres fixes, els drons tenen una gran mobilitat i poden operar de manera menys visible. Això significa que moltes persones poden no ser plenament conscients de quan estan sent observades.

Per aquest motiu, diversos autors assenyalen que l'ús de drons en activitats de vigilància pot augmentar el risc de control excessiu o de captació desproporcionada d'informació.

A més de la seguretat i la vigilància, els drons s'utilitzen també en situacions d'emergència i rescat. En aquest àmbit, la seva rapidesa de desplegament i la seva capacitat per arribar a zones de difícil accés els converteixen en una eina molt útil. Per exemple, alguns projectes han utilitzat drons per monitoritzar incendis forestals o transportar material sanitari en entorns urbans.

En aquests casos, els drons permeten obtenir informació en temps real i millorar la coordinació dels equips d'emergència. Això demostra que aquestes tecnologies poden tenir una funció clarament beneficiosa des del punt de vista social.

Un altre àmbit rellevant és la gestió urbana. Primer, hi ha diversos estudis sobre ciutats intel·ligents assenyalen que els drons poden contribuir a la supervisió i manteniment d'infraestructures, al control del trànsit i a la monitorització ambiental. Així, aquests dispositius s'utilitzen en inspeccions de ponts, carreteres, línies elèctriques o edificis, permetent reduir costos i riscos laborals.

També s'han desenvolupat aplicacions relacionades amb la gestió del trànsit i la mobilitat urbana on els drons poden facilitar la detecció d'accidents i controlar zones congestionades. Això explica que cada vegada més administracions considerin aquestes tecnologies com una eina útil dins del desenvolupament de les "smart cities".

Tot i això, aquest augment dels usos civils també implica nous reptes jurídics i socials, perquè la mateixa tecnologia que pot ajudar en emergències és també capaç de recopilar grans quantitats d'informació sobre les persones. Per això, el debat no se centra únicament en la utilitat dels drons, sinó també, en els límits que haurien d'existir per evitar usos excessius.

En resum, els drons s'han convertit en una tecnologia amb múltiples aplicacions en l'àmbit civil. La seva flexibilitat, mobilitat i capacitat de captació d'informació expliquen el seu creixement en sectors com la seguretat, la vigilància, les emergències i la gestió urbana. No obstant això, aquestes mateixes característiques fan que el seu ús plantegi riscos importants per a la privacitat i els drets fonamentals, especialment quan les activitats de control es desenvolupen de manera poc visible.

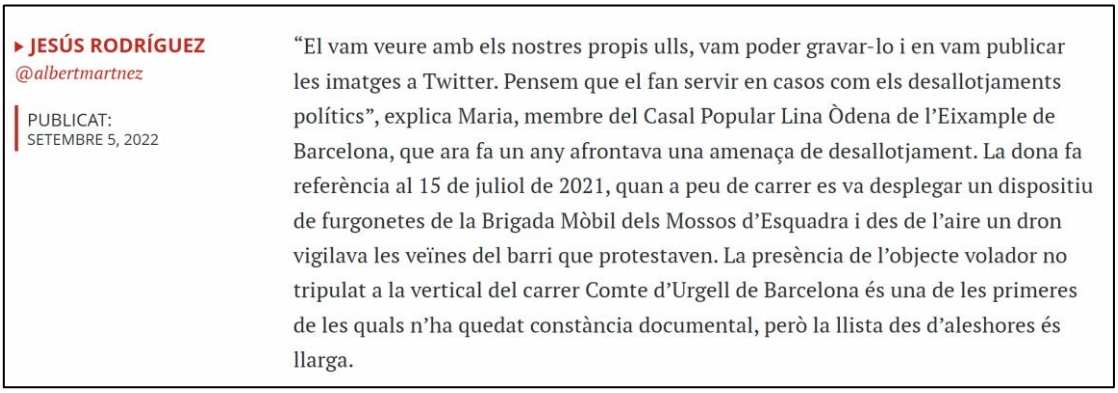
5.4. Drons i vigilància

Una de les característiques principals dels drons és que poden captar imatges i informació des del cel, on, la majoria tenen càmeres d'alta resolució, sensors i sistemes de geolocalització. Això els permet gravar espais, persones i moviments amb bastanta precisió. D'aquesta manera, aquests dispositius són útils en activitats de vigilància i control, però també poden augmentar els riscos per a la privacitat humana.

A diferència d'altres sistemes de videovigilància, els drons destaquen per la seva gran mobilitat i rapidesa, ja que poden operar des de diferents altures i angles, a més d'obtenir una àmplia visibilitat del lloc que s'està enregistrant. Aquesta flexibilitat els ajuda a arribar a llocs on les càmeres no poden accedir i a seguir situacions en moviment amb més facilitat, precisament aquesta capacitat de desplaçament és una de les coses que distingeix els drons d'altres sistemes tradicionals de control.

Molts drons són petits i difícils de veure a distància, especialment en entorns urbans o en llocs amb molta activitat, això provoca que, en nombroses ocasions, les persones no se n'adonin que estan sent gravades. S'ha de tenir en compte que aquest element d'invisibilitat és molt rellevant des del punt de vista legal, perquè dificulta el control social sobre aquestes pràctiques de vigilància.

Aquest problema es pot observar en alguns casos d'ús policial de drons: un exemple és el desplegament de drons dels Mossos d'Esquadra durant manifestacions i desnonaments a Barcelona. Alguns informes i testimonis indiquen que aquests objectes enregistraven imatges aèries dels participants sense que moltes persones fossin conscients de que estaven sent gravades. A més, des de l'any 2021, part de les actuacions de drons en usos policials es fan sense el control judicial i el marc jurídic existent a Catalunya.



▸ JESÚS RODRÍGUEZ
@albertmartnez

PUBLICAT:
SETEMBRE 5, 2022

"El vam veure amb els nostres propis ulls, vam poder gravar-lo i en vam publicar les imatges a Twitter. Pensem que el fan servir en casos com els desallotjaments polítics", explica Maria, membre del Casal Popular Lina Òdena de l'Eixample de Barcelona, que ara fa un any afrontava una amenaça de desallotjament. La dona fa referència al 15 de juliol de 2021, quan a peu de carrer es va desplegar un dispositiu de furgonetes de la Brigada Mòbil dels Mossos d'Esquadra i des de l'aire un dron vigilava les veïnes del barri que protestaven. La presència de l'objecte volador no tripulat a la vertical del carrer Comte d'Urgell de Barcelona és una de les primeres de les quals n'ha quedat constància documental, però la llista des d'aleshores és llarga.

Figura 2. Fragment de testimoni sobre l'ús de drons en l'acció policial
Font: fragment de testimoni publicat a "Drons, càmeres i acció policial sense control", Directa (2022).

Aquestes situacions demostren que el problema no és només que els drons captin imatges, sinó també, el fet de no saber què es faran amb aquestes dades, quant temps es guarden o qui hi pot accedir.

Com recorden organitzacions de protecció de dades, la captació d'imatges de persones identificables és un tractament de dades personals, per tant, està sotmès als principis i garanties del Reglament General de Protecció de Dades.

En aquest sentit, una de les principals preocupacions es que els drons ens poden facilitar una vigilància contínua, poc visible i difícil de limitar en la pràctica, i, la combinació de mobilitat, captació d'imatges i baixa perceptibilitat converteix aquests dispositius en una eina molt sensible des del punt de vista dels drets fonamentals.

6. MARC NORMATIU ESPANYOL

6.1. Regulació dels drons

La regulació dels drons a Espanya s'ha tornat molt més complexa i detallada durant els darrers anys perquè l'augment d'aquestes tecnologies en l'àmbit civil ha provocat que apareixin nous problemes relacionats amb la seguretat, la privacitat i el control de l'espai aeri. Fa relativament poc, els drons s'usaven sobretot en activitats recreatives o en usos molt puntuals dins del món audiovisual, però actualment s'utilitzen en àmbits molt més amplis, com la vigilància policial, la supervisió d'infraestructures, la gestió d'emergències o fins i tot el control d'espais públics, fet que ha obligat les administracions a desenvolupar un marc normatiu molt més específic i tècnic per intentar controlar els riscos que poden generar aquestes operacions. Per aquest motiu, la regulació actual no tracta els drons com simples aparells electrònics, sinó com aeronaus capaces d'afectar la seguretat aèria, la seguretat ciutadana i els drets fonamentals de les persones.

Actualment, la principal norma estatal és el Real Decreto 517/2024, aprovat el 4 de juny de 2024 i publicat al BOE, que desenvolupa el règim jurídic aplicable a la utilització civil dels sistemes d'aeronaus no tripulades (UAS) i adapta la normativa espanyola al marc europeu establert pels Reglaments (UE) 2019/947 i 2019/945. Aquest Reial Decret és especialment rellevant perquè no es limita només a regular aspectes bàsics del vol, sinó que introdueix una regulació molt més àmplia sobre qüestions relacionades amb les zones geogràfiques de vol, els requisits tècnics dels operadors, les limitacions en entorns urbans o les activitats desenvolupades per organismes públics i forces de seguretat. A més, una de les modificacions més importants és que desapareix la diferenciació tradicional entre ús recreatiu i ús professional, de manera que, la normativa passa a centrar-se principalment en el nivell de risc que genera cada operació i no tant en la finalitat concreta en la qual es fa servir el dron. Això implica que qualsevol persona que utilitzi un dron amb càmera en espais on hi pugui haver terceres persones està sotmesa a obligacions específiques, encara que el vol tingui una finalitat personal, recreativa o d'oci.

La supervisió d'aquesta normativa correspon principalment a l'Agencia Estatal de Seguridad Aérea (AESA), que es un organisme dependent del Ministeri de Transports i Mobilitat Sostenible, aquest és l'encarregat de controlar gran part de les operacions amb drons a Espanya.

AESA no només publica instruccions i limitacions de vol, sinó que també gestiona registres oficials, certificacions, formacions i autoritzacions específiques per a determinades activitats. A més, AESA és responsable d'establir gran part dels criteris tècnics relacionats amb la seguretat operacional dels vols i coordina les restriccions aplicables a l'espai aeri juntament amb altres organismes com ENAIRE.

Aquesta coordinació és una de les qüestions més importants de la normativa actual, ja que l'augment dels drons ha provocat que cada vegada existeixin més conflictes entre les operacions amb aeronaus no tripulades i la resta d'usuaris de l'espai aeri.

