

Videovigilància al sector públic: què cal revisar amb la nova Circular de l'APDCAT



El DOGC de 19 d'octubre de 2026 ha publicat la **Circular 1/2026 de l'Autoritat Catalana de Protecció de Dades** (APDCAT), que deroga i substitueix la Instrucció 1/2009 i actualitza les garanties aplicables als sistemes de videovigilància implantats per les administracions i entitats del sector públic.

Àmbits d'aplicació i entrada en vigor

La Circular 1/2026 de l'Autoritat Catalana de Protecció de Dades (en endavant, la “**Circular**”) és d'obligat compliment per a les **administracions catalanes**, els **ens locals** i les **entitats del sector públic** incloses en el seu àmbit, així com per a determinades entitats privades.

S'aplica al **tractament d'imatges** i, si escau, de veu amb finalitats de **vigilància o control**, mitjançant **càmeres fixes o mòbils, drons i dispositius instal·lats en vehicles o indumentària**, encara que les imatges només es visualitzin en temps real.

La seva entrada en vigor transcorreguts vint (20) dies a comptar des de la seva publicació; això és, el pròxim **8 de novembre de 2026**. La videovigilància per part de les forces i cossos de seguretat es regeix per la normativa específica, amb l'aplicació supletòria de la Circular en els supòsits que aquesta preveu.

La Circular **actualitza la regulació de la videovigilància** i l'adapta al marc normatiu establert pel Reglament (UE) 2016/679, de 27 d'abril de 2016, general de protecció de dades (RGPD), i per la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD).

Justificar el sistema de videovigilància

Abans de posar en marxa el sistema de videovigilància, el responsable del tractament ha de garantir l'elaboració d'una memòria que justifiqui la base jurídica, la finalitat, la necessitat i la proporcionalitat del tractament, i concreti la ubicació de les càmeres, les característiques tècniques del sistema, el període de conservació, el compliment del deure d'informació i les mesures de seguretat. També cal valorar alternatives menys intrusives, documentar la ponderació efectuada i mantenir la memòria a disposició de l'APDCAT.

Quan la videovigilància impliqui una **observació sistemàtica a gran escala d'una zona d'accés públic o pugui comportar un alt risc per als drets i les llibertats** de les persones, cal una **avaluació d'impacte relativa a la protecció de dades (AIPD), que substitueix la memòria.**

El tractament també s'ha d'incloure en el registre d'activitats de tractament de l'entitat responsable, encara que les imatges no s'enregistrin.

Revisar els cartells informatius

Els cartells han de ser visibles abans d'entrar a la zona videovigilada i estar instal·lats abans de captar imatges, fins i tot durant les proves. Cal **identificar el responsable, informar dels drets i facilitar l'accés a la informació completa d'acord amb les obligacions d'informació previstes al RGPD.**

En el cas del tractament pel control laboral, també cal informar prèviament i expressament el personal i, si escau, els seus representants.

En el cas de les càmeres mòbils, incloses les instal·lades en aeronaus no tripulades (drons), vehicles o indumentària de les persones, cal informar de la seva existència mitjançant cartells en els accessos a les zones videovigilades o, si això no és possible, a través d'altres mitjans.

Així mateix, **no cal substituir immediatament tots els cartells existents**. Els que s'ajustin a la Instrucció 1/2009 es poden mantenir fins que calgui substituir-los pel manteniment ordinari. En qualsevol cas, els nous tractaments hauran d'utilitzar el contingut i el disseny de la Circular.

Limitar la captació i la conservació de les dades

Cal ajustar el camp de visió, els horaris i les funcionalitats al que sigui necessari. La captació de la via pública està restringida als supòsits previstos; per vigilar edificis, només se'n permet la captació incidental si és inevitable. La gravació de veu és excepcional i requereix una justificació específica.

