

DIPUTACIÓ DE
VALÈNCIA



Protecció de Dades i Seguretat de la Informació



Quaderns DivalData

Quaderns dirigits a delegats,
responsables i especialistes en protecció
de dades personals

Quadern núm. 16 | Octubre 2021

***SMART CITIES: AVANTATGES I PRINCIPALS RISCOS PER ALS
DRETS I LLIBERTATS DELS CIUTADANS***



ÍNDEX



SMART CITIES: AVANTATGES I PRINCIPALS RISCOS PER ALS DRETS I LLIBERTATS DELS CIUTADANS

	Pàgina
Introducció	2
Avantatges de les <i>Smart Cities</i>	3
Riscos per als drets i llibertats associats a les <i>Smart Cities</i>	4
Salvaguardes relatives al tractament de dades personals en els projectes de <i>Smart Cities</i>	5
Material complementari i notícies	9



Vos convidem a traslladar-nos les temàtiques que resulten de vostre interès per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent

[enllaç](#)



INTRODUCCIÓ

La Comissió Europea ha definit les ciutats intel·ligents o *Smart Cities* com a agrupacions de projectes tecnològics diversos, orientats a optimitzar la gestió de recursos a les ciutats mitjançant l'ús de la tecnologia aplicada a gestionar, d'una manera més eficient, els serveis típics d'una ciutat, com poden ser els transports, infraestructures, subministraments de llum, aigua i gas, gestió dels residus o ajudes socials.

Els projectes més característics de les ciutats intel·ligents es basen en la recollida de dades de manera automatitzada mitjançant sensors distribuïts per la ciutat: de trànsit, de moviment de persones, de qualitat de l'aire, de consums energètics, etc. Després, es procedeix a l'anàlisi automatitzada d'aquestes dades, que pot realitzar-se de forma integrada i fins i tot enriquint les dades d'altres fonts. Si aquestes dades es combinen adequadament poden servir per a dimensionar i predir quins serveis oferir i en quina quantitat. Finalment, es disposa d'una fase d'elaboració de conclusions o decisions que, en determinats casos, podrien aplicar-se de manera automatitzada mitjançant activadors, per exemple, per a regular el trànsit rodat en una gran ciutat, i que poden implicar altres tecnologies. En definitiva, les *Smart Cities* es podrien considerar la integració de diferents tecnologies, -com a tècniques d'intel·ligència artificial i Big Data, i, en particular, el desenvolupament de projectes de IoT- amb un propòsit de gestió urbana.

Si bé les *Smart Cities* comporten la prestació de serveis públics de manera òptima i eficaç, no hem d'obviar els riscos inherents a les mateixes pel que fa a la protecció de les dades personals dels ciutadans. A continuació, parlarem d'aquests riscos i de les salvaguardes a aplicar en el desenvolupament d'aquestes ciutats, amb la finalitat de protegir el dret a la protecció de dades personals de la ciutadania.

“SI BÉ LES SMART CITIES COMPORTEN LA PRESTACIÓ DE SERVEIS PÚBLICS DE MANERA ÒPTIMA I EFICAÇ, NO HEM D'OBVIAR ELS RISCOS INHERENTS A LES MATEIXES PEL QUE FA A LA PROTECCIÓ DE LES DADES PERSONALS DELS CIUTADANS”.



“LA TECNOLOGIA SMART CITY OFEREIX LA CAPACITAT D'OBTINDRE INFORMACIÓ, EN TEMPS REAL, MITJANÇANT SENSORS O FONTS DE DADES DE DETERMINATS SERVEIS, DEL COMPORTAMENT DE LES CIUTATS I DELS SEUS HABITANTS. AIXÒ ES TRADUEIX EN UNA GESTIÓ MÉS EFICIENT DELS SERVEIS TÍPICS D'UNA CIUTAT”.

AVANTATGES DE LES SMART CITIES

En el marc de les competències de les Administracions Públiques, a les quals correspon la prestació de serveis de qualitat a la ciutadania, la tecnologia *Smart City* ofereix la capacitat d'obtenir informació, en temps real, mitjançant sensors o fonts de dades de determinats serveis, del comportament de les ciutats i dels seus habitants. Això es tradueix en una **gestió més eficient dels serveis típics d'una ciutat**, per exemple, en els següents àmbits:



Eficiència energètica en instal·lacions

Mitjançant la instal·lació de càmeres o sensors que detecten la presència de persones en les instal·lacions es pot automatitzar l'encesa i apagat de llums de manera eficient o la posada en funcionament de sistemes de refrigeració.