Un dels aspectes més detallats del Reial Decret 517/2024 és la regulació de les anomenades "zones geogràfiques UAS", és a dir, espais en què els vols amb drons poden estar prohibits, restringits o sotmesos a condicions especials per motius relacionats amb la seguretat pública, la protecció d'infraestructures, la defensa nacional o la privacitat. Aquesta part de la normativa és especialment extensa perquè estableix diferents tipus de limitacions segons el tipus d'espai afectat. Per exemple, existeixen restriccions específiques al voltant d'aeroports i heliports, limitacions sobre espais aeris controlats, prohibicions relacionades amb infraestructures estratègiques i restriccions vinculades a entorns urbans amb una elevada concentració de persones.

El mateix Reial Decret inclou articles específics dedicats a aquestes qüestions i estableix que la informació oficial sobre les restriccions de vol ha de consultar-se obligatòriament a través de la plataforma *ENAIRE Drones* abans de cada operació. Aquest aspecte és especialment rellevant perquè mostra clarament que el legislador és conscient que els drons poden generar riscos molt més amplis que els estrictament tècnics, especialment quan operen en espais públics o zones urbanes.

A més, la normativa actual introdueix regulacions específiques per a les operacions desenvolupades per organismes públics i forces de seguretat, especialment en activitats relacionades amb vigilància, control fronterer, recerca i salvament, lluita contra incendis o operacions policials. El mateix Reial Decret 517/2024 estableix que determinades activitats públiques poden operar sota condicions diferents de les operacions civils ordinàries sempre que existeixi una justificació vinculada a l'interès general i s'apliquin mesures de seguretat adequades. Aquesta qüestió és especialment important perquè demostra que els drons s'han convertit en eines estratègiques dins de les polítiques de vigilància i control institucional. Aquí, apareixen moltes de les preocupacions jurídiques actuals, ja que l'augment de la vigilància aèria fa créixer també els dubtes sobre els límits reals del control policial i sobre la capacitat de supervisar adequadament aquestes pràctiques.

Un exemple especialment rellevant de l'expansió d'aquestes pràctiques és l'ús de drons durant el control de platges i espais turístics massificats en diferents municipis espanyols després de la pandèmia de la COVID-19. Diversos ajuntaments i policies locals van començar a utilitzar drons equipats amb càmeres per supervisar l'aforament de platges, controlar aglomeracions i detectar possibles incompliments de les restriccions sanitàries. A municipis com Benidorm o Marbella, aquests dispositius permetien observar grans extensions de territori des de l'aire i transmetre imatges en temps real als centres de control policial.

Tot i que aquestes mesures es justificaven per motius de seguretat i salut pública, diferents experts i organismes de protecció de dades van advertir que aquest tipus de vigilància podia generar problemes importants relacionats amb la privacitat, especialment perquè moltes persones desconeixien fins a quin punt estaven sent monitoritzades mentre es trobaven en espais públics. Aquest tipus de situacions mostren com els drons han passat de ser eines tècniques molt concretes a convertir-se en instruments habituals de supervisió i control de l'espai, ampliant considerablement la capacitat d'observació.

Un altre aspecte destacat del nou Reial Decret és que introdueix noves obligacions relacionades amb la identificació dels drons, els registres oficials i els requisits tècnics dels operadors. Per exemple, la normativa estableix l'obligació de registrar-se oficialment com a operador en nombrosos casos i reforça la necessitat d'utilitzar sistemes d'identificació remota en determinades operacions. A més, també apareixen noves exigències relacionades amb les assegurances, les formacions tècniques i els certificats necessaris per desenvolupar activitats més complexes.

Aquest increment de requisits mostra clarament que les administracions consideren els drons tecnologies amb una capacitat creixent de generar riscos no només físics, sinó també relacionats amb la privacitat, la seguretat pública i la protecció de dades personals.

Tot i aquest desenvolupament normatiu cada vegada més ampli i detallat, diferents organismes i experts continuen assenyalant que encara existeixen problemes importants relacionats amb l'aplicació real de la regulació, especialment perquè la tecnologia evoluciona molt més ràpidament que les normes i perquè moltes pràctiques desenvolupades amb drons es mouen en espais jurídics difícils de controlar a la pràctica.

En conclusió, una de les principals qüestions que apareixen actualment en el debat jurídic és si el marc normatiu vigent és realment suficient per garantir una protecció efectiva dels drets fonamentals davant l'expansió de les tecnologies de vigilància aèria i de captació massiva d'informació.

6.2. Protecció de dades i privacitat

La protecció de dades personals és una part essencial del marc jurídic que s'ha de tenir en compte quan es parla de drons, perquè molts d'aquests dispositius no només volen per l'aire, sinó que també poden captar imatges, enregistrar vídeos, recollir ubicacions o obtenir informació que permet identificar persones concretes.

Per això, quan un dron incorpora una càmera i grava persones en un espai públic, ja no estem parlant només d'una qüestió de seguretat aèria, sinó també d'un possible tractament de dades personals, i aquest tractament queda sotmès a les normes de protecció de dades. El Reglament General de Protecció de Dades, conegut com a RGPD, parteix d'aquesta idea, protegir les persones físiques quan es tracten les seves dades personals i garantir que aquest tractament respecti els seus drets i llibertats fonamentals. El RGPD afirma que la protecció de les dades de les persones és un dret fonamental reconegut a la Carta dels Drets Fonamentals de la Unió Europea.

En el cas dels drons, aquesta qüestió és important perquè la captació d'imatges pot produir-se d'una manera menys evident que amb altres sistemes tradicionals. Una càmera fixa situada en una façana o en un edifici sol ser més visible i més fàcil d'identificar, mentre que un dron pot moure's, canviar d'altura, acostar-se a zones diferents i captar imatges des de perspectives que una persona no sempre pot preveure. Això fa que el problema no sigui només si es grava o no es grava, sinó en quines condicions es fa, amb quina finalitat, durant quant temps es conservaran les imatges i qui hi podrà accedir. Aquesta és la idea central que convé mantenir: la protecció de dades no prohibeix tota captació d'imatges, però exigeix que aquesta captació estigui justificada, sigui limitada i respecti unes garanties mínimes.

El RGPD no tracta els drons com una cosa neutra sense conseqüències, sinó que recorda que la ràpida evolució tecnològica ha creat nous reptes per a la protecció de dades personals, perquè, són una tecnologia que ha crescut molt ràpidament i que permet formes de captació d'informació que fa uns anys eren molt menys habituals. A més, el RGPD també deixa clar que la protecció de dades ha de ser "tecnològicament neutra", és a dir, que no depèn del tipus concret d'eina utilitzada, sinó del fet que hi hagi tractament de dades personals. Per tant, si una imatge captada per un dron permet identificar una persona, encara que sigui en un espai públic, aquella imatge pot ser una dada personal i s'han d'aplicar les garanties corresponents.

A l'Estat espanyol, aquesta protecció es duu a terme amb la Llei orgànica 3/2018, de protecció de dades personals i garantia dels drets digitals, coneguda com a LOPDGDD. Aquesta llei adapta el RGPD al context espanyol i parteix de la idea de que la protecció de les persones en relació amb el tractament de dades personals és un dret fonamental protegit per l'article 18.4 de la Constitució espanyola. Aquest article diu que la llei ha de limitar l'ús de la informàtica per garantir l'honor, la intimitat personal i familiar i el ple exercici dels drets de la ciutadania.

La LOPDGDD també recull que la protecció de dades dona a la persona un cert control sobre les seves dades, sobre l'ús que se'n fa i sobre la finalitat per a la qual es van recollir. Això vol dir que no n'hi ha prou en dir que una imatge s'ha captat "per seguretat" o "per control", sinó que cal concretar quina és la finalitat real, si aquesta finalitat és legítima i si el tractament és necessari per aconseguir-la. En el cas d'un dron utilitzat per vigilar un espai públic, aquesta exigència és clau, perquè pot haver-hi una finalitat legítima, com protegir la seguretat o controlar una situació de risc, però això no dona ''carta blanca'' per gravar qualsevol cosa, durant qualsevol temps i sense informar a les persones afectades.

Un dels principis més importants del RGPD és el principi de licitud, lleialtat i transparència. Aplicat als drons, això significa que la captació d'imatges ha de tenir una base jurídica que la justifiqui, ha de fer-se d'una manera que no sigui abusiva i ha de ser comprensible per a les persones afectades. El problema pràctic és que, amb els drons, la transparència pot ser més difícil que amb altres sistemes. Per exemple, si una administració utilitza un dron per controlar una zona concreta, la ciutadania hauria de poder saber que s'estan captant imatges, qui és el responsable del tractament i amb quina finalitat s'utilitzaran. Si aquesta informació no és clara, la persona afectada difícilment podrà exercir els seus drets d'accés, supressió o oposició.

Un altre principi essencial és el de limitació de la finalitat. Aquest principi obliga que les dades es recullin amb una finalitat concreta, explícita i legítima, i que després no s'utilitzin per a altres objectius incompatibles. En el cas dels drons, això és especialment delicat perquè una mateixa gravació pot contenir molta informació que no estava directament relacionada amb l'objectiu inicial. Per exemple, un dron utilitzat per controlar l'estat d'una infraestructura pot captar també persones que passen per la zona, vehicles, domicilis o altres elements de la vida quotidiana. Per això, el responsable del tractament hauria de limitar l'ús de les imatges només a la finalitat prevista i evitar que aquest material acabi utilitzant-se per altres objectius sense una justificació adequada.

A més, és molt important el principi de minimització de dades. Aquest principi vol dir que només s'han de recollir les dades necessàries per a la finalitat perseguida i no més. En relació amb els drons, això obliga a preguntar-se si realment cal gravar imatges identificables de persones, si es podria reduir l'angle de captació, si es podria evitar enregistrar determinades zones o si seria suficient utilitzar imatges menys invasives. Les directrius europees sobre videovigilància insisteixen en aquesta idea i indiquen que, abans d'instal·lar o utilitzar un sistema de videovigilància, el responsable ha d'analitzar de manera crítica si la mesura és adequada i necessària, i que només s'hauria d'utilitzar si la finalitat no es pot aconseguir raonablement per altres mitjans menys intrusius. Aquest criteri és molt útil per analitzar l'ús dels drons perquè obliga a no donar per fet que la tecnologia és necessària només perquè és útil. Un dron pot ser ràpid, eficaç i pràctic, però això no significa automàticament que sigui proporcional.

La proporcionalitat exigeix valorar si el benefici que aporta compensa la possible afectació sobre la privacitat. Per exemple, pot ser més justificable utilitzar un dron en una situació d'emergència, com la recerca d'una persona desapareguda o el control d'un incendi, que utilitzar-lo de manera continuada per observar una zona urbana sense una causa concreta. En aquest punt es veu clarament que el dret no només pregunta si la tecnologia funciona, sinó si és legítim utilitzar-la d'aquella manera.

