

NOTA INFORMATIVA SOBRE ELS REQUISITS APLICABLES ALS SISTEMES DE VIDEOVIGILÀNCIA

1. Objecte

Aquesta nota té per objecte exposar, amb caràcter general, els principals requisits que han de complir les persones físiques o jurídiques, públiques o privades, que pretenguin instal·lar i utilitzar un sistema de videovigilància (fix o mòbil) al Principat d'Andorra.

La captació d'imatges de persones identificades o identificables constitueix un tractament de dades personals i, en conseqüència, queda sotmesa a la normativa de protecció de dades personals i a la regulació específica en matèria de seguretat pública i videovigilància.

El marc normatiu principal està constituït per:

- La Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals —d'ara endavant, LQPD—.
- El Reglament d'aplicació de l'LQPD, aprovat pel Decret 391/2022, del 28 de setembre.
- La Llei 30/2018, del 6 de desembre, qualificada de seguretat pública.
- El Reglament del 9 de desembre del 2020, relatiu a la instal·lació de sistemes de videovigilància.

2. Determinació de la finalitat i de la base jurídica

Abans d'instal·lar el sistema, el responsable del tractament ha de determinar de manera clara, concreta i documentada:

- La finalitat perseguida.
- La necessitat d'instal·lar les càmeres.
- La base jurídica que legitima el tractament.
- L'àmbit físic que serà objecte de captació.
- Les persones que podran accedir a les imatges.
- El termini de conservació.
- Les mesures de seguretat aplicables.

La videovigilància únicament es pot utilitzar per a finalitats legítimes, determinades i explícites, principalment la protecció de les persones, els béns, els edificis, les instal·lacions i els seus accessos.

En el cas de les entitats privades, la base legitimadora habitual pot ser l'interès legítim del responsable en la protecció de les persones i els béns, sempre que aquest interès no quedi superat pels drets i les llibertats de les persones afectades. Les administracions públiques han de fonamentar el tractament en el compliment d'una obligació legal, l'exercici de poders públics o una missió d'interès públic. El consentiment no constitueix, amb caràcter general, la base jurídica adequada per justificar un sistema ordinari de videovigilància. Article 6 de l'LQPD.

3. Necessitat, idoneïtat i proporcionalitat

La instal·lació ha de respectar els principis de necessitat, idoneïtat, proporcionalitat, minimització de dades i intervenció mínima.

Això implica que:

- El sistema només s'ha d'instal·lar si la finalitat no es pot assolir raonablement mitjançant mesures menys intrusives.
- El nombre de càmeres ha de ser el mínim imprescindible.
- L'angle de visió s'ha de limitar a les zones que sigui estrictament necessari protegir.
- S'han d'utilitzar, quan sigui possible, màscares de privacitat o altres mecanismes que impedeixin captar zones alienes a la finalitat.
- No s'han de captar habitatges, accessos a domicilis o altres espais privats de terceres persones.
- No s'han d'instal·lar càmeres en lavabos, vestidors, zones de descans o altres espais en què existeixi una expectativa reforçada d'intimitat.
- No es poden utilitzar les imatges per a finalitats diferents de les que van justificar la instal·lació.

Les càmeres privades no poden captar la via pública o els espais públics, llevat que aquesta captació sigui estrictament necessària, limitada a la franja mínima imprescindible, proporcionada al risc existent i disposi de l'autorització corresponent. Articles 20 i 23 de la Llei Qualificada de Seguretat pública.

4. Autorització o comunicació prèvia davant del ministeri competent en matèria d'interior

Abans de posar el sistema en funcionament s'ha de determinar el règim administratiu aplicable:

a) Autorització prèvia

Requereixen autorització prèvia del ministre competent en matèria d'interior els sistemes, públics o privats, que captin imatges o sons:

- De la via pública.
- D'espais públics.
- D'espais oberts al públic.

En aquests casos, la sol·licitud ha d'anar acompanyada d'una memòria explicativa que inclogui, entre altres elements, la justificació i la finalitat del sistema, el plànol amb el camp de visió de cada càmera, les característiques tècniques, la necessitat eventual de captar sons, les persones encarregades de l'exploració i les mesures de seguretat.

L'autorització requereix l'informe previ i vinculant de la Comissió Nacional de Videovigilància. Té una durada màxima de cinc anys i s'ha de renovar abans del seu venciment.

b) Comunicació prèvia

Els sistemes privats que no captin imatges o sons de la via pública, d'espais públics o d'espais oberts al públic s'han de comunicar prèviament al ministre competent en matèria d'interior.

La comunicació també ha d'identificar el titular, la finalitat, les càmeres, els espais captats, les característiques tècniques, les persones autoritzades i les mesures de seguretat.

Qualsevol modificació substancial del sistema —incorporació o reubicació de càmeres, ampliació del camp de visió, activació de l'àudio, canvi de finalitat o modificació rellevant de les condicions d'ús— s'ha de comunicar o sotmetre a una nova autorització, segons correspongui. El tràmit es pot efectuar mitjançant la Seu electrònica de Govern.