Mobilitat i gestió eficient del trànsit

Instal·lant càmeres i sensors en punts estratègics, es pot comptabilitzar a les persones i vehicles que hi ha en una zona, i donar prioritat a els uns o els altres en funció del volum i necessitat.



Eliminació de residus a través de sistemes de fem intel·ligents

Instal·lant sensors que detecten els nivells de fem en els contenidors i notificant als camions d'eliminació de deixalles quan és el moment de recollir, es podria reduir la contaminació acústica dels camions de fem i els costos en desenvolupar rutes més eficients adaptades al nivell real de residus generats en cada lloc.



**“FINS I TOT QUAN ES RECULLEN DADES
INICIALMENT ANONIMITZADES,
L'EXTENSIÓ, FREQÜÈNCIA,
COMBINACIÓ I ENRIQUIMENT DE
DADES PODEN RESULTAR EN UNA
REIDENTIFICACIÓ DE LES PERSONES”.**

RISCOS PER ALS DRETS I LLIBERTATS ASSOCIATS A LES SMART CITIES

Aquests tractaments són, en la majoria dels casos, d'alt risc, per la **gran acumulació de dades** que es realitza per part de les Administracions Públiques. Fins i tot quan es recullen dades inicialment anonimitzades, l'extensió, freqüència, combinació i enriquiment de dades poden resultar en una reidentificació de les persones, perquè tots tenim uns hàbits de comportament que són únics i revelen el nostre treball, amb qui vivim, la nostra salut o fins i tot les nostres conviccions polítiques i religioses.

D'un altre costat, la **instal·lació de sensors i actuadors de manera massiva incrementa la probabilitat que es produïsquen fallades de seguretat** en les tres dimensions de seguretat: confidencialitat, disponibilitat i integritat, per la qual cosa un aspecte molt delicat a considerar és la seguretat davant possibles fallades i davant atacs intencionats. L'anàlisi de riscos de seguretat des del punt de vista de protecció de dades ha de donar les màximes garanties perquè no es puguin produir accessos no autoritzats que permeten monitorar persones singulars o un filtrat massiu de dades personals, un dels grans riscos que tenen les *Smart Cities*.

Segons el parer de l'Agència Espanyola de Protecció de Dades (AEPD), els **dos moments crítics** que poden suposar un major risc per als drets i llibertats de la ciutadania són els següents:

- El **moment de desplegament del sistema**. És convenient que els desplegaments siguin limitats i que se sol·licite el consell de les autoritats de control.
- El **moment de la retirada o substitució del sistema** complet, ja que un sistema abandonat, o mig abandonat, pot resultar en una vulnerabilitat afegida.



“L'ANÀLISI DE RISCOS DES DEL PUNT DE VISTA DE PROTECCIÓ DE DADES HA D'OFERIR LES MÀXIMES GARANTIES PERQUÈ NO ES PUGUEN PRODUIR ACCESSOS NO AUTORITZATS QUE PERMETEN MONITORAR PERSONES SINGULARS O UN FILTRAT MASSIU DE DADES PERSONALS”.

SALVAGUARDES RELATIVES AL TRACTAMENT DE DADES PERSONALS EN ELS PROJECTES DE SMART CITIES

ANÀLISI PRÈVIA A LA POSADA EN MARXA DEL PROJECTE

La Guia per a Administracions Locals de l'AEPD destaca la necessitat que abans del desplegament d'un projecte d'aquest tipus és necessari realitzar:

- Una **anàlisi prèvia** del projecte sobre el **volum de la informació** que es pretén processar, el **número i tipus de fonts** des de les quals es pretén obtindre aquesta informació, la **frequència de recollida** de dades i el **temps durant el qual es pretén conservar** aquesta informació.
- L'anàlisi de l'enriquiment **de dades**, tant planificat en el tractament com del risc que aquest es produïska.
- Una **avaluació d'impacte** en els termes establits en l'article 35 del RGPD, valorant fins i tot la necessitat, segons les característiques del projecte, d'eleva una consulta prèvia a l'AEPD .

L'anàlisi de riscos de seguretat des del punt de vista de protecció de dades ha d'oferir les màximes garanties perquè no es puguén produir accessos no autoritzats que permeten monitorar persones singulars o un filtrat massiu de dades personals. La seguretat no pot ser total, però sí que es poden posar en marxa plans preventius d'auditoria contínua, com el *hacking* ètic, anàlisi de com evolucionen els riscos en funció del context (per exemple, amb el desplegament de nous serveis i tecnologies) i mesures que minimitzen l'impacte que una bretxa pot tindre. Aquestes mesures passen per l'aplicació de criteris de minimització de dades, separació de dades en diferents sistemes, en el temps i en les categories, ocultació de dades mitjançant tècniques de xifratge oseudonimizació primerenca o bloqueig de dades. En alguns casos podria ser interessant permetre a l'administrat tindre control de la recollida automàtica de les seues dades, posant en marxa mecanismes autònoms i transparents que contemplen la participació dels propis ciutadans, de manera que aquests puguén comprovar el compliment efectiu de les garanties establides.