La guia de l'AEPD (l'Agència Espanyola de Protecció de Dades) sobre videocàmeres també és útil encara que no parli només de drons, perquè explica que el tractament d'imatges amb finalitats de videovigilància ha d'estar vinculat a una finalitat concreta, com pot ser garantir la seguretat.

Un altre element important és la conservació de les imatges. Des del punt de vista de la protecció de dades, no és acceptable conservar informació personal durant més temps del necessari. En el cas dels drons, això vol dir que les imatges captades no haurien de guardar-se indefinidament "per si de cas", sinó només durant el temps necessari per a la finalitat que va justificar la gravació. Aquesta qüestió és important perquè una gravació aèria pot incloure moltes dades no buscades, per això, limitar el temps de conservació és una garantia bàsica per evitar que una captació puntual es converteixi en una acumulació innecessària d'informació.

La seguretat de les dades també és una obligació essencial ja que quan es capten imatges amb drons, no només importa el moment de la gravació, sinó també què passa després amb aquests arxius. Les imatges poden descarregar-se, emmagatzemar-se, enviar-se a altres dispositius o ser revisades per diferents persones. Per aquest motiu, el responsable del tractament ha de garantir que aquestes dades estiguin protegides davant accessos no autoritzats, pèrdues o usos indeguts. La LOPDGDD preveu infraccions relacionades amb l'incompliment de mesures exigides pel RGPD, com no fer una avaluació d'impacte quan sigui necessària o no adoptar garanties suficients en determinats tractaments.

En determinats casos, l'ús de drons podria exigir una avaluació d'impacte en protecció de dades. Aquesta eina serveix per analitzar prèviament els riscos que un tractament pot generar sobre els drets i llibertats de les persones, i és especialment important quan s'utilitzen tecnologies que poden comportar una vigilància més difícil de controlar. En aquests casos, aquesta avaluació pot ser necessària si l'operació implica gravacions sistemàtiques, captació d'imatges en espais amplis i/o tractaments que poden afectar moltes persones. El RGPD relaciona aquestes avaluacions amb tractaments que poden suposar un alt risc per als drets i llibertats de les persones, i la LOPDGDD també considera greu no dur-les a terme quan són exigibles.

L'AEPD és l'autoritat encarregada de vetllar pel compliment de la normativa de protecció de dades a Espanya i publica guies, criteris i recomanacions que ajuden a aplicar el RGPD en casos concrets.

En conjunt, el RGPD i la LOPDGDD estableixen un marc de garanties que afecta clarament l'ús de drons quan aquests capten dades personals. Aquest marc no prohibeix l'ús dels drons, però sí obliga a utilitzar-los amb límits: ha d'existir una finalitat clara, una base jurídica adequada, una captació proporcional, una informació suficient a les persones afectades, una conservació limitada de les imatges i unes mesures de seguretat adequades. Dit d'una manera senzilla, el dret no diu que no es puguin utilitzar drons, sinó que no es poden utilitzar de qualsevol manera.

Per tant, en relació amb la qüestió principal, la protecció de dades permet veure que el problema principal no és només la regulació del vol, sinó la regulació de la informació que el dron pot obtenir. Un dron pot complir les normes d'AESA, volar en una zona autoritzada i respectar les condicions de seguretat aèria, però això no vol dir automàticament que el tractament de les imatges sigui correcte des del punt de vista de la privacitat.

Una cosa és que el vol sigui legal i una altra que la captació i ús de les dades personals sigui legítima, proporcional i respectuosa amb els drets de les persones.

Per últim, el marc normatiu de protecció de dades funciona com una segona capa de control sobre l'ús dels drons. Primer cal preguntar-se si el dron pot volar segons la normativa aeronàutica, però després cal preguntar-se què està captant, per què ho capta, qui ho tracta, durant quant temps i amb quines garanties. Aquesta segona pregunta és la que connecta directament amb el dret a la privacitat i amb els riscos de vigilància tecnològica que estem analitzant.

Per això, el RGPD i la LOPDGDD no són normes secundàries, sinó peces essencials per valorar si el marc normatiu espanyol protegeix realment la privacitat davant l'ús civil dels drons amb finalitats de vigilància.

6.3. Límits legals a la vigilància

La vigilància sempre ha estat vinculada a la idea de seguretat i control, però en l'actualitat, aquest debat s'ha tornat molt més complex. Els drons són probablement un dels exemples més clars d'aquest canvi, ja que permeten captar imatges des de l'aire amb una gran mobilitat i arribar a espais que abans resultaven molt més complicats de controlar. Per aquest motiu, el dret ha hagut d'establir límits jurídics que intentin evitar que aquesta capacitat tecnològica es converteixi en una forma de vigilància excessiva. En aquest sentit, la regulació espanyola no prohibeix la vigilància amb drons, però sí obliga que aquesta compleixi determinades garanties relacionades amb la proporcionalitat, la necessitat i la legitimitat de les mesures adoptades.

El primer gran límit és el principi de proporcionalitat. Aquest principi és fonamental perquè obliga a valorar si la vigilància és adequada respecte de la finalitat perseguida i si la possible afectació sobre la privacitat és raonable o, per contra, excessiva. La Llei orgànica 4/1997 sobre la utilització de videocàmeres per les Forces i Cossos de Seguretat estableix expressament que l'ús de sistemes de captació d'imatges ha d'estar presidit pel principi de proporcionalitat i per la intervenció mínima. Això significa que no es poden utilitzar mecanismes de control simplement perquè siguin moderns, sinó només quan realment existeixi una justificació suficient i quan la vigilància no superi allò estrictament necessari. Aquest criteri és especialment important en el cas dels drons perquè aquests dispositius permeten captar una quantitat molt més gran d'informació que altres sistemes tradicionals de videovigilància, especialment per la seva mobilitat i capacitat per desplaçar-se sobre espais amplis sense gaire dificultat.

El principi de necessitat obliga a demostrar que la vigilància és realment imprescindible i que no existeix una altra alternativa menys intrusiva per aconseguir la mateixa finalitat. Això és important perquè evita que les empreses utilitzin tecnologies de control simplement perquè són eficients o perquè permeten obtenir més informació. En el cas dels drons, la necessitat obliga a justificar per què cal utilitzar un dispositiu capaç de captar imatges aèries i no altres mecanismes menys agressius des del punt de vista de la privacitat. Aquesta idea apareix de manera molt clara en les guies de l'Agència Espanyola de Protecció de Dades, que insisteixen que qualsevol sistema de videovigilància ha d'analitzar prèviament si la finalitat perseguida es pot aconseguir d'una altra manera menys invasiva.

Aquest criteri és especialment rellevant perquè els drons tenen una capacitat molt alta de captar informació que va més enllà de l'objectiu inicial. Per exemple, un dron utilitzat per controlar un esdeveniment multitudinari pot acabar enregistrant també habitatges, matrícules, moviments de persones o recorreguts que no tenien cap relació directa amb la finalitat original de l'operació.

Això provoca que el problema no sigui només la captació inicial d'imatges, sinó també l'acumulació posterior d'informació. Diversos informes jurídics sobre protecció de dades i drons han advertit precisament d'aquest risc, especialment perquè les noves tecnologies permeten emmagatzemar grans quantitats d'informació durant períodes llargs de temps i combinar-les posteriorment amb altres dades.

A més, el principi de necessitat també afecta la durada i intensitat de la vigilància. Una vigilància puntual en una situació concreta no té el mateix impacte que un control continuat i permanent sobre un espai públic. El problema és que els drons faciliten precisament aquesta vigilància constant perquè poden moure's, seguir persones o monitoritzar zones àmplies sense grans dificultats tècniques. Per això, moltes de les discussions actuals sobre drons no es centren només en la legalitat del vol, sinó en el risc que aquestes tecnologies acabin normalitzant formes de control molt més permanents sobre la ciutadania.

El tercer gran límit és la legitimitat. Jurídicament, qualsevol mesura de vigilància ha de perseguir una finalitat legítima prevista per una norma i compatible amb els drets fonamentals. Això vol dir que no es pot vigilar simplement per curiositat, control genèric o acumulació preventiva d'informació. La finalitat ha de ser concreta i suficientment important per justificar la possible afectació sobre la privacitat.

La legislació espanyola permet la utilització de sistemes de videovigilància per motius relacionats amb la seguretat ciutadana, la prevenció de delictes o la protecció d'infraestructures, però sempre dins d'uns límits determinats i sota mecanismes de control.

Aquesta qüestió és especialment delicada en el cas dels drons perquè la seva capacitat tecnològica és molt superior a la de molts sistemes tradicionals de videovigilància.

Això incrementa molt la capacitat d'observació de les administracions i fa créixer també el risc d'una vigilància més invasiva. Per això, diferents estudis jurídics han advertit que la legitimitat de la vigilància no depèn només de la finalitat general de seguretat, sinó també de la manera concreta en què aquesta vigilància es desenvolupa a la pràctica.

També és important tenir en compte que la legitimitat exigeix transparència i control posterior sobre les imatges obtingudes. El Reial decret 596/1999, que desenvolupa la Llei orgànica 4/1997, regula qüestions com la conservació de les gravacions, la seva destrucció o l'exercici dels drets de les persones afectades.

Això és especialment important perquè el problema de la vigilància no acaba en el moment de la captació d'imatges, sinó que continua després, quan aquestes dades es guarden, s'analitzen o es comparteixen. Un sistema de vigilància podria començar amb una finalitat aparentment legítima i acabar convertint-se en una

eina de control molt més extensa si no existeixen garanties suficients sobre l'ús posterior de la informació.

En definitiva, els límits legals a la vigilància intenten evitar que la capacitat tècnica dels drons es converteixi automàticament en una justificació per ampliar el control sobre la ciutadania. La proporcionalitat obliga a evitar mesures excessives, la necessitat exigeix demostrar que la vigilància és realment imprescindible i la legitimitat reclama que qualsevol captació d'imatges tingui una finalitat concreta i jurídicament justificada.

Precisament el gran problema actual és que la tecnologia evoluciona molt més ràpidament que la capacitat del dret per controlar-ne els efectes, fet que provoca que moltes pràctiques de vigilància acabin situant-se en espais jurídics difícils de supervisar i generin dubtes reals sobre si la protecció de la privacitat és suficient davant l'expansió de les tecnologies de control aeri.

7. ESTUDI PRÀCTIC: PERCEPCIONS PROFESSIONALS SOBRE LA NORMATIVA I LA PRIVACITAT EN L'ÚS DELS DRONS

7.1. Objectiu de l'estudi

L'objectiu principal d'aquest qüestionari és conèixer la percepció de persones que utilitzen drons en diferents àmbits professionals sobre la normativa vigent, la protecció de la privacitat i les dificultats que poden aparèixer durant el desenvolupament de les seves activitats professionals.