Les gravacions s'han de suprimir quan deixin de ser necessàries i, com a màxim, en un mes, llevat de les excepcions previstes. Si es conserven per acreditar actes contra la integritat de persones, béns o instal·lacions, s'han de posar a disposició de les autoritats competents en un màxim de 72 hores des que se'n tingui constància.

Reforçar la seguretat i revisar els proveïdors

La Circular **concreta mesures** com els perfils d'accés autoritzats, el registre d'accessos a les imatges conservades, el xifrat, la protecció dels equips, la formació del personal i les revisions periòdiques. Els responsables inclosos en l'article **77 de la LOPDGGD** han de tenir en compte l'**Esquema Nacional de Seguretat** a l'hora de determinar les mesures de seguretat aplicables.

Si un proveïdor accedeix a les imatges per compte de l'entitat, cal formalitzar un contracte de tractament de dades i incorporar-hi les previsions exigides per la normativa de contractació pública. Això inclou les empreses de seguretat privada que accedeixin a les imatges del sistema.

Atendre els drets i valorar les funcions d'IA

Cal disposar d'un **procediment per atendre els drets, protegir les imatges** de tercers mitjançant **anonimització** quan correspongui i **preservar les gravacions necessàries** per resoldre determinades sol·licituds. L'obligació de respondre existeix encara que les imatges no s'hagin gravat o ja s'hagin suprimit.

Si **el sistema incorpora intel·ligència artificial**, també s'ha de complir el Reglament (UE) 2024/1689, de 13 de juny de 2024, pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial.

La Circular remet expressament a les pràctiques prohibides i a les garanties aplicables als sistemes d'identificació biomètrica remota, tant en temps real en espais d'accés públic com en diferit. El reconeixement facial destinat a identificar unívocament persones constitueix un tractament de dades biomètriques i requereix, a més d'una base jurídica, que concorri una de les excepcions de l'article 9.2 del RGPD.

Properes accions

A partir d'ara, les administracions i entitats del sector públic **hauran de revisar els seus sistemes de videovigilància** per comprovar que s'ajusten a la nova Circular. **En particular:**

- Inventariar els sistemes existents, incloses les càmeres que només permeten visualitzar imatges en temps real, i identificar-ne la finalitat, la ubicació, el camp de visió i les funcionalitats a fi de tenir un control sobre les mateixes i adoptar les accions necessàries.
- Revisar o elaborar la memòria del sistema i determinar si, per les característiques del tractament, és necessària una avaluació d'impacte en protecció de dades, que substituïria la memòria.
- Actualitzar el registre d'activitats de tractament, encara que les imatges no s'enregistrin.
- Comprovar els cartells i la informació facilitada a la ciutadania i, si escau, al personal de l'entitat. Els cartells existents conformes a la Instrucció 1/2009 es poden mantenir fins que s'hagin de substituir pel seu manteniment ordinari.
- Revisar els terminis de conservació, els perfils i registres d'accés, les mesures de seguretat i el procediment per atendre els drets de les persones afectades.
- Revisar els contractes amb empreses de seguretat, instal·ladors i altres proveïdors que puguin accedir a les imatges, incloent-hi les exigències derivades de la normativa de contractació pública.
- Analitzar específicament qualsevol funcionalitat d'àudio, reconeixement facial o intel·ligència artificial abans d'implantar-la o activar-la.

Des de Durán-Sindreu podem acompanyar les entitats en aquesta revisió així com, en elaborar i revisar els procediments interns i contractes per donar compliment a la Circular.

Contacte



Carme Setó

Sòcia | Dret Digital, IT i
protecció de dades
cseto@duransindreu.com
93 602 52 22



Núria Galera

Advocada | Dret Digital, IT
i protecció de dades
ngalera@duransindreu.com
93 602 52 22



Iván Roda

Advocat | Dret Digital, IT
i protecció de dades
iroda@duransindreu.com
93 602 52 22



Bàrbara Boguñá

Advocada | Dret Digital, IT i
protecció de dades
bboguena@duransindreu.com
93 602 52 22