

holding que, sota el nom de “Jocs del Mediterrani”, estava format per INDRA i l'americana Scientific Games.

Aquesta “lumbera” corporativa va dissenyar un joc totalment allunyat de l'atzar, fent 228 combinacions (228€) es guanyaven segur 3.000€, 2.772€ de benefici. Ningú va detectar l'error i la primera setmana del joc van haver 33 guanyadors 99.000€ en premis, molt més del que s'havia recaptat....

Detectat l'error l'Entitat Autònoma de Jocs i Apostes va retirar el joc, perdent així els 99.000€ que van passar a la butxaca dels espavilats i tot el cost de la operació (terminals, software...) i 100.000€ en una campanya de publicitat..

El nom de COMBI es manté actualment com una versió de la 6/49, però desgraciadament l'atzar d'aquesta versió ha estat curosament revisat.

Val a dir que “Jocs del Mediterrani” va ser adjudicatària el 2005 de les loteries de la Generalitat, el contracte era per 8 anys (ara s'acaba) prorrogable uns altres 8 més...□Es van adjudicar les loteries de la Generalitat el 2005 essent consellera d'interior Montserrat Tura i es va promoure el COMBI-3 essent conseller d'interior en Joan Saura... dos noms per a la història.

Una riallada pot fer caure, fins i tot als monstres corporatius, no son infal·libles!! NO SON INVULNERABLES!!



Passejada d'observació del “smart” control social i la videovigilància al barri de Sants



**Sortida des de A l'Ateneu Llibertari de Sants
Carrer Maria Victòria 10 (Metro Plaça de Sants
L5), el dissabte dia 20 de febrer a les 12 hores.
(durada aproximada una mica menys de 2 HORES)**

<http://antimwc.alscarrers.org>

El control social s'estén com una maligna planta enfiladissa al nostra voltant, no és res de nou... des de temps immemorials el nostre entorn, la societat, ens vigila, arxiva dades, ens controla... podem dir que l'inici de la civilització ve lligat a, entre altres coses, al control i a la vigilància. Els veïns xafarders vigilant les nostres anades i tornades, les tietes velles, alguns germans... que delataven (i delaten) als pares i patriarques.... i més enllà el senyor rector de la parròquia, l'alcalde, l'agutzil, els municipals i els mossos tenen els ulls oberts i les orelles tieses... i encara més enllà el director de l'escola, el metge i el farmacèutic tancaven la trama que ens vigilava.

La “quantitat de control” disponible avui en dia multiplica per milers la de fa unes dècades i segurament d'aquí uns pocs anys serà per centenars de milers..

Primer de tot la capacitat de memòria és pràcticament il·limitada en la mida, però també en el temps (mai existeix l'oblit ni la pèrdua involuntària de dades).

Els moderns suports de memòria fan que la mida dels fitxers, la seva durada (conservació) i velocitat d'accés sigui infinitament més gran que la dels arcaïcs arxiu en paper.

Els recursos tecnològics per el control són ara immensos i la seva “immensitat” no deixa de créixer. Des del pare que pot controlar per GPS on es el telèfon del seu fill, fins l'estat (o alguna corporació) que pot revisar les imatges de videovigilància amb un programa de reconeixement facial... vídeo vigilància “intel·ligent”, biometria, computació ubíqua, bigdata, mineria de dades, nanotecnologies diverses...

s'implantarà a tots els automòbils nous uns sistema de geoposicionament obligatori l'e-call que moltes vegades es vincularà a l'assegurança.

AL CARRER:

17.-Telefonia mòbil: permet als operadors i als serveis d'intel·ligència determinar, per triangulació o per el seu GPS, la posició aproximada de l'usuari i activar remotament l'auricular, el micro i la càmera.

18.-Càmeres tèrmiques i sensors acústics: presents en molts espais públics de les ciutats, permeten mesurar el flux de vianants, de ciclistes i els nivells de soroll.

19.-Mobiliari urbà intel·ligent: progressivament es van incorporant sensors a les parades de busos, fanals, papereres... per detectar presència, però també dades estretes dels telèfons mòbils.

20.-Sistemes de Parking: el pagament amb targeta de zones blaves i verdes generen dades sobre els usuaris, recentment s'estan instal·lant sensors a les places d'aparcament per determinar si estan lliures o ocupades...

Als dibuixos de la “ciutat vigilada” podem veure d'altres possibles capturadors d'informació, alguns vigents com els xips de les mascotes o els caixers automàtics i d'altres futuristes (no massa) com els drons d'observació... tampoc apareix cap vianant amb un wearable... (aquest text està basat en el text “anonymise yourself” extret de la web de la empresa experta en seguretat pública “Éticas Research and Consulting”)

EL CAS DE LA LOTERIA QUE SEMPRE TOCAVA

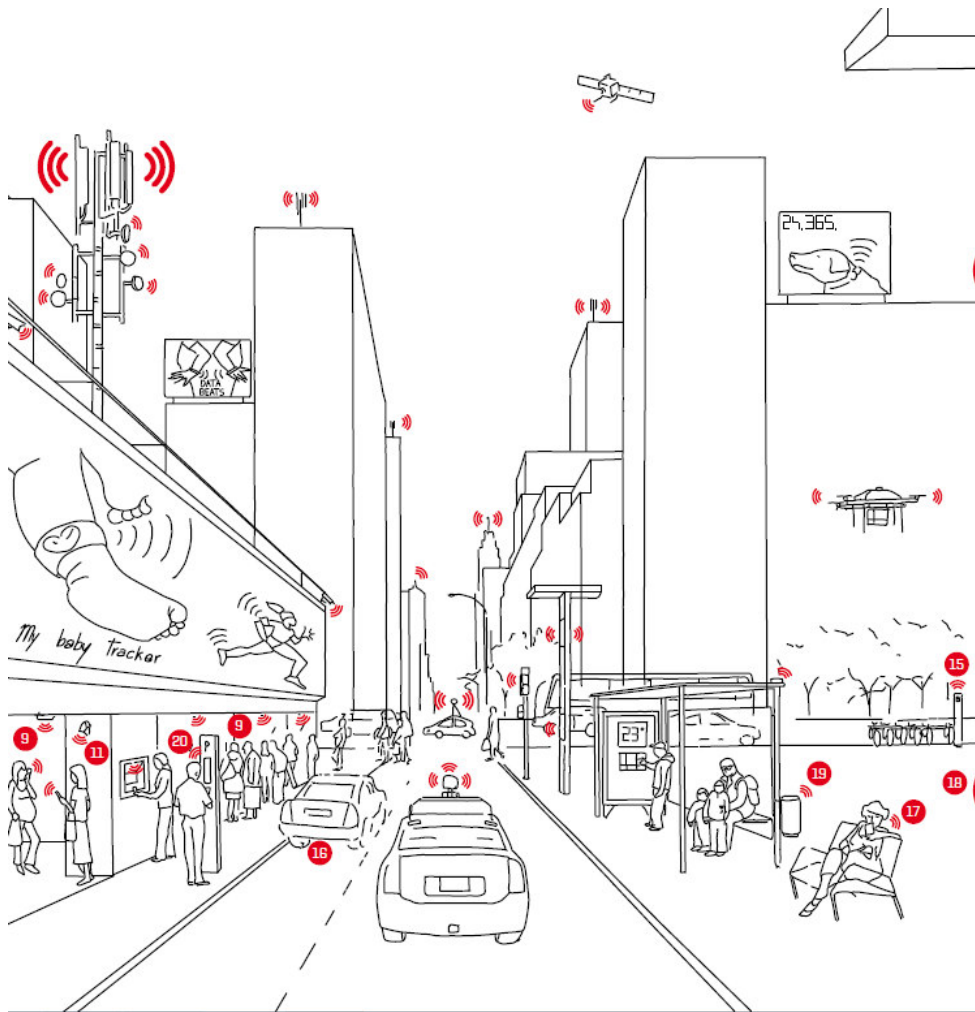
(o l'estupidesa corporativa)