Es vol identificar quin grau de coneixement tenen aquests professionals sobre la regulació actual, com valoren les mesures existents per protegir la privacitat i quins problemes o limitacions detecten en l'aplicació de la pràctica de la normativa.

Aquest objectiu es important perquè gran part de la regulació analitzada al llarg del treball està pensada per aplicar-se en situacions reals desenvolupades per operadors. Per tant, conèixer la seva experiència permet complementar l'anàlisi jurídica amb una perspectiva més propera a la realitat quotidiana de l'ús dels drons.

Per últim, aquest estudi pretén aportar informació que ajudi a valorar si el marc normatiu actual és percebut com una eina suficient per protegir la privacitat de les persones o si, per contra, els professionals consideren que existeixen mancances. D'aquesta manera, els resultats obtinguts permetran contrastar el contingut de la normativa amb l'experiència de les persones que treballen habitualment amb aquesta tecnologia.

7.2. Metodologia

Per complementar l'anàlisi teòrica desenvolupada en els apartats anteriors, s'ha dut a terme un estudi de caràcter descriptiu basat en un qüestionari en línia dirigit a professionals que utilitzen drons. L'objectiu principal d'aquesta part pràctica és conèixer la seva experiència directa amb aquesta tecnologia, el grau de coneixement de la normativa vigent i la seva percepció sobre els riscos que l'ús dels drons pot comportar per a la privacitat.

El qüestionari es va elaborar mitjançant l'eina Google Forms i es va difondre a través de diferents xarxes de contacte i xarxes socials relacionades amb el sector dels drons. La participació va ser voluntària i anònima, garantint en tot moment la confidencialitat de les dades recollides, i, les respostes obtingudes, es van utilitzar exclusivament amb finalitats acadèmiques.

La mostra està formada per professionals de diferents àmbits en què l'ús dels drons és habitual, com ara la seguretat, les emergències i la protecció civil, la fotografia i el sector audiovisual, etc. Aquesta diversitat de perfils permet obtenir una visió àmplia sobre els usos actuals dels drons i les diferents problemàtiques.

El qüestionari està definit per catorze preguntes, combinant preguntes tancades i preguntes obertes. Les deu primeres preguntes tenen un format tancat i permeten obtenir informació general sobre el perfil professional dels participants, la freqüència amb què utilitzen drons, el seu coneixement de la normativa espanyola, la formació rebuda en matèria de protecció de dades i la seva valoració sobre la claredat i l'eficàcia de la regulació actual.

A més, aquestes preguntes també recullen informació sobre la percepció dels professionals respecte als riscos que els drons poden generar per a la privacitat, els dubtes legals que han pogut experimentar i quins consideren que són els principals reptes normatius associats a aquesta tecnologia.

Les quatre preguntes obertes tenen com a finalitat aprofundir en aspectes que no es poden recollir únicament mitjançant respostes tancades. Concretament, permeten identificar els avantatges que els professionals observen en l'ús dels drons, els riscos que detecten en relació amb la privacitat, les possibles millores que proposen per a la normativa actual i altres experiències o reflexions derivades de la seva pràctica professional. Les preguntes obertes i algunes de les respostes obtingudes es poden consultar a l'annex 1 del treball.

La mostra final està formada per 18 professionals que utilitzen drons en diferents àmbits d'activitat. A més, l'accés a professionals especialitzats en aquest àmbit presenta certes limitacions, especialment en sectors com la seguretat o les emergències, fet que condiciona el nombre de participants.

Malgrat això, la diversitat de perfils inclosos permet obtenir una visió general sobre la percepció dels usuaris professionals respecte a la normativa vigent i els reptes que planteja la protecció de la privacitat.

Finalment, les dades obtingudes s'analitzaran de manera descriptiva mitjançant gràfics i percentatges elaborats a partir de les respostes recollides. Les aportacions qualitatives obtingudes a través de les preguntes obertes es classificaran segons els temes principals que apareguin amb més freqüència.

Aquest qüestionari permetrà comparar la percepció dels professionals amb el marc teòric i normatiu analitzat al llarg del treball i valorar fins a quin punt la regulació actual respon als reptes que planteja l'ús dels drons en relació amb la protecció de la privacitat de les persones.

Cal dir, però, que l'estudi pràctic s'ha desenvolupat a partir d'una mostra reduïda de divuit professionals. Tot i que la diversitat dels sectors representats permet obtenir una visió general sobre la percepció dels usuaris de drons, el nombre de participants no és suficient per extrapolar els resultats al conjunt d'operadors que desenvolupen activitats amb aquesta tecnologia.

En segon lloc, la rapidesa amb què evolucionen els drons i les seves aplicacions fa que part de l'anàlisi normativa pugui quedar desactualitzada en un període curt. La regulació d'aquest àmbit es troba en constant transformació i és probable que en els pròxims anys apareguin nous requisits, tecnologies i mecanismes de control.

També cal tenir present que aquest treball s'ha centrat específicament en l'ús civil dels drons amb finalitats de vigilància, deixant fora altres àmbits d'estudi, com ara els usos militars o tecnologies emergents com la intel·ligència artificial

7.3. Resultats

Es van obtenir 18 respostes de professionals que utilitzen drons en diferents àmbits d'activitat en total. Tot i que es tracta d'una mostra reduïda, la diversitat de perfils professionals representats permet obtenir una visió general sobre la percepció dels usuaris respecte a la normativa vigent i als riscos associats a la privacitat.

7.3.1. Perfil dels participants i coneixement de la normativa

Pel que fa al sector professional, els participants provenen d'àmbits molt diversos. El sector de la fotografia i l'audiovisual és el més representat, amb un 27,8% de les respostes. A continuació, destaquen els professionals de la seguretat, que representen el 16,7%, i els sectors d'emergències i protecció civil i inspecció d'infraestructures, amb un 11,1% cadascun.

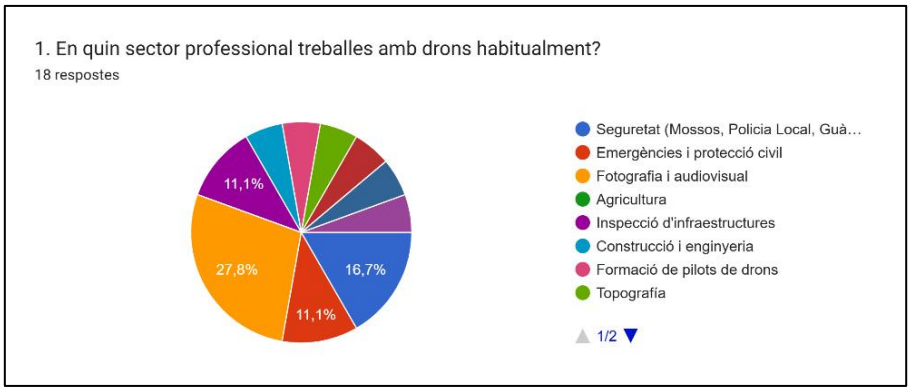


Figura 3. Resultats de la pregunta 1 del qüestionari.

Font: elaboració pròpia

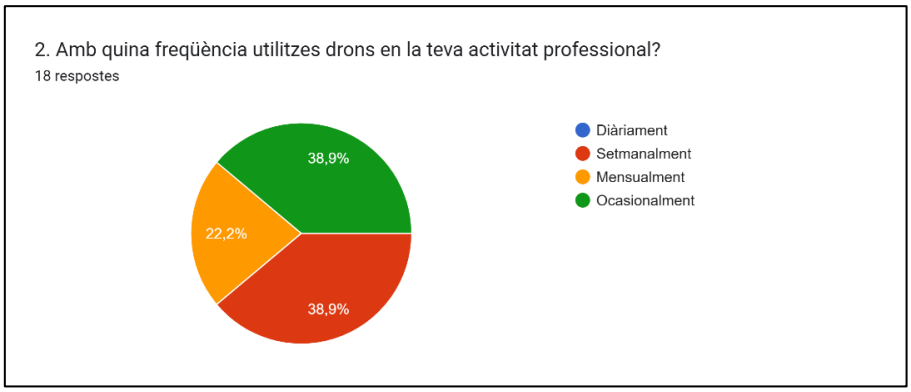


Figura 4. Resultats de la pregunta 2 del qüestionari.

Font: elaboració pròpia

En relació amb la freqüència d'ús dels drons, el 38,9% dels participants afirma utilitzar-los setmanalment, mentre que un altre 38,9% ho fa de manera ocasional. El 22,2% restant utilitza drons mensualment. Cap dels participants indica fer-ne un ús diari.

Aquests resultats mostren que la major part de les persones enquestades tenen un contacte habitual amb els drons dins de la seva activitat professional, fet que aporta valor a les seves opinions.

Pel que fa al coneixement de la normativa espanyola, la meitat dels participants (50%) afirma conèixer-la completament. A més, un 27,8% indica tenir-ne un coneixement general i un 16,7% assegura conèixer-ne només alguns aspectes. Només un 5,6% manifesta no conèixer la normativa.

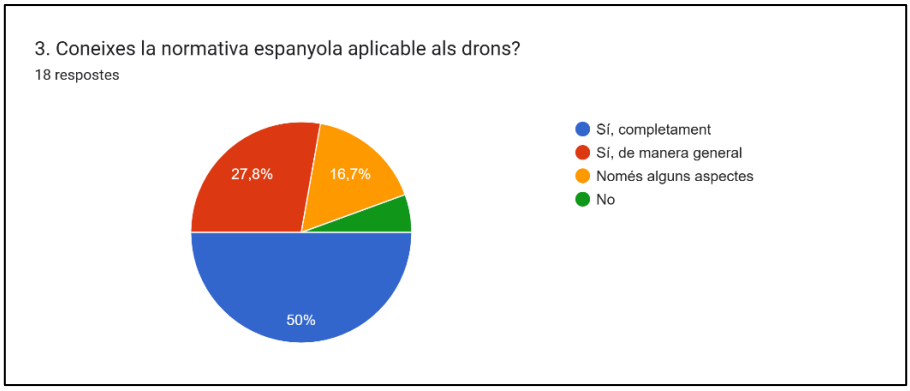


Figura 5. Resultats de la pregunta 3 del qüestionari.

Font: elaboració pròpia

Els resultats suggereixen que la majoria dels professionals enquestats disposen d'un nivell de coneixement elevat sobre la regulació que afecta l'activitat dels drons.