“EL COMPLIMENT DELS OBJECTIUS D'EFICIÈNCIA DE LES SMART CITIES NO JUSTIFICA UNA RECOLLIDA MASSIVA I INDISCRIMINADA DE DADES PERSONALS. LES DADES RECAPTADES HAN DE SER ADEQUATS, PERTINENTS I LIMITATS AL NECESSARI EN RELACIÓ AMB ELS FINS PER ALS QUALS SÓN TRACTATS (PRINCIPI DE MINIMITZACIÓ DE DADES)”.

MINIMITZACIÓ DE DADES PERSONALS

El compliment dels objectius d'eficiència de les *Smart Cities* no justifica una recollida massiva i indiscriminada de dades personals. Atés el principi de minimització, les dades recaptades han de ser **adequats, pertinents i limitats al necessari** en relació amb els fins per als quals són tractats.

FINALITAT DE LA RECOLLIDA DE DADES

La finalitat de la informació recollida pot ser la d'executar **tant la funció pública com la investigació científica o fins estadístics**. En aqueixos casos, cal tindre en compte la compatibilitat d'aquests últims tractaments amb els fins anteriors, en els termes de la normativa de protecció de dades, sempre que estiguen subjectes a les garanties adequats. Per exemple, a l'hora de la recollida automàtica, en temps real, d'informació amb propòsit estadístic, entre altres mesures legals, tècniques i organitzatives, s'ha d'analitzar la grandària de la mostra, determinada pel nombre de subjectes o elements d'una població necessaris perquè les dades obtingudes siguen representatius i eficaços. La quantitat de dades personals recollits, entesa tant com l'extensió del nombre de subjectes com el conjunt de dades recollides d'un mateix subjecte, s'han de sotmetre a una anàlisi de proporcionalitat i necessitat.

DADES ANÒNIMS I AGREGATS

En molts tractaments vinculats a la *Smart Cities* no serà necessari identificar unívocament als ciutadans, sinó que es podria complir amb la finalitat emprant dades anònimes i agregats. Per exemple, per a predir quan i on es produeixen els pics de trànsit, on és necessari optimitzar el subministrament energètic o on cal millorar la recollida de residus. Per tant, s'haurà d'analitzar **si es requereix identificar als ciutadans**, valorat si és suficient per als objectius del tractament l'ús de dades anònimes i agregats.



***“EN AQUESTA MENA DE PROJECTES,
SOLEN SER DIVERSOS ELS
INTERVINENTS. SERÀ IMPORTANT
ACLARIR QUI PRESA LES DECISIONS A
CADA MOMENT ACTUANT COM A
RESPONSABLE DEL TRACTAMENT, O
COM A CORRESPONSABLE, I QUI
OSTENTA LA CONDICIÓN
D'ENCARREGAT; I COM ES
FORMALITZA LA RELACIÓ ENTRE ELLS”.***

Fins i tot quan es recullen dades inicialment anonimitzades, com apuntàvem abans, l'extensió, freqüència, combinació i enriquiment de dades poden resultar en una reidentificació de les persones. **El risc de reidentificació s'ha d'avaluar i prendre mesures per a mitigar-lo**, com pot ser aplicar tècniques de privacitat diferencial, ús d'estratègies d'agregació d'informació per a evitar correlacions, recórrer al processament local i distribuït per a reduir la quantitat de dades emmagatzemades de manera centralitzada per un mateix responsable, etc.

LLEIALTAT

Les dades recollides s'han d'utilitzar per a la finalitat **perseguida i el propòsit original**. Per exemple, quan un tractament té com a objecte el garantir que una determinada àrea de la ciutat tinga restriccions d'accés, s'ha de diferenciar el propòsit de controlar aquest accés del que és l'activitat sancionadora d'aquells que no compleixen amb aquestes restriccions. Per tant, el tractament ha de buscar la màxima efectivitat en el propòsit original sent proporcional al grau d'intrusió en la privacitat dels administrats, no ha de centrar-se exclusivament a buscar la màxima eficiència en un dels seus instruments d'aplicació.