A vegades després de parlar de tot l'entramat estatocorporatiu/tecnològic/dominador podem caure en la depressió i en el derrotisme, són uns gegants imbatibles, uns monstres als que no podem fer front i ens queda una sensació d'impotència,... RES D'AIXÓ.□

Ara mateix, fa uns dies, els Centres de Control de Rodalies i del Metro de Barcelona van fer figa ells solets, el de rodalies gestionat per Telvent (una filial de la multinacional de mesuradors i sensor i smartpuntera Schneider) i el del Metro (linies 9 i 10), encara que no s'ha esbombat massa sembla que INDRA va tenir alguna cosa a veure...

INDRA no sols és coneguda com el principal proveïdor no USA del Cos de Marines i com la principal multinacional tecnològica de matriu espanyola... INDRA també es coneguda per tot un seguit de nyaps i putinades, d'INDRA era el programa del referèndum de la Diagonal, el que governa la línia 9 (els trens es van aturar de cop) ... els riscos de les hipoteques es mesuren en part mitjançant complexos models de software (INDRA n'és un més dels proveïdors) i tots veiem com son de fal·libles...

Segurament el cas més graciós d'ineptitud corporativa va ser el de la loteria COMBI-3 de la Generalitat de Catalunya. La Generalitat volia augmentar la recaptació per joc, per emportant-se un bon tall de la ludopatia catalana. Així que va encarregar un nou joc a un



AL TRANSPORT URBÀ:

13.-Abonaments de transport: les targetes recarregables (especialment les lligades a un compte bancari com T-mobilitat) cada cop més utilitzades produeixen dades sobre els desplaçaments dels seus usuaris.

14.-Videovigilància a las andanes, parades, vagons i vehicles de transport: cada cop més estesa, a alguns vagons hi ha fins i tot 6 petites càmeres.

15.-Xarxes de bicicleta pública: les targetes registren l'horari i l'itinerari de l'usuari.

16.-Automòbils: les matricules poden ser llegides per videocàmeres amb reconeixement, i els teletacs de pagament de peatges permeten reconstruir els itineraris. Properament

SANTS, BARRI SMART?

El Sistema Operatiu de ciutat obtindrà les dades connectant-se al sistema SENTILO (<http://www.sentilo.io/wordpress/>) de gestió de sensors ambientals, aquest sistema ha estat desenvolupat per la ciutat de Barcelona. Està implementada no sols a Barcelona sinó també a Terrassa, en breu a Reus i, segurament s'estendrà per tot Catalunya, (Vilafranca, Igualada, Manresa, Granollers i Mataró integrats al OS-region). També algunes ciutats europees s'han interessat per el sistema... De moment, gestiona sensors de meteorologia, contaminació, omplerta de contenidors, trànsit, places d'aparcament, anàlisi de la xarxa de subministrament de l'enllumenat...

La empresa que ha desenvolupat el Sentilo en partenariat amb Barcelona és Opentrends, especialista en "open source" i "programari lliure". Opentrends ha anat acumulant darrerament contractes amb Barcelona, la majoria lligats a Sentilo, dos concursos de manteniment per un total de 1,5 milions d'euros i ara està a l'espera, és el cavall guanyador, d'un concurs específic per Sentilo de 130.000€. Opentrends forma part de l'aliança TICxCAT "rigorosament de proximitat" i que va ser afavorida amb més de 29 milions en el "concurs del segle" de la Generalitat de 2012 (va ser l'únic adjudicatari local en un pastis de gairebé 2.000 milions). Opentrends va facturar 4,6 milions el 2013 i 6 milions el 2014 hi ha qui diu que serà l'INDRA català.

De tota manera darrera de l'aplicació de Sentilo, a Barcelona està la xarxa de fibra òptica, controlada sobretot per Vodafone i d'altres operadors de telecomunicacions. I, més al darrera, d'una manera que encara no està totalment clara Cisco, que és el principal fabricant mundial d'equipaments per la xarxa (i de l'internet de les coses IoT).