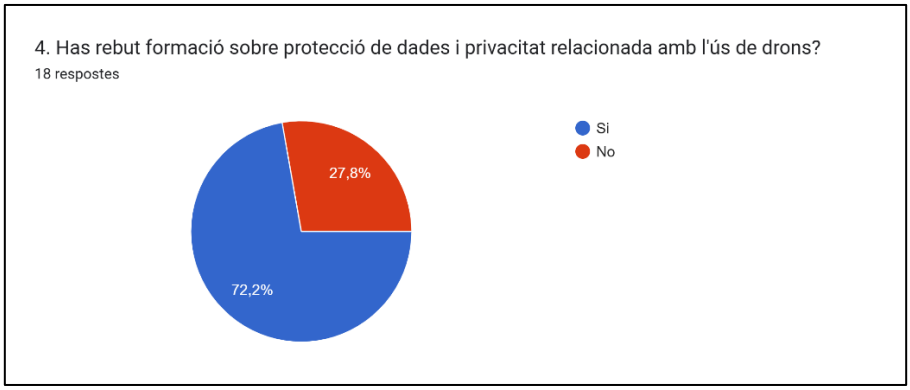


Figura 6. Resultats de la pregunta 4 del qüestionari.

Font: elaboració pròpia

En relació amb la formació específica en protecció de dades i privacitat, el 72,2% dels participants afirma haver-ne rebut, mentre que el 27,8% indica no haver rebut cap formació en aquesta matèria. Això indica, que gran part dels professionals tenen una idea clara de la normativa aplicable.

7.3.2. Percepció sobre la normativa i la privacitat

En quant a la claredat de la normativa actual, el 61,1% dels participants considera que és bastant clara i fàcil d'aplicar. D'altra banda, un 16,7% la considera molt clara, mentre que un altre 16,7% opina que és poc clara. Només un 5,6% considera que la normativa no és gens clara.

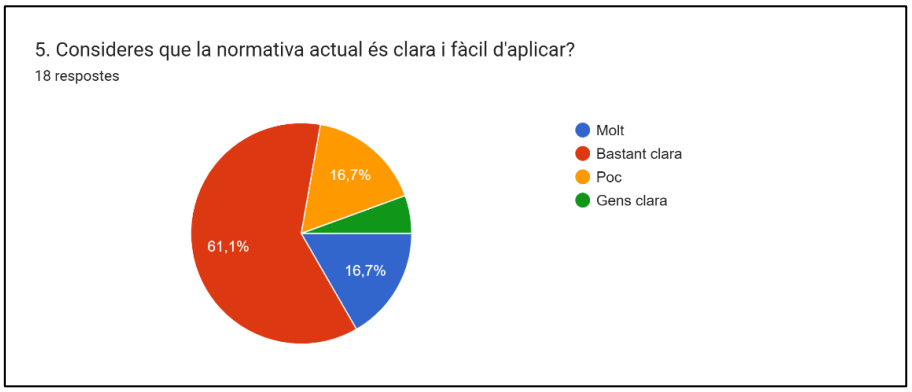


Figura 7. Resultats de la pregunta 5 del qüestionari.

Font: elaboració pròpia

D'acord amb això, l'impacte dels drons sobre la privacitat, la majoria dels participants coincideix a assenyalar que aquest risc depèn principalment de l'ús que es faci de la tecnologia. Concretament, el 66,7% considera que els drons poden afectar la privacitat en funció del context i de la finalitat de l'operació, mentre que el 22,2% opina que l'afectació és clara i directa. Només un 5,6% afirma que els drons no afecten la privacitat i un altre 5,6% manifesta no tenir una opinió definida.

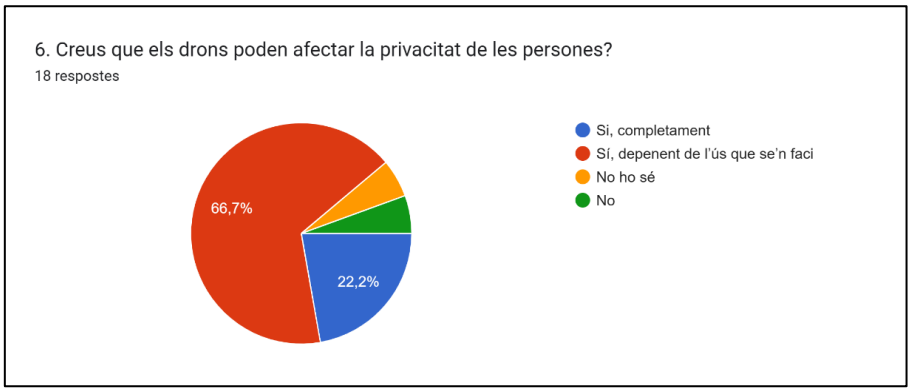


Figura 8. Resultats de la pregunta 6 del qüestionari.

Font: elaboració pròpia

Respecte a la capacitat de la normativa actual per protegir la privacitat, el 38,9% dels participants considera que la protegeix bastant, mentre que el 33,3% opina que la protegeix poc. Per la seva banda, el 22,2% considera que la normativa la protegeix molt i un 5,6% manifesta no saber-ho.

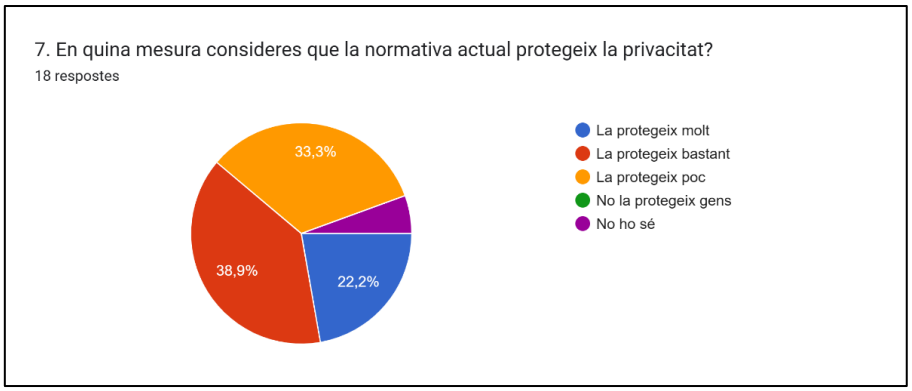


Figura 9. Resultats de la pregunta 7 del qüestionari.

Font: elaboració pròpia

Aquestes dades mostren una percepció generalment positiva sobre la normativa vigent, tot i que una part significativa dels participants considera que encara hi ha marge de millora en la protecció de la privacitat.

7.3.3. Dubtes normatius, reptes legals i riscos associats

En relació amb els dubtes legals o normatius durant les operacions amb drons, la meitat dels participants (50%) afirma haver-ne tingut alguna vegada. A més, un 11,1% assegura experimentar-los sovint i un 27,8% manifesta haver-los tingut molt poques vegades. Només un 11,1% indica no haver tingut mai dubtes relacionats amb la normativa.

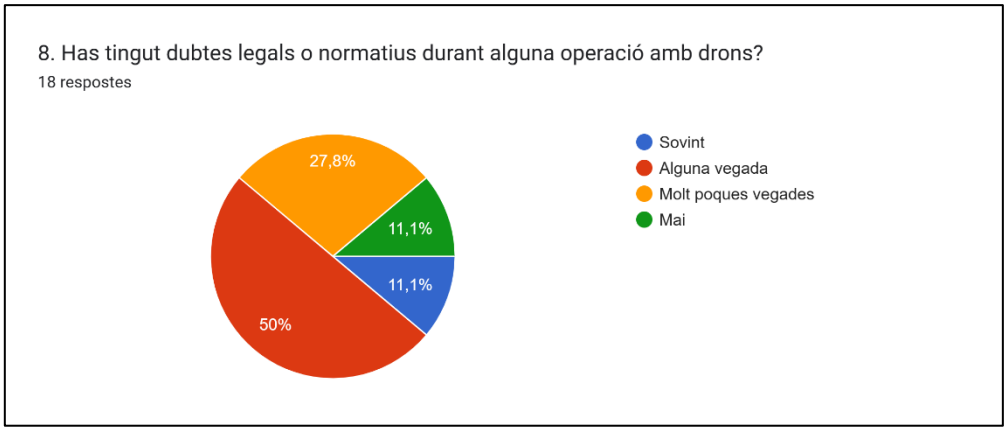


Figura 10. Resultats de la pregunta 8 del qüestionari.

Font: elaboració pròpia

Els principals reptes legals associats a l'ús dels drons, les autoritzacions administratives apareixen com l'aspecte més assenyalat pels participants, amb un 55,6% de les respostes. A continuació, la protecció de dades i la privacitat i les restriccions d'espai aeri són identificades pel 44,4% dels enquestats. En menor mesura, també s'assenyalen el control i la supervisió de les operacions (27,8%) i la formació dels operadors (16,7%).

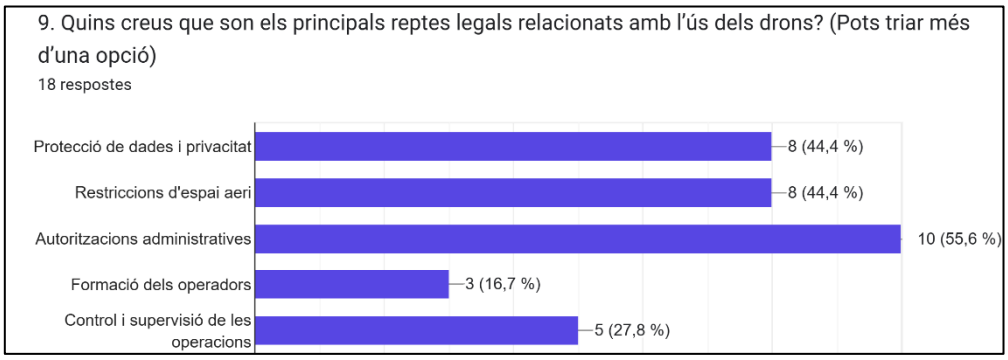


Figura 11. Resultats de la pregunta 9 del qüestionari.

Font: elaboració pròpia

Finalment, el principal risc associat a l'ús dels drons, la manca de control sobre les imatges enregistrades és l'opció més seleccionada, amb un 44,4% de les respostes. A continuació, un 16,7% identifica com a principal risc la vulneració de la privacitat i un altre 16,7% assenyala els riscos per a la seguretat aèria. La captació excessiva de dades personals és indicada per un 11,1% dels participants, mentre que l'ús indegut per part d'operadors i l'ús per part de persones no autoritzades obtenen un 5,6% de les respostes cadascun.

