LA PROTECCIÓ DE DADES DE CARÀCTER PERSONAL EN LES CIUTATS INTEL·LIGENTS ("SMART CITIES")

-Document per al debat-

Barcelona, febrer de 2013

INDEX

1. INTRODUCCIÓ

Aquest document de treball constitueix un punt de partida en l'estudi de l'impacte en la privacitat de les persones de la implantació de les anomenades ciutats intel·ligents o "Smart cities"[1]. Per fer-ho, ens caldrà definir, en primer lloc què s'entén per Smart City, i quins són els eixos d'interès de les Smart Cities. Com veurem, en aquest context moltes ciutats estan desenvolupant diferents serveis i prestacions que es posen a disposició dels ciutadans, i que pretenen aconseguir un model de ciutat més habitable, més eficient i més sostenible.

El desenvolupament de les Smart Cities genera (i és previsible que en el futur això s'incrementi exponencialment) un tractament d'informació de tot tipus (mediambiental, de recursos energètics, de consum, de trànsit i moviments urbans,...). En aquest treball no ens referirem a tota la informació vinculada al desenvolupament de les Smart Cities sinó que ens centrarem només en analitzar si en el context de les Smart Cities es produeix un "tractament de dades personals" (article 3.a i 3.c) de la Llei orgànica de Protecció de Dades, LOPD), de quin tipus, i quines afectacions pot tenir aquest tractament des de la perspectiva de la protecció de dades i la privacitat, en concret, en atenció als principis i obligacions de la normativa de protecció de dades (Directiva 95/46/CE, així com la LOPD i el RLOPD, especialment)[2].

En aquesta anàlisi s'han tingut en compte diversos exemples del que anomenarem "experiències Smart City" per tal d'examinar quines dificultats es poden trobar per aplicar adequadament els principis de la protecció de dades, però òbviament les aplicacions i els serveis que es poden encabir dins del concepte d'Smart City poden anar molt més enllà.

[1] Atès que en aquest document es fa referència a diversos conceptes que es coneixen i s'utilitzen de forma generalitzada en anglès, es considera adient mantenir certes referències en la seva versió anglesa.

[2] Normativa citada: Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (DOCE L 281, de 23.11.1995), Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (BOE núm. 298, de 14.12.1999) i Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la LOPD (BOE núm. 17, de 19.1.2008).

Per fonamentar les consideracions i reflexions que es fan a continuació, que només pretenen ser un "punt de partida" o un apunt sobre diversos aspectes clau sobre els que caldrà reflexionar des de la perspectiva de la protecció de dades, s'ha tingut en compte la normativa reguladora de la protecció de dades i també la relativa al desenvolupament de qüestions relacionades amb les Smart Cities, principalment en el marc de la UE (Recomanacions, Grups de treball...), així com diversos documents que considerem rellevants, per provenir de grups d'experts i autoritats rellevants en matèria de protecció de dades personals.

2. OBJECTIUS DEL DOCUMENT DE TREBALL

Aquest Document de Treball es vol configurar com un element que ajudi a valorar possibles actuacions que aquesta Autoritat[3] pot dur a terme en relació amb les Smart Cities i altres temes relacionats, en el sentit d'obrir el debat i l'anàlisi sobre la qüestió, des de la perspectiva de la protecció de dades personals i també com un element de reflexió tan per a les administracions públiques de Catalunya que volen implantar algun dels serveis que s'engloben dins les Smart Cities, com per a les empreses que duen a terme el disseny i la implantació d'aquestes tecnologies. En aquest sentit, resulta convenient obrir la possibilitat que les diferents "parts interessades" -*stakeholders*- (Ajuntaments i altres administracions, sector públic i privat implicat en desenvolupaments d'experiències Smart City, grups de treball, universitats...) puguin fer aportacions, comentaris a aquest Document de Treball o obrir altres vies de col·laboració, amb vistes a contribuir a millorar, des de la perspectiva de la protecció de dades personals, el desplegament de les Smart Cities.

En qualsevol cas, ja avancem que en aquest Document de Treball posarem alguns exemples d'Smart Cities, d'aplicacions concretes que s'han dut a terme i que podem englobar en aquest concepte ampli (que poden afectar al trànsit -carrils VAO, Teletacs, etc-, a l'aparcament, sistemes de geolocalització de places d'aparcament disponibles, gestió de flotes de vehicles o bicicletes, enllumenat públic, recollida d'escombraries, localització d'espais o comerços, títols de transport públic personalitzats, etc), i tractarem amb deteniment el que es refereix al desenvolupament energètic sostenible,

[3] Veure la Llei 32/20010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades (DOGC núm. 5731, de 8.10.2010).

en el marc de les Smart Cities. Actualment, un dels punts clau de les Smart Cities, és l'aprofitament sostenible de recursos energètics. Això ha portat a la UE a elaborar una sèrie de documents (recomanacions, comunicacions, que citarem en detall més endavant) que tracten precisament de la progressiva implantació de xarxes intel·ligents i de comptadors intel·ligents. Això pot comportar un tractament de dades important, i per això aquestes xarxes i comptadors, i els textos que des de la UE es van elaborant, han estat objecte d'anàlisi per part dels experts en protecció de dades (Supervisor Europeu de Protecció de Dades "SEPD", el Grup de Treball de l'Article 29 "GT29", o Grup de Treball en Protecció de Dades i Telecomunicacions "Grup de Berlín"). Com que aquests textos analitzen qüestions importants en relació amb la protecció de dades, en farem esment abastament en diferents punts d'aquest Document de Treball. Certament, bona part d'aquests documents es centren en les xarxes i els comptadors intel·ligents, però les qüestions apuntades (aplicació de principis de protecció de dades, seguretat de les dades, advertiments al legislador...) pensem que són extrapolables, al menys en part, a d'altres exemples o concrecions de les Smart Cities, que poden generar un important tractament de dades personals.