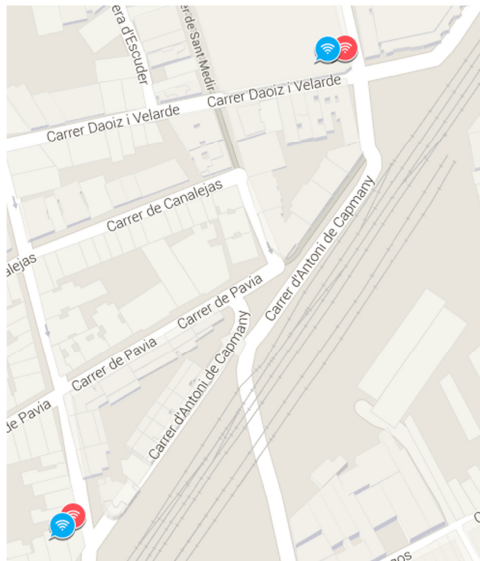
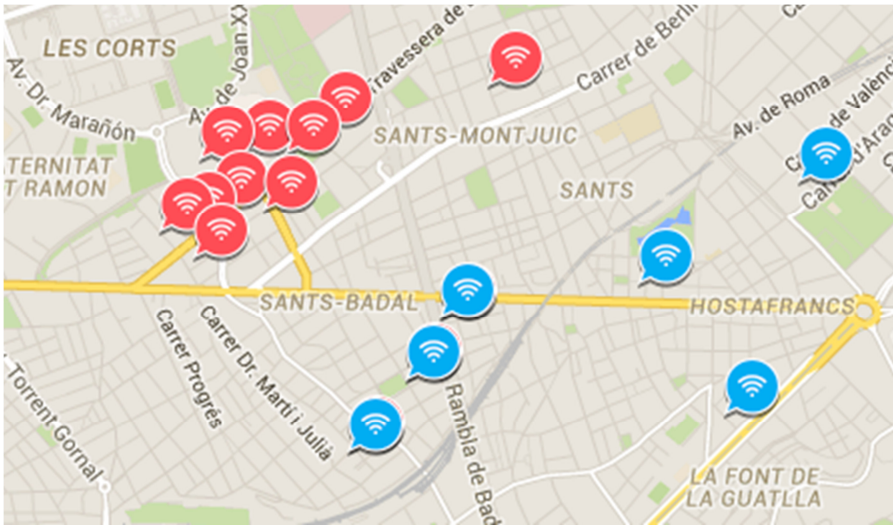
El terme smart s'ha posat, relativament de moda, hi ha smartphones, hi ha smart cars, smart grids i, sobretot hi ha smart city...o sia, telèfons sabiondos, cotxes setciències, xarxes espavilades i ciutats repel·lents... El terme smart city te molts significats diferents segons el punt de vista, sigui del neoliberalisme urbà, o dels progressisme tecnosimple (per exemple bona part del "cyberactivisme"). Però finalment tots acaben en la connexió a la xarxa a través d'artefactes electrònics.

La imatge d'una smart citie és aquella en que tots els serveis i tot l'espai públic (i l'espai privat si no estàs atent!) està connectat... connectat, paraula màgica... connectat a on?... connectat a tot un seguit de bases de dades que en breu (si no es ja un fet) estaran interconnectades per tal de traçar una imatge fidel d'individus, grups i comunitats.

Pot semblar ridícul, però nosaltres mateixos estem farcint aquest monstre a canvi d'uns suposats serveis. Per exemple, a canvi de tenir una factura electrònica dels proveïments energètics i d'aigua de casa nostra, permetem la instal·lació generalitzada de comptadors intel·ligents d'aigua, gas i electricitat, que van prenent dades de consum real cada minut.

Aquests reculls de dades permeten saber moltes coses de la teva vida, per exemple quins son els teus hàbits higiènics (quan et dutxes...) i saber quan estàs a casa, mirant el consum d'energia instantani i fins i tot quan tens descomposició intestinal per un augment del consum d'aigua.

En la smart city cada pas que dona un individu queda registrat. La smart city és el pas previ a generalitzar l'Internet dels Objectes, on cada objecte estarà connectat i l'univers de dades serà global i el nostre entorn serà una xarxa de sensors.



A Sants no està molt desplegada la xarxa Sentilo (<http://connecta.bcn.cat/connecta-catalog-web/component/map>) a la zona sols hi ha sensors de soroll sobretot entre Avinguda de Madrid i Travessera de les Corts. Al centre de Sants, al Nord de la via del tren

A CASA:

1.-Videovigilància domèstica: és un control "voluntari", per exemple per vigilar bebes, la senyal pot ser, sobretot si és IP, piratejada.

2.-Contadors de llum i termòstats intel·ligents: permeten estudiar el comportament quotidià de cada llar (us d'aigua calenta, rentadores, aparells elèctrics...)

3.-Televisor intel·ligent : estan a punt de generalitzar-se els televisors connectats a internet i proveïts de càmera, poden permetre monitoritzar els hàbits de consum i, fins i tot l'ús d'espais comuns.

4.-Consola de videojocs: els darrers models porten incorporada càmera de vídeo i infrarojos a més de la connexió a internet.

A LA FEINA:

5.-Control d'entrades i sortides biomètric: cada cop més estesos, especialment els d'empremta dactilar, són un pas més en el control de la presència.

6.-Videovigilància: es pot utilitzar per reconstruir les activitats dels treballadors, moltes càmeres graven també el so.

7.-Monitorització remota de la pantalla de treball: molts sistemes de control de la productivitat emmagatzemen regularment captures de pantalla dels treballadors per comprovar la seva activitat, també s'utilitza per confirmar presència les càmeres dels ordinadors.

8.-Bases de dades del personal: les empreses recullen nombroses dades sobre el seu personal, especialment si disposen de "millores socials" com és el cas dels xecs menjador...

ALS ESPAIS COMERCIALS:

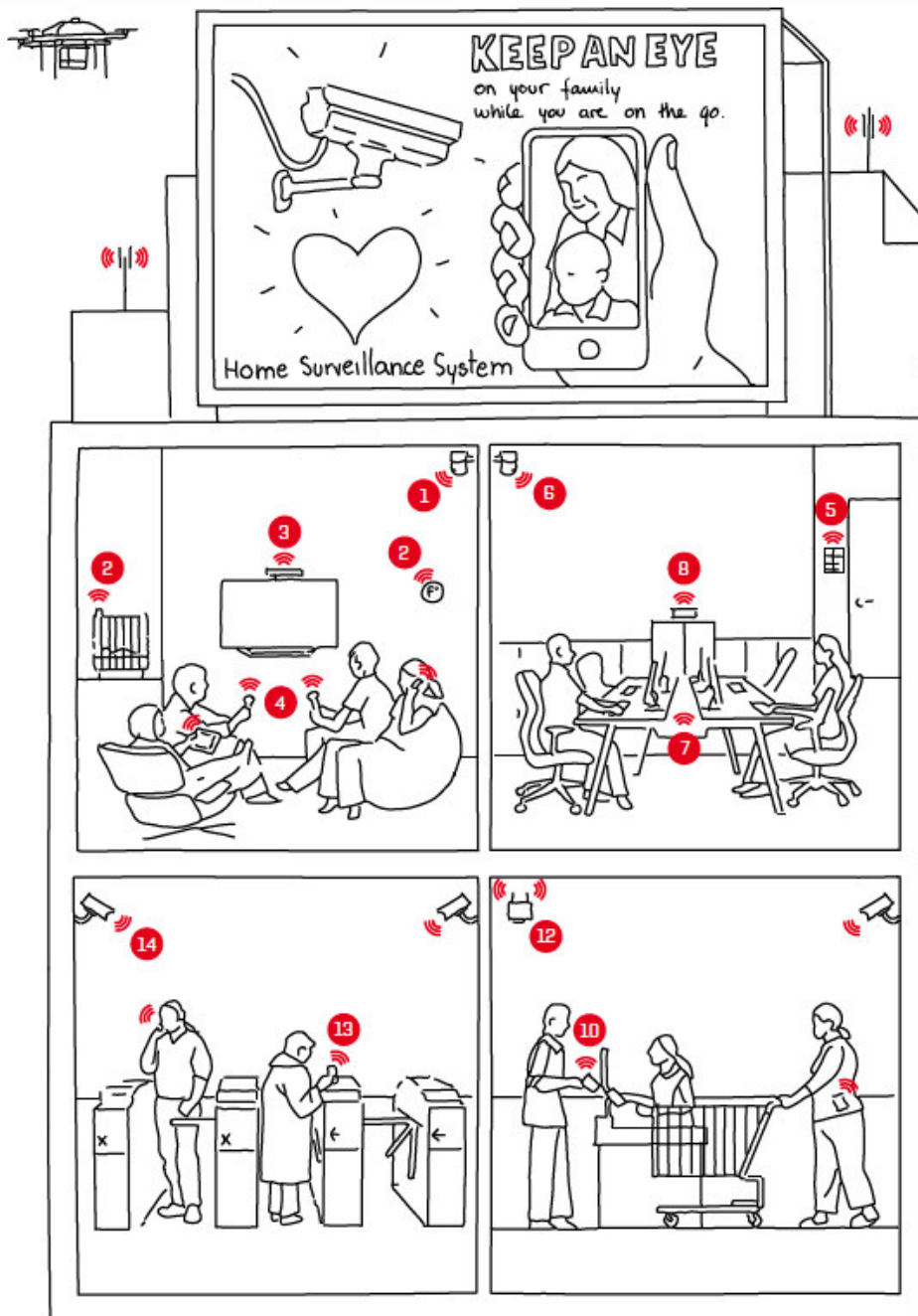
9.-Sensors de recompte de persones: monitoritzen el transit de clients als centres comercials i el temps que està aturat, els és molt útil per l'anàlisi de marketing.

10.-A la caixa: targeta de fidelització: es fa servir per crear un perfil de consumidor, etiquetes RFID, permeten un control del que has comprat fins i tot fora de la botiga.

11.-Ibeacons: apps per enviar anuncis amb novetats i ofertes si s'està a prop del comerç (geoposicionats) pot servir per traçar els moviments a la zona.

12.-Wi-Fi gratuït: a canvi d'oferir servei gratuït molts centres comercials demanen que se'ls facilitin dades.

ESCENES QUOTIDIANES EN UNA CIUTAT SOTA VIGILÀNCIA



(Carrers Antoni Campmany i Daoiz i Velarde més o menys) hi ha sensors de soroll (3) i contaminació atmosfèrica (3), per sobre de carrer de Sants, a la alçada del Parc de l'Espanya Industrial hi ha un sensor de la xarxa d'enllumenat.

MERCAT I MERCADERIA EN ELS CARRERS DE SANTS

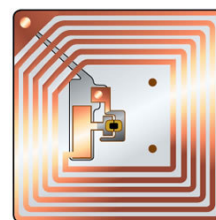
El barri de Sants és una zona comercial de primer ordre, en els nombrosos comerços de modes i d'articles de luxe podem veure a les sortides els clàssics arcs de detecció de furt. Aquest arc detecten el pas de diferents dispositius les VEA (vigilància electrònica d'articles). Hi ha diverses menes de VAE, les etiquetes electromagnètiques, les magnetoacústiques i les RFID.

Les dues primeres permeten detectar el seu pas per un punt determinat, però les terceres contenen informació i la poden transmetre, aquesta particularitat les fa especialment invasives per les persones. Les etiquetes RFID pel fet de facilitar un codi únic, fins i tot les passives de sola lectura, creuades amb d'altres dades poden donar una informació molt important a qualsevol corporació o estat "lector".

A més de com dispositiu antifurt les RFID s'usen també com instrument per fer inventaris més ràpids i per la traçabilitat de mercaderies i màquines... També s'usen per la identificació personal...

RFID (sigles de "**R**adio **F**requency **I**Dentification"), és un sistema d'emmagatzemament i recuperació remota de dades. Contenen antenes per rebre i respondre per radiofreqüència a un lector RFID i un xip on estan gravades les dades.

Les etiquetes poden ser passives, que no necessiten alimentació (la obtenen de l'emissor), són les més barates, però solen tenir menys capacitat d'emmagatzemament i un abast més curt. Les etiquetes actives són les que tenen alimentació pròpia (una petita bateria), són més costoses, més grans però poden emmagatzemar més informació, transmeten millor a una distància més gran. També hi ha semipassives que tenen propietats de les dues. Les etiquetes poden ser només de lectura, poden ser també reescribibles o poden registrar nova informació sense sobreescritura.



Diferents tipus d'etiqueta RFID, flexible, petita i rígida per articles de roba...

Poden ser flexibles o dures, d'un sol ús o reutilitzables, de diferents mides... L'antena pot ser llarga o curta, en poden tenir una o varies... Les etiquetes més petites es situen en els 0,05mmx0,05mm (Hitachi) i poden estar integrades en un full de paper. I cada cop és més viable l'ús de etiquetes RFID unides a sensors (de temperatura, d'humitat, de moviment...).

Malgrat les moltes esperances que els controladors havien dipositat en elles no acabaven de "desplegar", però aquests darrers temps el seu ha anat en augment, degut per una part

a la baixada de preu (més d'un 2% entre el 2000 i el 2014), a la millora tècnica que ha augmentat l'abast i a disminuït els falsos positius.

LA SMART VIDEOVIGILANCIA, LA VIDOVLIGILÀNCIA INTEL·LIGENT.