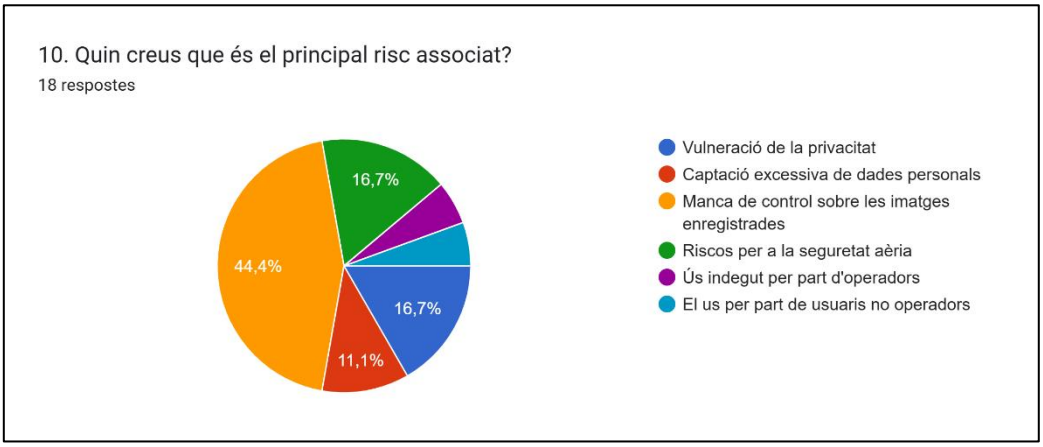


Figura 12. Resultats de la pregunta 10 del qüestionari.

Font: elaboració pròpia

7.3.4. Resultats de les preguntes obertes

Les preguntes obertes han permès veure la percepció dels professionals sobre els avantatges, els riscos i les possibles millores relacionades amb l'ús dels drons. Tot i que les respostes recollides són diverses, s'han identificat diferents temes comuns que ajuden a complementar la informació obtinguda a través de les preguntes tancades.

Pel que fa als **principals avantatges** dels drons en l'àmbit professional, els participants destaquen especialment la seva capacitat per obtenir informació de manera ràpida i eficient, així com la possibilitat d'accedir a espais de difícil accés o de captar imatges des de perspectives que no serien possibles amb altres tecnologies. També assenyalen la versatilitat i la seva utilitat per obtenir imatges i vídeos de gran qualitat.

Alguns participants resumeixen aquests avantatges destacant la ‘’rapidesa i fiabilitat de les dades’’, la ‘’visió general a temps real d'un espai determinat’’ o la possibilitat de captar ‘’imatges i vídeos únics’’. En relació amb això, els drons són percebuts com una eina que millora l'eficiència i amplia les possibilitats d'actuació en diferents sectors professionals.

En **els riscos per a la privacitat**, la majoria de les respostes coincideixen a que la captació ‘’accidental’’ d'imatges de persones sense el seu consentiment com la principal preocupació. Així mateix, diversos participants destaquen la dificultat de controlar l'ús posterior de les imatges enregistrades i la possibilitat que aquestes dades es difonguin de manera inadequada.

Alguns dels comentaris recollits fan referència a la possibilitat de ‘’gravar qualsevol persona’’ o a la ‘’captació accidental d'imatges de persones sense el seu consentiment i la possible difusió inadequada del material enregistrat’’. Tot i això, alguns professionals indiquen que l'impacte sobre la privacitat depèn del tipus d'activitat desenvolupada i que, en determinats contextos, com ara els vols en espais naturals o poc habitats, aquest risc és menor.

En relació als **aspectes de la normativa** que els participants consideren millorables, les respostes es centren principalment en la necessitat de simplificar els procediments administratius, agilitzar les autoritzacions i fer la normativa més clara i accessible. Diversos professionals consideren que els tràmits actuals poden resultar excessivament complexos i que cal una major diferenciació entre els usos professionals i els usos recreatius.

També es posa de manifest la necessitat de reforçar les mesures de formació, especialment en matèria de privacitat i protecció de dades. Alguns participants assenyalen la importància d'adaptar determinats requisits tècnics a la realitat del sector i de revisar aspectes concrets, com ara els límits de pes establerts per a algunes categories de drons.

Finalment, les reflexions aportades pels participants mostren una preocupació compartida per trobar un equilibri entre el desenvolupament tecnològic i la protecció dels drets de les persones.

Diversos professionals consideren que els drons són una eina amb un gran potencial en nombrosos àmbits d'activitat, però insisteixen en la necessitat de disposar d'una regulació clara, àgil i adaptada a l'evolució constant d'aquesta tecnologia. Alguns proposen una major digitalització dels tràmits administratius, una millora de les eines i plataformes d'AESA i una implantació més generalitzada de sistemes d'identificació remota que facilitin el control i la traçabilitat de les operacions. Tal com comenta un dels participants, ‘’els drons són una eina molt útil per al sector audiovisual, però és important combinar la innovació tecnològica amb el respecte a la privacitat i al marc legal vigent’’.

ÀMBIT ANALITZAT	TEMES RECURRENTS IDENTIFICATS
AVANTATGES DELS DRONS	Rapidesa, accés a zones remotes, versatilitat, obtenció de dades en temps real, captació d'imatges des de perspectives úniques
RISCOS PER A LA PRIVACITAT	Captació involuntària d'imatges, enregistrament de persones sense consentiment, difusió inadequada del material, manca de control sobre les dades
ASPECTES NORMATIUS A MILLORAR	Simplificació administrativa, agilització de les autoritzacions, major claredat normativa, diferenciació entre ús recreatiu i professional
REFLEXIONS FINALS	Equilibri entre innovació i privacitat, millora dels sistemes de control, digitalització dels tràmits, evolució constant de la tecnologia

Taula 2. Resultats de les respostes obertes del qüestionari.

Font: elaboració pròpia.

7.4. Discussió dels resultats i limitacions de l'estudi

Els resultats obtinguts permeten contrastar l'anàlisi desenvolupada en els apartats anteriors amb l'experiència de professionals que utilitzen drons en el seu dia a dia. En general, les respostes mostren que els participants tenen un bon coneixement de la normativa, ja que la majoria afirma conèixer-la completament o, com a mínim, de manera general. A més, una part important dels enquestats ha rebut formació específica sobre protecció de dades i privacitat.

Una gran part dels participants reconeix haver tingut dubtes legals durant alguna operació. Aquest fet posa de manifest que conèixer la normativa no sempre implica que sigui fàcil d'aplicar en situacions concretes, encara que la regulació actual estableix unes normes clares, la seva aplicació pràctica pot generar dificultats, especialment en operacions que impliquen la captació d'imatges o el vol en espais amb més restriccions.

Els resultats també mostren que les autoritzacions administratives són percebudes com el principal repte legal relacionat amb l'ús dels drons; destaquen la protecció de dades i les limitacions derivades de l'espai aeri. Aquestes percepcions coincideixen amb el que s'ha exposat al marc teòric, on s'ha vist que la regulació dels drons combina requisits tècnics, operatius i de protecció de dades que poden resultar complexos per als operadors.

Pel que fa a la privacitat, la majoria dels participants considera que els drons poden afectar aquest dret, tot i que el risc depèn principalment de l'ús que se'n faci. Els riscos per a la privacitat no depenen només de la tecnologia, sinó també de la finalitat de l'operació, del context en què es realitza i de les mesures adoptades per l'operador.

La captació accidental d'imatges de persones sense el seu consentiment i la manca de control sobre el material enregistrat apareixen com les principals preocupacions dels professionals. Així mateix, molts participants consideren que la normativa hauria de ser més clara i que els tràmits administratius haurien de ser més àgils.

D'altra banda, els participants valoren positivament l'ús dels drons i destaquen avantatges com la rapidesa en l'obtenció d'informació, la possibilitat d'accedir a espais de difícil accés i la captació d'imatges des de perspectives que altres eines no poden oferir.

Cal tenir en compte, però, que aquest estudi presenta algunes limitacions. La principal és la mida reduïda de la mostra, formada per 18 participants. A més, es tracta d'un sector específic i relativament reduït, fet que dificulta l'accés a un nombre més elevat de professionals, per aquesta raó, els resultats no es poden extrapolar.

8. CONCLUSIONS

8.1. Resolució de la hipòtesi de recerca

La pregunta que ha guiat aquest treball ha estat la següent: és suficient el marc normatiu espanyol per protegir el dret a la privacitat davant l'ús de drons amb finalitats de vigilància en l'àmbit civil?

Després d'analitzar el context actual de la vigilància tecnològica, la regulació aplicable als drons i les percepcions dels professionals que utilitzen aquesta tecnologia, es pot concloure que el marc normatiu espanyol disposa d'un conjunt ampli de normes i garanties destinades a protegir la privacitat, però aquestes mesures no són suficients per assegurar una protecció plenament efectiva en tots els casos.

Per concloure, **la resposta a la pregunta inicial és**, per tant, **negativa.** El problema principal no és l'absència de regulació, ja que existeix un marc jurídic extens format per la normativa aeronàutica europea, el Reial decret 517/2024, el Reglament General de Protecció de Dades, la Llei orgànica 3/2018 i altres disposicions relacionades amb la videovigilància i la protecció dels drets fonamentals.

La dificultat es troba, sobretot, en l'aplicació pràctica d'aquestes normes i en la rapidesa amb què evolucionen les tecnologies de vigilància.

Els drons incorporen característiques que els diferencien d'altres sistemes tradicionals de control, com la mobilitat, la capacitat de captar imatges des de múltiples perspectives i la possibilitat d'operar de manera poc visible. Aquestes particularitats incrementen els riscos per a la privacitat i fan que les garanties jurídiques existents no sempre siguin fàcils de supervisar.

En conseqüència, es pot afirmar que el marc normatiu actual constitueix una base sòlida per regular l'ús dels drons, però encara presenta limitacions importants pel que fa al control efectiu de determinades pràctiques, la claredat d'alguns procediments i la capacitat d'adaptar-se a l'evolució constant de la tecnologia.

Tal com assenyalen diversos autors, la societat actual es caracteritza per una presència cada vegada més gran de sistemes capaços de recollir i tractar informació sobre les persones, sovint de manera poc visible.

L'estudi del marc normatiu ha posat de manifest que la regulació actual prioritza principalment la seguretat operacional i l'organització de l'espai aeri. Tot i que la protecció de dades i la privacitat hi tenen un paper important, aquestes qüestions sovint apareixen com una segona capa de control que depèn de la correcta aplicació del RGPD i de la LOPDGDD.

A més, s'ha observat que la legalitat del vol no implica necessàriament que la captació d'imatges sigui legítima des del punt de vista de la privacitat. Un dron pot operar dins dels límits establerts per AESA i, al mateix temps, generar dubtes sobre la proporcionalitat, la necessitat o la finalitat del tractament de les dades obtingudes.

Els resultats del qüestionari reforcen aquesta idea. Tot i que la majoria dels professionals enquestats considera que la normativa és relativament clara i afirma tenir un bon coneixement de la regulació vigent, una part important reconeix haver tingut dubtes legals durant el desenvolupament de les seves activitats. Aquest fet evidencia que la dificultat normativa continua sent una dificultat real.