5. Deure d'informació

Les persones que puguin accedir a la zona vigilada han de ser informades abans d'entrar en el camp de captació de les càmeres.

A aquest efecte, s'ha de col·locar un cartell informatiu clar, visible i llegible en cadascun dels accessos principals. El cartell ha d'indicar, com a mínim:

- L'existència del sistema de videovigilància.
- La identitat del responsable del tractament.
- La finalitat del tractament.
- La base jurídica.
- Els destinataris o les possibles comunicacions de les imatges.
- L'adreça o el mitjà per exercir els drets i la possibilitat de interposar reclamació davant l'APDA.
- El lloc on es pot consultar la informació completa sobre el tractament.

El cartell constitueix una primera capa informativa. El responsable també ha de posar a disposició de les persones interessades una segona capa amb tota la informació exigida per l'LQPD, en paper, en una pàgina web o mitjançant un codi QR. L'APDA disposa d'un model de cartell de videovigilància.

6. Captació de sons

La captació d'àudio comporta una ingerència més intensa en la intimitat que la captació exclusiva d'imatges. Per aquest motiu, la gravació de sons ha d'estar desactivada per defecte.

Només es pot activar quan sigui estrictament indispensable per a la finalitat perseguida, no existeixi una alternativa menys intrusiva i la mesura resulti necessària i proporcionada. Aquesta circumstància s'ha de justificar expressament en la sol·licitud d'autorització o en la comunicació prèvia i ha de quedar reflectida en l'anàlisi de riscos i en la informació facilitada a les persones afectades.

No es poden captar converses privades ni utilitzar el sistema per observar la intimitat de les persones, excepte en els supòsits expressament emparats per la normativa.

7. Termini de conservació

Les gravacions s'han de suprimir en el termini màxim d'un mes des de la captació.

Només es poden conservar durant un termini superior quan les imatges estiguin relacionades amb:

- La possible comissió d'un delicte.
- Una infracció administrativa en matèria d'ordre públic.
- Una investigació policial en curs.
- Un procediment judicial o administratiu que no hagi estat arxivat definitivament.

En aquests casos, les imatges necessàries s'han d'extreure, bloquejar i conservar separatament, amb accés restringit, per posar-les a disposició de l'autoritat competent. La resta de les gravacions ha de continuar sotmesa a la supressió automàtica. Article 24 de la Llei qualificada de seguretat pública.

8. Accés, extracció i comunicació de les imatges

L'accés ha de quedar limitat a les persones expressament autoritzades que necessitin consultar les imatges per raó de les seves funcions.

El responsable ha d'establir un protocol que reguli:

- Les persones i els perfils autoritzats.

- Els supòsits en què es poden consultar les imatges.
- El procediment d'extracció i de còpia.
- El registre dels accessos i de les operacions efectuades.
- La comunicació a les autoritats judicials o policials.
- La conservació excepcional de les gravacions.
- La destrucció segura de les còpies.
- El deure de confidencialitat.

Les imatges no s'han de mostrar, enviar o facilitar a terceres persones, ni difondre's per correu electrònic, missatgeria o xarxes socials, fora dels supòsits legalment previstos. Les còpies només s'han de generar quan siguin necessàries per investigar o acreditar una infracció o per atendre un requeriment de l'autoritat competent.

9. Mesures de seguretat

El sistema ha de disposar de mesures tècniques i organitzatives adequades al risc, com ara:

- Credencials individuals i contrasenyes robustes.
- Eliminació de les contrasenyes predeterminades dels dispositius.
- Perfils d'accés diferenciats.
- Registre i revisió dels accessos.
- Xifratge de les comunicacions i, quan sigui procedent, dels enregistraments.
- Actualització periòdica del programari i del firmware.
- Segmentació o protecció adequada de la xarxa.
- Restricció de l'accés remot.
- Protecció física dels gravadors i equips.
- Esborrament automàtic un cop transcorregut el termini de conservació.
- Verificació periòdica de l'orientació i del camp de visió de les càmeres.
- Procediments de gestió d'incidents i de violacions de seguretat.
- Auditories o revisions periòdiques del sistema.

Aquestes mesures han de garantir la confidencialitat, integritat, disponibilitat i resiliència dels sistemes, d'acord amb l'article 35 de l'LQPD.

10. Registre d'activitats i anàlisi de riscos

El tractament de videovigilància s'ha d'incorporar al Registre d'activitats de tractament del responsable. La fitxa corresponent ha d'incloure, com a mínim, la finalitat, la base jurídica, les categories de persones i dades, els destinataris, el termini de conservació, les transferències internacionals eventuais i una descripció de les mesures de seguretat.

Abans de posar el sistema en funcionament, també s'ha de fer una anàlisi de riscos per identificar els possibles efectes sobre els drets i les llibertats de les persones i determinar les mesures necessàries per mitigar-los.