La omnipresent videovigilància clàssica es va quedar petita per atendre les necessitats del sistema... ja no en tenia prou amb el poc àgil registre simple d'imatges, tan analògiques com digitals. De fet l'afany controlador de l'estat i les corporacions necessita alguna cosa més que la proliferació de càmeres arreu, i guardar imatges per el moment en que les precisin... Necessita saber on anem, per on passem, que fem... i molt més!, vol saber el nostre estat d'ànim, que fem i que portem (literalment) a les mans. La excusa, com passa casi sempre, és la seguretat. Per exemple, el fet de que els atemptats del 11-S a Londres fossin "possibles", demostra, segons el discurs dels ideòlegs i propagadors de la por, que no és suficient la quantitat (es diu, exageradament, que Londres té el 20% de les càmeres de videovigilància del món), sinó la qualitat d'aquests sistemes de control.

Ja no interessa tan el nombre (encara que cada cop en tindrem més) sinó altres coses lligades amb la qualitat de la mirada de l'estat. El control automatitzat sense operador humà, la detecció d'objectes, de situacions i d'actituds i estats d'ànim, el reconeixement d'escenaris... Es tracta d'obtenir sistemes que en temps real detectin objectes abandonats, identifiquin persones, identifiquin els objectes que porten, actituds "sospitoses", els sentiments d'aquestes persones (la por, l'alegria, la tensió, l'enuig...) tot el que permeti prevenir i preveure situacions de "risc" (brots violents, formació de concentracions...). EL MES IMPORTANT ARA ÉS LA PREDICCIÓ DE CONDUCTES I DE POSSIBLES ACCIONS.

Al mateix temps que es busca l'anàlisi en temps real es busca també l'accés ràpid a les enormes llibreries de vídeo que generen els sistemes de vigilància, els medis de comunicació i les xarxes socials. La baixa velocitat d'accés i la necessitat de molta ma d'obra humana (per visionar o per etiquetar escenes) han estat fins ara un dels esculls més importants per l'ús massiu de la informació registrada en vídeo.

Actualment, poder fer la recerca i seguiment d'un sospitós o d'un client en el cas del marketing (el marketing i el control social són germans bessons) a les gravacions de les videocàmeres de un carrer comercial durant un llarg període de temps, o poder escanejar una xarxa social buscant-lo, és una possibilitat massa temptadora perquè qualsevol controlador (poli, governant, estudiosos dels mercats...) pugui defugir-la.

De fet ja hi ha al mercat programes amb aquestes funcionalitats escanejats d'arxius a 150fps (desenes de vegades més ràpid que el convencional) i localitzacions en vases de dades de 500.000 ítems en menys d'un segon emprant mètodes biomètrics per identificar cares, és l'oferta de venda de, per exemple, Heras (filial de la multinacional de la seguretat i de la tecnologia militar EVERIS) o els de la spinoff de la Universitat Autònoma de Barcelona DAVANTIS, (buscant amb els noms de les empreses a youtube es poden visionar vídeos de publicitat sobre els seus productes).

L'Estat Espanyol, especialment a través del seu Ministeri de Defensa, però també per mitjà d'Universitats, gestors d'infraestructures i el sector privat participa en el desenvolupament

Fitxer: Qualsevol conjunt organitzat de dades de caràcter personal que permeti l'accés a les dades d'acord amb uns criteris determinats, sigui quina sigui la forma o modalitat de la creació, l'emmagatzematge, l'organització i l'accés del fitxer.

Il·luminació: mesura de la llum per metre quadrat, la unitat és el lux.

Il·luminació amb infrarojos: il·luminació d'una zona fosca mitjançant la emissió d'espectre infraroig per permetre veure imatges en absència de llum visible.

Persona identificable: Qualsevol persona la identitat de la qual es pugui determinar, directament o indirectament, mitjançant qualsevol informació referida a la seva identitat física, fisiològica, psíquica, econòmica, cultural o social.

PIXEL: un punt en una imatge digital. El punt simple d'un sensor CCD o el més petit punt il·luminós d'un monitor LCD.

Profunditat de camp: àrea de la imatge enfocada per una càmera dins la que una imatge resulta nítida.

PTZ: pan-tilt-zoom, càmeres que poden rotar en els dos eixos, vertical i horitzontal.

Soroll: efecte en pantalla que mostra elements que no són part de la imatge útil, com punts, neu, ondes, ratlles...

Resolució: és una mesura del grau de detall que pot contenir una imatge digital, quant major és la resolució major és també el nivell de detall. La resolució es pot especificar en el nombre de columnes de píxels (ample) o per el nombre de files de píxels (alt), per exemple 320x240. També es pot emprar el nombre total de píxels (generalment en mega).

Sensibilitat: lluminositat necessària (en lux) per obtenir un senyal de vídeo de qualitat estàndard.



De tota manera hi ha una “majoria” social a favor de la videovigilància, els baròmetres d'opinió on s'ha consultat el tema donen al voltant d'un 75% de recolzament i un 10% d'oposició.

Es pot tractar exercir els drets d'accés, rectificació, cancel·lació i oposició davant del titular del fitxer, si se'ns nega es pot denunciar a la AEPD o la ACPD. Però per exercir-los cal facilitar al titular del fitxer una foto teva i la indicació del dia i hora en que creus haver estat gravat... pot ser pitjor cancel·lar que deixar les dades on son!!

També es pot demanar al titular un imprès amb tota la informació (bàsicament la del cartell) que han de tenir a disposició impresa o preimpresa, on s'han de detallar els drets i el nom i adreça del titular del fitxer. Els molesta i pot fer que canviïn alguna activitat.

GLOSSARI DE VIDEOVIGILANCIA

Afectat o interessat: Persona física titular de les dades que són objecte del tractament. La víctima de la gravació.

Àngul de visió: àrea de visió d'una càmera depenent de la lent instal·lada.

Cancel·lació: Procediment en virtut del qual el responsable cessa en l'ús de les dades. La cancel·lació implica el bloqueig de les dades, consistent en la identificació i la reserva d'aquestes amb la finalitat d'impedir-ne el tractament excepte per posar-les a disposició de les administracions públiques, jutges i tribunals, per atendre les possibles responsabilitats nascudes del tractament i només durant el termini de prescripció de les responsabilitats esmentades. Una vegada transcorregut aquest termini, s'han de suprimir les dades.

CCTV: circuit tancat de televisió, sistema de vigilància per visualitzar imatges en “privat”. Les càmeres també han d'estar senyalitzades.

Cessió o comunicació de dades: Tractament de dades que implica revelar-les a una persona diferent de la persona interessada.