Les autoritzacions administratives, les restriccions de l'espai aeri i la protecció de dades apareixen com els principals reptes identificats pels participants. Al mateix temps, la manca de control sobre les imatges enregistrades i la captació accidental de persones sense el seu consentiment són percebudes com els riscos més importants per a la privacitat.

Finalment, les aportacions dels professionals mostren una idea compartida: els drons són eines útils i amb un gran potencial en sectors com les emergències, la seguretat, la inspecció d'infraestructures o l'àmbit audiovisual, però el seu desenvolupament ha d'anar acompanyat d'una regulació clara, accessible i adaptada a la realitat tecnològica actual.

8.2. Propostes i línies futures de recerca

Els resultats obtinguts indiquen la necessitat de continuar avançant cap a un model regulador més flexible i capaç d'adaptar-se als canvis tecnològics.

D'una banda, seria convenient reforçar les accions formatives en matèria de protecció de dades i privacitat, tant per als operadors professionals com per als usuaris recreatius. Igualment, caldria simplificar alguns procediments administratius i millorar les eines per facilitar el compliment de la normativa.

D'altra banda, seria interessant impulsar mecanismes que incrementin la transparència i la traçabilitat de les operacions amb drons, especialment aquelles que impliquen la captació d'imatges en espais públics. La implantació generalitzada de sistemes d'identificació remota o el desenvolupament de protocols més clars sobre la conservació i l'ús de les dades podrien contribuir a reforçar la confiança de la ciutadania.

A més, les noves tecnologies com la intel·ligència artificial, el reconeixement facial o els sistemes de seguiment automatitzat planteja nous reptes que requeriran una revisió específica en els pròxims anys. En definitiva, el repte principal no és decidir si els drons s'han d'utilitzar o no, sinó establir les condicions necessàries perquè el seu desenvolupament sigui compatible amb la protecció dels drets fonamentals. Garantir aquest equilibri serà una de les qüestions clau en la regulació de les tecnologies de vigilància del futur.

9. ANNEXES

Annex 1. Les preguntes obertes i respostes del qüestionari

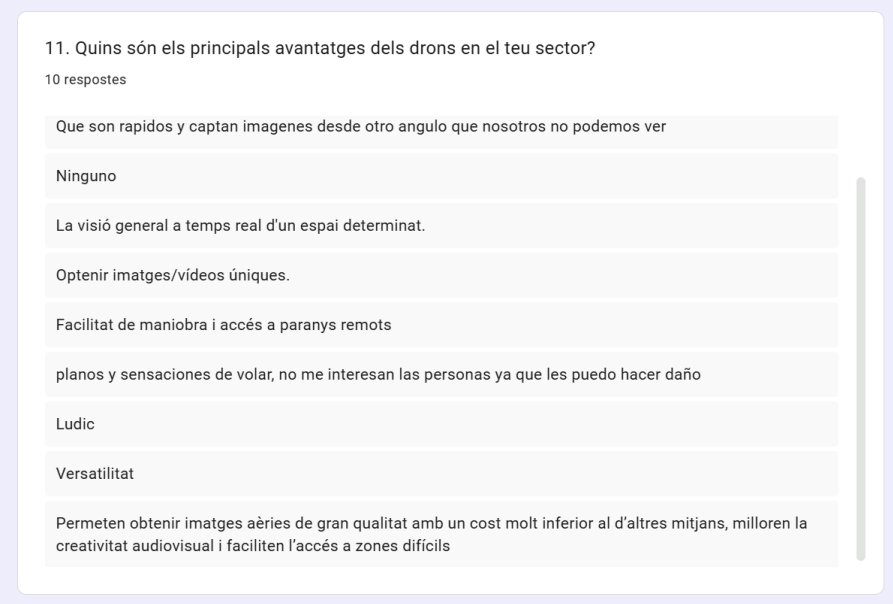


Figura 13. Captura de la pregunta oberta 1 del qüestionari.

Font: elaboració pròpia.

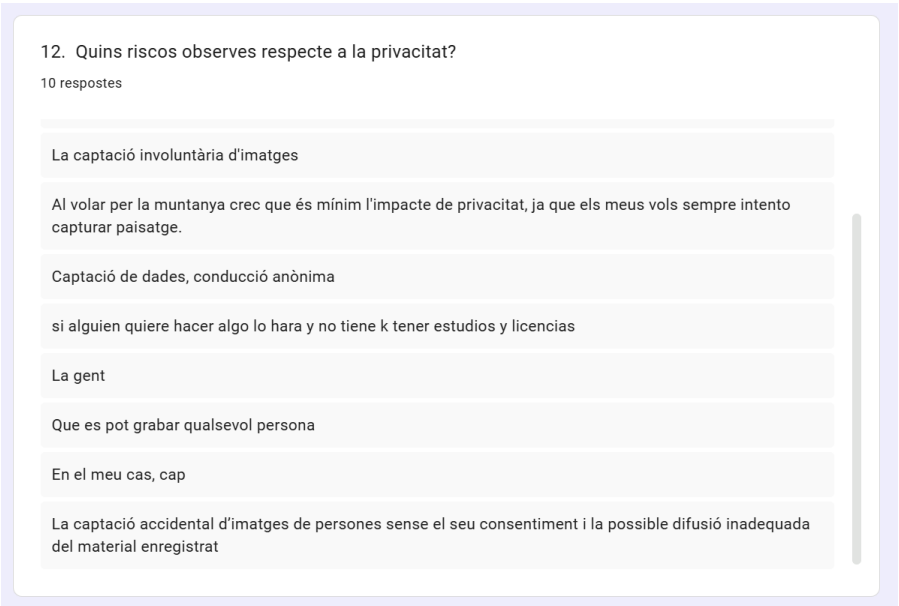


Figura 14. Captura de la pregunta oberta 2 del qüestionari.

Font: elaboració pròpia

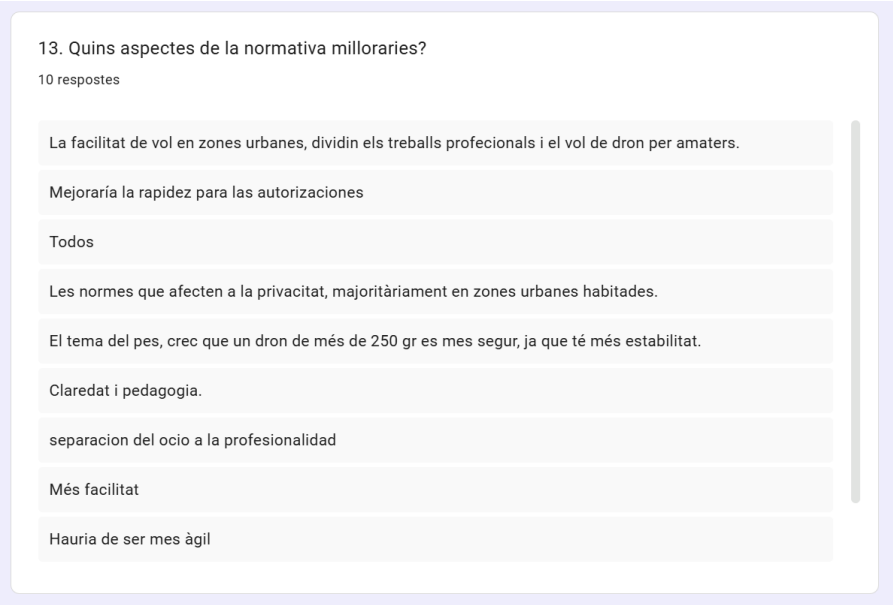


Figura 15. Captura de la pregunta oberta 3 del qüestionari.

Font: elaboració pròpia

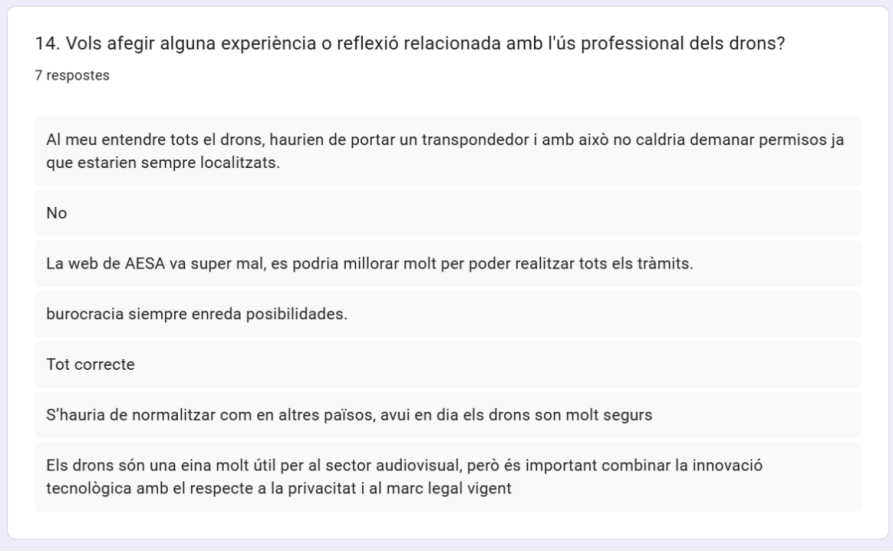


Figura 16. Captura de la pregunta oberta 4 del qüestionari.