11. Avaluació d'impacte

S'ha de dur a terme una avaluació d'impacte en protecció de dades quan el sistema pugui comportar un risc alt per als drets i les llibertats de les persones. És obligatòria, en particular, quan es produeix una observació sistemàtica a gran escala d'una zona d'accés públic. Article 32 de l'LQPD.

També s'ha de valorar especialment la necessitat d'una avaluació d'impacte quan el sistema:

- Abasta un nombre elevat de persones o una extensió territorial significativa.
- Controla de manera continuada persones treballadores, menors o col·lectius vulnerables.
- Incorpora captació de so.
- Utilitza càmeres intel·ligents o analítica automatitzada.
- Permet el seguiment de moviments o comportaments.
- Utilitza reconeixement facial o altres dades biomètriques.
- Combina les imatges amb altres bases de dades.

Si l'avaluació conclou que persisteix un risc alt que no es pot mitigar adequadament, cal efectuar una consulta prèvia a l'APDA abans d'iniciar el tractament.

12. Proveïdors i encarregats del tractament

Quan una empresa externa pugui accedir a les imatges —per exemple, una empresa de seguretat, manteniment, central receptora o proveïdor d'emmagatzematge al núvol— tindrà la condició d'encarregada del tractament.

La relació s'ha de formalitzar mitjançant un contracte escrit d'encàrrec del tractament que reguli, entre altres qüestions:

- L'objecte i la durada del servei.
- Les instruccions del responsable.

- La confidencialitat.
- Les mesures de seguretat.
- El règim d'accés a les imatges.
- La subcontractació.
- La notificació d'incidents.
- La devolució o destrucció de les dades en finalitzar el servei.
- Les auditories i els mecanismes de control.

Si les imatges o els serveis d'emmagatzematge estan ubicats fora d'Andorra, s'ha d'analitzar també el règim aplicable a les transferències internacionals de dades.

13. Exercici dels drets

El responsable ha de disposar d'un procediment per atendre els drets de les persones interessades, particularment els drets d'accés, supressió, limitació i oposició, quan siguin aplicables.

Quan es demani accés a una gravació, la persona interessada ha d'aportar la informació necessària per localitzar-la. Si en les imatges apareixen tercers persones, s'han d'aplicar tècniques d'emascarament, difuminació o ocultació, o bé facilitar una resposta alternativa que permeti atendre el dret sense perjudicar els drets de tercers.

14. Videovigilància en l'àmbit laboral

Quan les càmeres puguin captar persones treballadores, aquestes han de ser informades prèviament, de manera clara i específica, sobre:

- L'existència i la ubicació general del sistema.
- Les finalitats perseguides.
- La possible utilització de les imatges en l'àmbit laboral o disciplinari.
- El termini de conservació.
- Les persones que poden accedir-hi.
- La forma d'exercir els seus drets.

El sistema no es pot utilitzar per efectuar una vigilància permanent, indiscriminada o desproporcionada de l'activitat laboral, ni per captar espais de descans, vestidors, lavabos o altres zones reservades a la intimitat.

15. Accions de sensibilització i comunicació de l'APDA

Durant el mes de setembre del 2026, l'Agència Andorrana de Protecció de Dades té previst dur a terme una campanya de comunicació a través de les xarxes socials i publicar una infografia específica sobre l'ús dels sistemes de videovigilància.

Aquesta iniciativa respon al fet que la videovigilància és una qüestió cada vegada més recurrent i rellevant, tant per l'augment de la instal·lació d'aquests sistemes com per l'impacte que poden tenir sobre els drets a la intimitat, a la pròpia imatge i a la protecció de les dades personals.

La campanya tindrà com a finalitat sensibilitzar la ciutadania i facilitar als responsables del tractament informació clara i pràctica sobre els requisits aplicables, especialment pel que fa a la necessitat i la proporcionalitat del sistema, els tràmits d'autorització o comunicació prèvia, el deure d'informació, la col·locació dels cartells, el termini de conservació de les imatges, les mesures de seguretat i l'exercici dels drets de les persones afectades.

16. Conclusió

La instal·lació d'un sistema de videovigilància no es limita a la col·locació de les càmeres i del cartell informatiu. Abans de posar-lo en funcionament, el responsable ha de justificar-ne la necessitat i la proporcionalitat, obtenir l'autorització o efectuar la comunicació prèvia davant del ministeri competent en matèria d'interior, determinar la base jurídica, informar adequadament les persones afectades, incorporar el tractament al Registre d'activitats, fer l'anàlisi de riscos i, quan escaigui, una avaluació d'impacte.

Durant el funcionament del sistema, ha de garantir-se que les càmeres s'utilitzen exclusivament per a la finalitat que n'ha justificat la instal·lació, evitant qualsevol ús incompatible o diferent. Així mateix, s'ha de garantir l'accés restringit, la confidencialitat, la supressió automàtica de les imatges en el termini màxim d'un mes, l'atenció dels drets de les persones i la revisió periòdica de la necessitat, la proporcionalitat i les mesures de seguretat del sistema.

Andorra la Vella, 23 de juliol del 2026.

Jèssica Obiols Obiols

Cap de l'APDA