Consentiment de la persona interessada: Qualsevol manifestació de voluntat, lliure, inequívoca, específica i informada, mitjançant la qual la persona interessada consent el tractament de dades personals que la concerneixen.

Dades de caràcter personal: Qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus que concerneix persones físiques identificades o identificables.

Definició: capacitat d'una camera, monitor, o videogravador de reproduir fidelment les imatges capturades.

Distància focal: es mesura en mm, està directament relacionada amb l'angle de visió. Una distància focal curta significa un angle de visió ampli i una distància focal llarga una angle petit.

d'aquestes eines. Avaluar les despeses en I+D en aquest sector és complicat, però ens podem fer una idea a través dels projectes de seguretat dels Fons del Programa VII. Espanya participa en, al menys, 14 projectes per un import total de més de 60 milions d'euros, com es pot veure una quantitat important de recursos, i això només en el programa VII, a part hi ha d'altres fons de finançament per indústries, universitats, l'Agència de Defensa Europea, la Europol... i els fons d'investigació dels ministeris militars... en el cas d'Espanya la “Subdirección de Tecnología e Innovación (SDG TECIN) de la Dirección General de Armamento y Material”.

El projecte més publicitat ha estat el INDECT (www.indect-ref_project.eu) de quasi 15 milions (participa la Universidad Carlos III i la empresa APIF Moviquity) el projecte ha estat titllat com a “gran germà” per els defensors de la intimitat a Europa. Un altre projecte important és el projecte SAVASA de xarxes de videovigilància intel·ligents, majoritàriament participat per entitats espanyoles IKUSI, RENFE, DGT..., en total sis de deu participants, el pressupost és de 6,5 milions (www.savasa.eu).

A part dels ministeris de defensa un dels sectors més interessats és el dels transports, especialment ferroviari i aeroports i el control fronterer. De fet les companyies de ferrocarrils deuen ser un dels principals posseïdors de càmeres de videovigilància, i els aeroports segurament els van darrera.

ABAST DE LA VIDEOVIGILANCIA

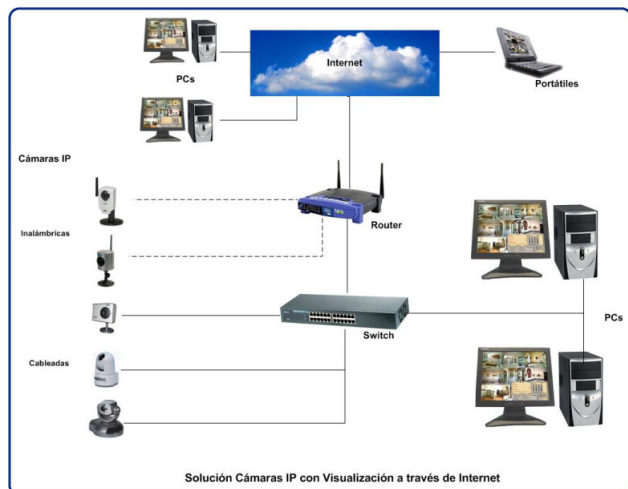
És molt difícil avaluar, ni aproximadament, l'abast de la videovigilància, no hi ha dades fiables i, a més una bona part de les càmeres no estan legalitzades i per tant no consten a les estadístiques. A la memòria de l'Agència Espanyola de Protecció de dades del 2013 (la darrera publicada) tenien registrats 176.317 fitxers (un creixement del 26% respecte a 2012) de videovigilància, dels que sols 2.821 (un 1,6% eren de titularitat pública), la major part d'aquests fitxers corresponen al comerç, amb 41.599 (24%), al turisme i l'hoteleria 20.672 (12%) i a comunitats de propietaris amb 12.831 (7%).

CAMERES IP:

Les càmeres analògiques envien un senyal analògic a un monitor o sistema de gravació, les càmeres digitals envien un senyal digital (poden ser inalambriques), aquestes imatges poden ser tractades digitalment i poden ser enviades o emmagatzemades al núvol. El sistema IP sempre presenta un retard en la visualització que pot ser crucial. El cablejat de les càmeres IP pot ser molt més senzill i a més el senyal pot estar encriptat.

Les càmeres IP obren tot un món nou per el control, especialment pel control “alegal” (per pols diverses, detectius privats i espies aficionats), ja que permet la visualització en temps real i el emmagatzematge, sense cablejat, i la vigilància des de qualsevol lloc, mitjançant qualsevol eina TIC mòbil (portàtil, smartfone o tablet).

Una microcàmera IP, amb connexió wifi i ben dissimulada pot controlar a qualsevol en qualsevol moment, lamentablement aquests darrers temps en tenim uns quant exemples. Les càmeres IP obren tot un món nou per el control, especialment pel control “alegal” (per pols diverses, detectius privats i espies aficionats), ja que permet la visualització en temps real i el emmagatzematge, sense cablejat, i la vigilància des de qualsevol lloc, mitjançant qualsevol eina TIC mòbil (portàtil, smartfone o tablet).



ALGUNS TIPUS DE CAMERES DE VIDEOVIGILANCIA

	Càmeres de xarxa fixes , la direcció i el camp d'observació ve definit per el muntatge.
	Càmeres de xarxa DOMO , són fixes estan dins d'una carcassa en forma de cúpula. Discretes la direcció de la càmera és difícil de determinar.
	Càmeres de xarxa PTZ . Combinen funcions de zoom i de moviment vertical i horitzontal.
	Càmeres de xarxa DOMO PTZ són les més adaptables fins 360° horitzontals i 220° verticals, amb funcions de zoom.
	Càmeres tèrmiques , poden ser de tots els tipus, però solen ser fixes. Creen imatges a partir del calor que emet l'objecte, poden per tant "veure" en la foscor total.

farmàcia aïllada no fa por a ningú... un núvol de càmeres a disposició d'un poder dotat de eines d'anàlisi és de tèmer.

Exteriors	Interiors botiga, banc...	Portal	Videoporter	Càmeres sense cartell	Càmeres apuntant a l'espai públic

QUE FER CONTRA EL VIDEOCONTROL?

El primer és ser conscients i tenir clar els riscos que suposa i que no totes les imatges tenen la resolució i la qualitat per permetre identificacions biomètriques.