Font: elaboració pròpia

10. BIBLIOGRAFIA

Aerocámaras. (s. f.). Clases de drones según la nueva normativa europea. Recuperat de: https://www.aerocamaras.es/clases-de-drones-segun-la-nueva-normativa-europea

Agència Espanyola de Protecció de Dades (AEPD). (2021). Guia sobre videovigilància. Recuperat de: https://www.aepd.es/guias/guia-videovigilancia.pdf

Agència Espanyola de Protecció de Dades (AEPD). (2021). Guía sobre el uso de drones. Recuperat de: https://www.aepd.es/guias/guia-drones.pdf

Agència Espanyola de Protecció de Dades (AEPD). (2021). La protección de datos en las relaciones laborales. Recuperat de: https://www.aepd.es/guias/la-proteccion-de-datos-en-las-relaciones-laborales.pdf

Agència Estatal de Seguretat Aèria (AESA). (2024). Entrada en vigor del nou Reial decret sobre UAS. Recuperat de: https://www.seguridadaerea.gob.es

Agència Estatal de Seguretat Aèria (AESA). (s. f.). Categoria específica d'operacions amb UAS/drones. Recuperat de: https://www.seguridadaerea.gob.es/es/ambitos/drones/operaciones-uas-drones

Agència Estatal de Seguretat Aèria (AESA). (s. f.). Diseño y producción de UAS/drones. Recuperat de: https://www.seguridadaerea.gob.es/es/ambitos/drones/requisitos-de-uas-drones/diseno-y-produccion-de-uas-drones

Agència Estatal de Seguretat Aèria (AESA). (s. f.). Formación de pilotos a distancia de UAS/drones en categoría abierta. Recuperat de: https://www.seguridadaerea.gob.es/es/ambitos/drones/formacion-de-pilotos-a-distancia-de-uas-drones/formacion-de-pilotos-uas-drones-en-categoria-rabiertar

Agència Estatal de Seguretat Aèria (AESA). (s. f.). Normativa oficial sobre drons i UAS. Recuperat de: https://www.seguridadaerea.gob.es/es/ambitos/drones

Agència Estatal de Seguretat Aèria (AESA). (s. f.). Nou marc normatiu dels UAS. Recuperat de: https://www.seguridadaerea.gob.es/es/ambitos/drones

Agència Estatal de Seguretat Aèria (AESA). (s. f.). Operaciones con UAS/drones: categoría abierta (subcategorías A1, A2 y A3). Recuperat de: https://www.seguridadaerea.gob.es/es/ambitos/drones/operaciones-uas-drones/operaciones-con-uas-drones---categoria-abierta-subcategorias-a1-a2-y-a3

Agència Estatal de Seguretat Aèria (AESA). (s. f.). Operacions amb UAS/drones: categoria oberta (subcategories A1, A2 i A3). Recuperat de:

https://www.seguridadaerea.gob.es/es/ambitos/drones/operaciones-uas-drones/operaciones-con-uas-drones---categoria-abierta-subcategorias-a1-a2-y-a3

BOE.es - DOUE-L-2016-80807. Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades, i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades). (s. f.). https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Butlletí Oficial de l'Estat. (1978, 29 desembre). Constitució espanyola. Recuperat de: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

Butlletí Oficial de l'Estat. (1997, 5 agost). Llei orgànica 4/1997, de regulació de la utilització de videocàmeres per les forces i cossos de seguretat en llocs públics. Recuperat de: https://www.boe.es/buscar/act.php?id=BOE-A-1997-17574

Butlletí Oficial de l'Estat. (1999, 16 abril). Reial decret 596/1999, pel qual s'aprova el Reglament de desenvolupament i execució de la Llei orgànica 4/1997. Recuperat de: https://www.boe.es/buscar/doc.php?id=BOE-A-1999-8924

Butlletí Oficial de l'Estat. (2016). DOUE-L-2016-80807. Reglament (UE) 2016/679 del Parlament Europeu i del Consell. Recuperat de: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Butlletí Oficial de l'Estat. (2016). Reglament d'execució (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016. Recuperat de: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Butlletí Oficial de l'Estat. (2018, 6 desembre). Llei orgànica 3/2018, de protecció de dades personals i garantia dels drets digitals. Recuperat de: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Butlletí Oficial de l'Estat. (2024, 4 juny). Reial decret 517/2024, de 4 de juny, pel qual es desenvolupa el règim jurídic per a la utilització civil de sistemes d'aeronaus no tripulades (UAS). Recuperat de: https://www.boe.es/buscar/doc.php?id=BOE-A-2024-11377

Castillero Mimenza, O. (2025, 3 de desembre). La teoria del panòptic de Michel Foucault. Psicología y Mente. https://psicologiaymente.com/social/teoria-panoptico-michel-foucault

Castillero Mimenza, O. (2025, 3 desembre). La teoria del panòptic de Michel Foucault. Psicología y Mente. Recuperat de: https://psicologiaymente.com/social/teoria-panoptico-michel-foucault

Civil Mercantil. (2019, 2 gener). Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales. Recuperat de: https://www.civil-mercantil.com/ley-organica-3-2018-proteccion-datos-personales-derechos-digitales.html

Civil UAVs Initiative. (2020). Plan estratégico de drones. Recuperat de: https://www.civiluavsinitiative.com/wp-content/uploads/2020/02/PlanEstrategicoDrones.pdf

Comitè Europeu de Protecció de Dades (EDPB). (2020). Directrius 3/2019 sobre el tractament de dades personals mitjançant dispositius de vídeo. Recuperat de: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_es.pdf

Departament de Seguretat Nacional. (s. f.). Drones y seguridad nacional. Recuperat de: https://www.dsn.gob.es/sites/default/files/documents/Accesible%20GT%20Drones%20y%20SN.pdf

Directa. (2022). Directa, núm. 552. Recuperat de: https://www.directa.cat/app/uploads/2022/09/Directa-552-1.pdf

Directa. (2022). Drons, càmeres i acció policial sense control. Recuperat de: https://www.directa.cat/drons-cameres-i-accio-policial-sense-control/

Document. (s. f.). Portal Jurídic de Catalunya. https://portaljuridic.gencat.cat/ca/document-de pjur/?documentId=554481#1086935

Drone Guru. (s. f.). Tipos de drones y clases CE en la normativa europea. Recuperat de: https://www.droneguru.es/tipos-de-drones-y-clases-ce-en-la-normativa-europea

Els drets digitals | Observatori de Drets Digitals. (s. f.). https://www.derechosdigitales.gob.es/es/derechos-digitales

Escola d'Administració Pública de Catalunya. (s. f.). La captació i la difusió d'imatges en actes públics: la concurrència del dret a la protecció de dades i del dret a la pròpia imatge. Recuperat de: https://www.formacioooberta.eapc.gencat.cat/espaistematics/gestio-dades/la-captacio-i-la-difusio-dimatges-en-actes-publics-la-concurrencia-del-dret-a-la-proteccio-de-dades-i-del-dret-a-la-propia-imatge.html

EU Drone Port. (s. f.). Diferencias entre categoría abierta y específica de AESA. Recuperat de: https://www.eudroneport.com/es/blog/abierto-y-especifico-de-la-aesa

El Món. (2022). Els Mossos van utilitzar drons en més de 300 serveis durant l'any 2022. Recuperat de: https://www.elmon.cat/societat/policial/mossos-drons-300-serveis-2022-602100

Fundació de l'Energia de la Comunitat de Madrid (FENERCOM). (2015). Los drones y sus aplicaciones a la ingeniería civil. Recuperat de: https://www.fenercom.com/wp-content/uploads/2015/03/Los-Drones-y-sus-Aplicaciones-a-la-Ingenieria-Civil-fenercom-2015.pdf

Govern d'Espanya. Secretaria d'Estat de Digitalització i Intel·ligència Artificial. (s. f.). Carta de drets digitals. Recuperat de: https://www.derechosdigitales.gob.es/es/derechos-digitales

Hovsha, J., & Brien, D. O. (2022). Drone Use Cases and their Privacy Impacts: A Taxonomy. Tilburg Law Review, 27(1), 60-80. https://doi.org/10.5334/tilr.281

Innovaspain. (2025, 30 de setembre). L'impacte de la vigilància en la societat: confiança, control i seguretat. Innovaspain. https://www.innovaspain.com/el-impacto-de-la-vigilancia-en-la-sociedad-confianza-control-y-seguridad/

Innovaspain. (2025, 30 setembre). El impacto de la vigilancia en la sociedad: confianza, control y seguridad. Recuperat de: https://www.innovaspain.com/el-impacto-de-la-vigilancia-en-la-sociedad-confianza-control-y-seguridad/

Institut de Dret Públic de Barcelona. (s. f.). Drons i seguretat pública. Recuperat de: https://www.idpbarcelona.net/ca/drons-i-seguretat-publica

International Organization for Migration. (s. f.). Three challenges for data protection and privacy. Recuperat de: https://weblog.iom.int/three-challenges-data-protection-and-privacy

LAE Consulting. (s. f.). Drones y protección de datos. Recuperat de: https://laeconsulting.net/drones-y-proteccion-de-datos/

La protecció de dades en les relacions laborals. (s. f.). Recuperat el 21 de febrer de 2026, de https://www.aepd.es/guias/la-proteccion-de-datos-en-las-relaciones-laborales.pdf

La societat de la vigilància. (2026, març). https://www.nuevarevista.net/la-sociedad-de-la-vigilancia-el-nuevo-instrumento-de-poder/

Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals. (2019, 2 de gener). Civil Mercantil. https://www.civil-mercantil.com/ley-organica-3-2018-proteccion-datos-personales-derechos-digitales.html

Lyon, D. (1995). El ojo electrónico: El auge de la sociedad de la vigilancia. Recuperat de: https://www.kubernetica.com/campus/documentos/bibliografia/LYON-El-ojo-electronico.pdf

LYON, David (1995). L'ull electrònic. L'auge de la societat de la vigilància. Alianza Editorial. Madrid. Traducció: Jesús Alborés. 322 pàgines. https://www.kubernetica.com/campus/documentos/bibliografia/LYON-El-ojo-electronico.pdf

Nueva Revista. (2026, març). La sociedad de la vigilancia: el nuevo instrumento de poder. Recuperat de: https://www.nuevarevista.net/la-sociedad-de-la-vigilancia-el-nuevo-instrumento-de-poder/

One Air. (2026). Normativa de drons a Espanya el 2026. Recuperat de: https://www.oneair.es/normativa-drones-espana-aesa

One Air. (s. f.). Normativa de drones en España según AESA. Recuperat de: https://www.oneair.es/normativa-drones-espana-aesa

Portal Jurídic de Catalunya. (s. f.). Document. https://portaljuridic.gencat.cat/ca/document-del-pjur/?documentId=554481#108693

Portal Jurídic de Catalunya. (s. f.). Llei orgànica 3/2018, de protecció de dades personals i garantia dels drets digitals. Recuperat de: https://portaljuridic.gencat.cat/ca/document-del-pjur/?documentId=554481#1086935

Reglament (UE) 2016/679 del Parlament Europeu i del Consell. (s. f.). Recuperat el 3 de març de 2026, de https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=es

Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades. (2016). Recuperat de: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=es

Three challenges in data protection and privacy. (s. f.). https://weblog.iom.int/three-challenges-data-protection-and-privacy

Tilburg Law Review. (2022). Privacy and drone regulation: current challenges and future perspectives. Recuperat de: https://tilburglawreview.com/articles/10.5334/tilr.281

UAV Navigation. (2020, desembre). Usos civiles de los UAV. Recuperat de: https://www.uavnavigation.com/sites/default/files/docs/2020-12/usos-civiles-uav-dic-2020.pdf

Universitat de Xile. (2022). Uso de drones en emergencias. Recuperat de: https://www.repositorio.uchile.cl/bitstream/2250/204444/1/uso-de-drones-en-emergencias.pdf