DETERMINACIÓ DE ROLS

En aquesta mena de projectes, solen ser diversos els intervinents, realitzant cadascun d'ells una part del tractament. En aquest punt, serà important **aclarir qui pren les decisions a cada moment actuant com a responsable del tractament, o com a corresponsable, i qui ostenta la condició d'encarregat**; i com es formalitza la relació entre ells. En concret, cal delimitar quines dades empra cadascuna de les parts i per a què.

A l'hora de redactar els contractes entre responsables, corresponsables i encarregats és important tindre en compte que aquest tipus de projectes són plantejaments a llarg termini, amb conseqüències que poden evolucionar molt en funció de canvis en el context social o tecnològic. El **manteniment dels dispositius i dels sistemes, la propietat i responsabilitat d'actualitzar els**



***“CAL INFORMAR ADEQUADAMENT ELS
CIUTADANS DEL MARC DEL SERVEI EN
EL QUAL ES PRODUUEIX LA RECOLLIDA
DE DADES, DE QUINES DADES ES
RECULLEN I PER A QUÈ I DE COM
PODEN EXERCIR ELS SEUS DRETS
SOBRE AQUESTS”.***

mateixos, així com el suport al responsable per a realitzar tota la gestió de riscos per als drets i llibertats (incloent la probable EIPD) són aspectes que hauran de reflectir-se en aquests contractes.

DEURE D'INFORMACIÓ

Quan es recullen dades de persones i, encara que després s'anonimitzen, cal **informar-los adequadament del marc del servei en el qual es produeix aquesta recollida, de quines dades es recullen i per a què i de com poden exercir els seus drets sobre aquests**. La pàgina web de l'Administració Pública pot ser un bon lloc per a donar publicitat a aquesta informació.

Això, més enllà del compliment de la normativa de protecció de dades, permet als ciutadans tindre coneixement dels riscos, les normes, les salvaguardes i els drets relatius al tractament de dades personals així com de la manera d'exercir els seus drets en relació amb el tractament, augmentant així el seu nivell de confiança i compromís amb el projecte.



MATERIAL COMPLEMENTARI

- Tecnologies i Protecció de Dades en les Administracions Públiques (AEPD). Consulta en [aquest enllaç](#).

- La protecció de dades de caràcter personal a les ciutats intel·ligents (APDCAT).

Consulta en [aquest enllaç](#).

- “Smart Cities: més enllà de la seguretat, la privacitat dels ciutadans” (Ponència del cicle de debats de l'AEPD sobre Innovació i Protecció de Dades).

Consulta el video en [aquest enllaç](#).

- Web *SmartCity València*.

Consulta la web en [aquest enllaç](#).

NOTÍCIES

- **L'Agència Espanyola de Protecció de Dades (AEPD) arxiva actuacions en relació amb un Ajuntament que, a partir del CSV de dos documents generats, va permetre accedir al conjunt d'informació de multitud d'interessats**

Un Ajuntament va remetre en paper canvis cadastrals a 750 interessats, que suposaven variacions en un cert impost municipal. Un dels interessats va comprovar el CSV en la web de l'Ajuntament i va resultar que podia veure la seua notificació i la de la resta d'implicats. L'Agència Espanyola de Protecció de Dades (AEPD) arxiva actuacions en considerar que l'Ajuntament disposava de mesures tècniques i organitzatives raonables per a evitar aquest tipus d'incidència; no obstant això, i una vegada detectada aquesta, va reaccionar de manera diligent en notificar-li'l a l'AEPD. Consulta la Resolució en [aquest enllaç](#).

- **L'AEPD es pronuncia sobre la possibilitat d'incloure el nom i cognoms de les persones accidentades en el document remés als Delegats de Prevenció, relatiu a la relació d'accidents de treball i malalties professionals que han causat al treballador una incapacitat laboral superior a un dia.**

L'Agència Espanyola de Protecció de Dades ha publicat la guia 'Gestió del risc i avaluació d'impacte en tractaments de dades personals', un document que incorpora l'experiència acumulada en l'aplicació de la gestió del risc en l'àmbit de la protecció de dades des de l'aplicació del Reglament General de Protecció de Dades (RGPD) i afegint les interpretacions de l'AEPD, el Comitè Europeu de Protecció de Dades i el Supervisor Europeu de Protecció de Dades.

El document, dirigit a responsables, encarregats de tractaments i delegats de protecció de dades (DPD), ofereix una visió unificada de la gestió de riscos i de les avaluacions d'impacte en protecció de dades, i facilita la integració de la gestió de riscos en els processos de gestió i governança de les entitats.

Consulta l'informe en [aquest enllaç](#).