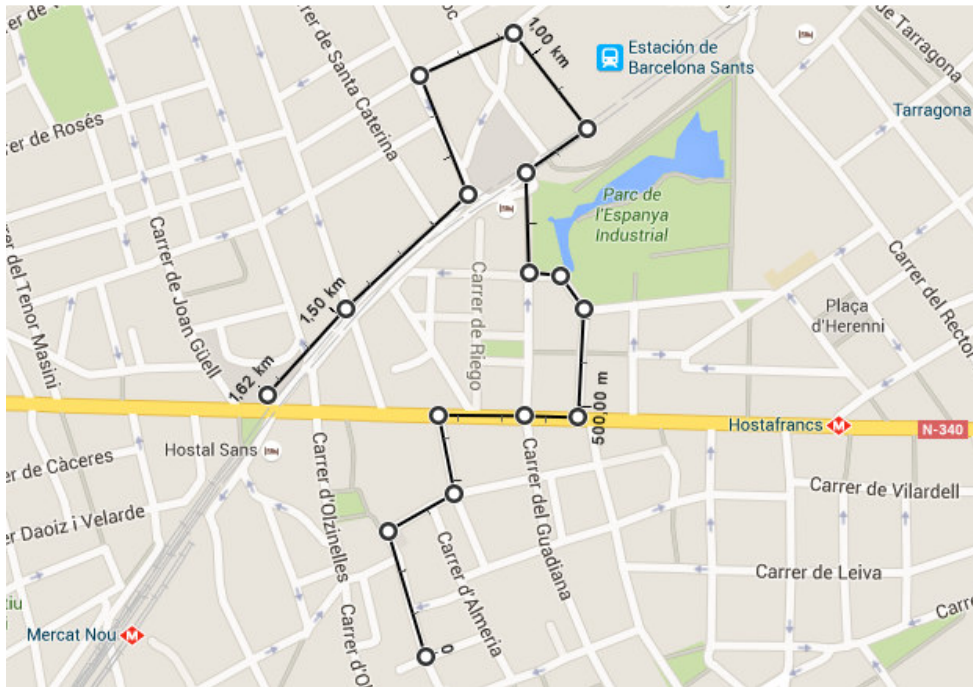
No obsedir-se amb el tema, es pot seguir fent el de sempre, sols s'ha de anar en conte i preveure quan s'entra en el camp de visió d'una càmera.

Actuar contra les càmeres pot ser molt gratificant, encara que la utilitat a mitjà termini no sembla molt alta, al link: http://www.antimilitaristas.org/spip.php?article3240&var_recherche=videovigilancia hi ha una miniguia contra la videovigilància. L'ús de punters làser per enlluernar-les sembla el mètode mes manejable.

Es pot denunciar davant les agències de protecció de dades totes les càmeres que es sospiti que no estan legalitzades o que no compleixen la llei, especialment en el tema de senyalització i d'invasió de l'espai públic. Es pot fer a través de l'Agència Espanyola de Protecció de Dades, AEPD www.agpd.es, en aquesta web, a l'apartat "canal ciudadano" hi ha un formulari electrònic de denúncia. L'Autoritat Catalana de Protecció de Dades, ACPD, també te potestat d'inspecció i sancionadora, no disposen de formulari al seu web... www.apd.cat. De tota manera la via legalista pot ser esgotadora ja que els processos s'allarguen molt en el temps i els resultats al final són decebedors, aconseguint finalment en lloc d'eliminar-les una xarxa de vigilància legal i perfeccionada. Per altra part les proves procedents de càmeres no legals son molt discutibles.

LA PASSEJADA PER SANTS

La passejada comença a la plaça major on hi ha la seu central de l'ajuntament i on celebra el mercat setmanal, fet social molt rellevant, al menys fins fa poc. Com una imatge del que és realment la societat tenim una càmera al costat de la porta principal, aquesta càmera enfoca l'acera de la porxada més o menys davant de la porta i està ben senyalitzada, a qui vigila aquesta càmera?.



Al llarg de la passejada ens fixarem en les diferents càmeres i avisos de càmeres que anem trobant, fa un temps sols en tenien les farmàcies i els bancs, ara fin i tot hi ha videovigilància a forns de pa i basars... TOTES les càmeres han d'estar senyalitzades si no tenen el típic cartellat o un de semblant o son il·legals o estan cometent una infracció.

Moltes de les petites càmeres que hi ha dins dels locals tancats han estat instal·lades per petits proveïdors amb habilitat comercial i no tenen manteniment ni contracte.

Sovint hi ha instal·lades càmeres falses posades amb l'esperança de que per un cost baix (molt baix) tinguin el mateix efecte dissuasiu que una de real, les càmeres falses no han d'estar obligatòriament senyalitzades, això fa que sigui difícil averiguar si una càmera no senyalitzada és il·legal.

Amb el recorregut per Sants volem fer veure el nombre de càmeres. De fet és el conjunt de sistemes i minisistemes de videovigilància el que és asfixiant. Una càmera a la porta d'una

	Videoporter , és una camera més, en principi no te la opció de registrar les imatges, però hi ha referències d'ofertes d'instal·ladors per dotar-les.
	Microcàmera : miniaturitzades, molt sovint funcionen sense fils o wifi, poden estar instal·lades a tota mena de llocs, estan limitades per l'alimentació.
	Amb il·luminació infraroja : poden ser fixes, domo, PTZ... però disposen d'una corona de LED's infrarojos al voltant de l'objectiu que permeten filmar en moments de poca llum
Una alternativa de baix cost a la videovigilància son les càmeres falses, s'instal·la sols la carcassa i tenen un efecte "dissuassori". Moltes vegades estan ben muntades i tenen fins i tot cablejat fals, encara que ara amb les sense fils no calen cables i és difícil saber si realment és una càmera falsa.	

LA LEGISLACIÓ:

La legislació està força dispersa, es poden trobar referències al tema a una pila de lleis, per exemple a la d'acompanyament dels pressupostos de l'estat de 2012, el que segueix és un recull de les més importants.

Llei 23/1992 de 30 de juliol, de Seguretat Privada.

Reial Decret 2364/1994, per el que s'aprova el Reglament de Seguretat Privada.

Llei Orgànica 4/1997, de 4 de agost, on es regula la utilització de videocàmeres per part de les forces i cossos de seguretat a espais públics.

Reial Decret 596/1999 de 16 d'abril en el que s'aprova el reglament de la Llei Orgànica 4/1997.

Llei Orgànica 15/1999, de 13 de desembre de protecció de les dades de caràcter personal (LOPD).

Reial Decret 1720/2007 de 21 de desembre, reglament de desenvolupament de la LOPDP. Instrucció 1/2006, de 8 de novembre, de la "Agencia Española de Protección de Datos", sobre el tractament de dades personals amb finalitat de vigilància a través de sistemes de càmeres o videocàmeres.

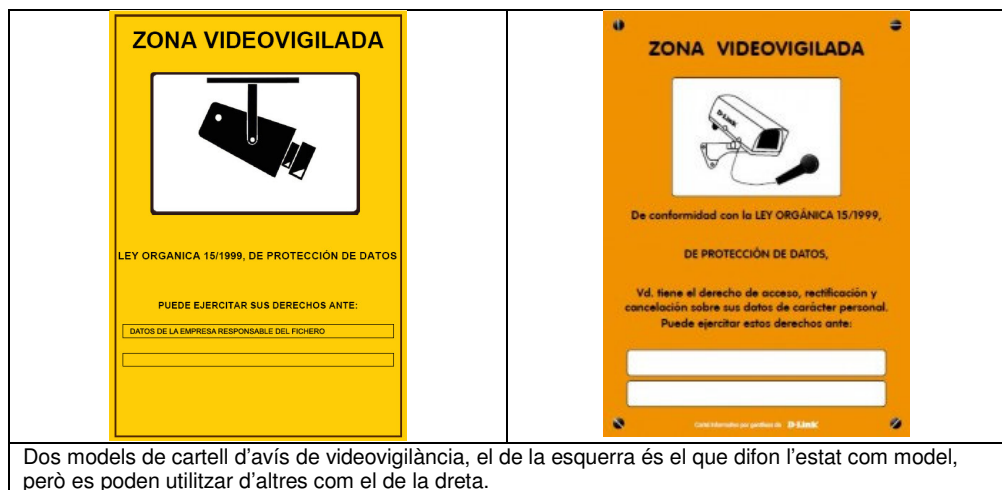
En teoria la legislació espanyola és molt garantista, però en la pràctica deixa en mans dels controladors moltes coses:

Per exemple les càmeres privades no poden gravar l'espai públic, però es posen tantes excepcions ("salvo que sea imposible evitarlo", "salvo que resulte imprescindible") que en la pràctica podem trobar multitud de càmeres privades enregistrant importants zones públiques, per exemple les càmeres instal·lades a les façanes.

És obligatori advertir de la videovigilància de les càmeres fixes, però no de les mòbils. És la “autoritat competent” qui fa la classificació de les infraccions (greus, lleus...) en la protecció del dret a la intimitat, si no es considera “greu” no serà perseguida.

ALGUNES PREGUNTES FREQUENTS SOBRE LA VIDEOVIGILÀNCIA:

S'ha d'informar obligatòriament i sempre de l'enregistrament d'imatges, mitjançant cartell i a més el titular ha de disposar d'un full (o d'un document preparat per ser imprès) a disposició de qui el demani informant de la existència del fitxer, la possibilitat d'exercir els drets i la identitat i adreça del responsable de tractament de les dades. Aquesta obligatorietat no queda clara en el cas de les càmeres mòbils, que en principi sols poden emprar els cossos de seguretat, però en l'avantprojecte de seguretat privada s'inclouen les mòbils dins del marc de la videovigilància privada. Si una zona videovigilada té varis accessos s'ha de posar un cartell a cada un d'ells. Els cartells identifiquen la zona videovigilada, però no han de identificar necessàriament la ubicació de la càmera.



Dos models de cartell d'avís de videovigilància, el de la esquerra és el que difon l'estat com model, però es poden utilitzar d'altres com el de la dreta.

S'haurà de crear un fitxer registrat, segons la LOPD, per totes aquelles dades que continguin informació personal (imatges que puguin identificar persones).

Els afectats poden demanar exercir els drets d'accés, rectificació, cancel·lació i oposició a aquests fitxers, aquest dret haurà de figurar al cartell d'informació de la videovigilància. Es podrà exercir sempre que aquestes accions no suposin perills per la seguretat, per la llibertat d'altres o obstaculitzin investigacions en curs. En el cas de circuits tancats sense enregistrament, no és necessari fitxer ni inscripció, però sí la resta de condicions, particularment la informació.

Les càmeres instal·lades a espais privats no poden obtenir imatges d'espais públics... només les que siguin “imprescindibles” per la vigilància, o sigui impossible

evitar-les per la seva ubicació... en definitiva que casi poden obtenir les que desitgin. Així no es legal videovigilar una terrassa de bar ja que és un espai públic.

Mai es poden gravar imatges en zones protegides pel “dret a la intimitat” banys, vestuaris, gimnasos, interior d'habitatges...

Les imatges es conservaran solament 30 dies... en el cas dels bancs 15 dies, tan sols es superarà aquest termini en el cas d'haver gravat un delictes o per ordre judicial. (veure cancel·lació en el glossari).

La utilització de **càmeres als espais públics** es reserva a les Forces i Cossos de Seguretat (exercit i cossos policials estatals, autonòmics i locals).

En el cas dels entorns escolars, la videovigilància ha de ser mínima, abastar només els espais públics (accessos o passadissos), en cap cas una aula o un espai de joc es pot considerar espai públic.

A les escoles **no s'utilitzarà la videovigilància per controlar l'assistència**.

Als espais docents **caldrà l'autorització** dels titulars de les dades personals (professors i alumnes), i si son menors de 14 anys dels seus pares o representants legals.

Als espais públics d'us privat no es podran gravar conversacions.

Als habitatges i als vestíbuls dels habitatges no es podran prendre imatges ni sons, sols amb el consentiment del titular o autorització judicial.

Als llocs de treball l'Estatut del Treballador autoritza les gravacions, però respectant els espais d'intimitat (banys, vestuaris, taquilles o zones de descans) i no es podran emprar per finalitats diferents del control laboral. Tampoc es podran registrar les conversacions privades.

Als llocs de treball també s'ha d'informar de les zones videovigilades i els treballadors poden exercir el dret d'accés i cancel·lació. Les imatges s'han de cancel·lar als 30 dies i sols es podran conservar en cas de registrar una infracció concreta.

Si els videoporters es limiten a verificar la identitat de la trucada, i a facilitar l'accés a l'habitatge no s'haurà d'aplicar la normativa de protecció de dades. Si hi ha reproducció (per exemple pel conserge) o gravació d'imatges s'haurà d'aplicar la reglamentació que correspongui (informació, drets d'accés i cancel·lació i fitxer de dades).