3. CONCEPTES

Per bé que no es disposa d'una definició tancada o uniforme del que són les "ciutats intel·ligents" o Smart Cities, es pot considerar que hi ha una sèrie d'elements que haurien d'estar presents en major o menor mesura, per tal de considerar una ciutat o un determinat servei com a *smart*.

La definició o, al menys, l'enumeració dels elements que haurien de concórrer per definir una Smart City, és rellevant perquè ens permetrà diferenciar les Smart Cities d'altres conceptes, que poden tenir major o menor rellevància des de la perspectiva de la protecció de dades personals.

Situar adequadament aquests conceptes permetrà situar l'objecte d'estudi, és a dir, l'impacte o incidència de les Smart Cities en la protecció de dades personals, així com deixar de banda altres qüestions que no tenen especial repercussió en la matèria que ens ocupa (per exemple, utilització d'informació mediambiental o d'estat del trànsit en

un municipi, sense cap relació amb persones concretes, que es posa a disposició dels ciutadans i del públic en general).

3.1. Què és una Smart City?

Com a primera aproximació al terme d'Smart City[4], es pot afirmar que es tracta d'un model de desenvolupament urbà que en els darrers anys ha despertat l'interès de diversos sectors (administracions públiques, autoritats locals, sector privat, etc), que té a veure amb qüestions tan diverses com ara el creixement i la gestió sostenible de les àrees urbanes, la prosperitat econòmica en termes "d'economia intel·ligent, sostenible i integradora"[5], la utilització més eficient de l'energia –apostant clarament per les energies renovables- i d'altres recursos en l'entorn urbà, la millora de les condicions de vida dels seus habitants en relació amb àmbits tan diversos com l'educació, el transport públic, la salut o el medi ambient, així com la major implicació dels propis habitants de nuclis urbans en aquest desenvolupament. Es busca, en aquest sentit, aprofundir en el concepte clàssic de "comunitat".

Alguns autors defineixen com a *smart* aquella ciutat en la que les inversions en capital humà i social i les infraestructures de comunicació (amb especial referència a les Tecnologies de la Informació i la Comunicació, "TIC"), estan enfocades al desenvolupament econòmic sostenible, i en les que hi ha –o es persegueix- una alta qualitat de vida, una gestió intel·ligent dels recursos naturals i una governança participativa a nivell social i cultural.[6] Certament, el terme de "governança", entesa com la manera de governar que es fonamenta en la interrelació dels organismes encarregats de la direcció política d'un territori i la societat civil, per donar poder, autoritat i influència a la societat sobre les decisions que afecten la vida pública, sembla que ha de prendre un clar protagonisme en l'entorn de les Smart Cities.

Es pot relacionar les Smart Cities amb el concepte d'"Ecobarri", que té la virtut de ser un entorn prou ampli com per fer-hi determinades transformacions que busquen el

[4] Especialment il·lustratiu, pels exemples exposats d'Smart Cities a diverses ciutats espanyoles, és: "Smart Cities: un primer paso hacia la internet de las cosas". Fund. Telefónica, Ed. Ariel.
[5] Comunicació de la Comissió Europea "Europa 2020. Una estrategia para un crecimiento inteligente, sostenible e integrador". Brussel·les, 3.3.2010, COM (2010)2020.
[6] "Smart Cities in Europe". A. Caragliu, C. del Po, P. Nijkamp (2009). http://ideas.repec.org/p/dgr/vuarem/2009-48.html

desenvolupament sostenible, i de ser, al mateix temps, prou acotat com per fomentar més fàcilment la implicació dels seus habitants.[7]

En definitiva, hi ha un cert consens a l'hora de considerar que l'habitabilitat, l'eficiència energètica, els recursos tecnològics avançats i la iniciativa econòmica i empresarial d'innovació, entre d'altres, són premisses que haurien d'estar presents, en major o menor mesura, quan ens referim a les Smart Cities. Es parla també dels "eixos" principals de les Smart Cities, en concret, l'economia intel·ligent; mobilitat intel·ligent; medi ambient intel·ligent; població intel·ligent; manera de viure intel·ligent i governança intel·ligent. Aquests eixos es basen en teories de competitivitat regional, transport i TIC, recursos naturals, capital humà i social, qualitat de vida i participació dels ciutadans en la governança de les ciutats.[8] Així doncs, àmbits com el de demografia, aspectes socials i econòmics, desenvolupament cívic, educació, medi ambient (tant a nivell d'espais públics com, per exemple, a través del desenvolupament d'edificis intel·ligents), transport i mobilitat, societat de la informació, oci i cultura, sembla que poden estar (o han d'estar) en major o menor proporció presents en l'agenda d'una ciutat que es vulgui considerar "smart".

D'entrada, cal dir que hi ha actualment un gran nombre de ciutats que poden ser catalogades -o que, com a mínim, es consideren a elles mateixes- com a Smart Cities. Són molts els exemples d'Smart Cities que es poden esmentar. Alguns autors en fan, fins i tot, una classificació segons l'àmbit prioritzat en cada cas (transport o mobilitat urbana, gestió energètica, medi ambient o e-govern, entre d'altres)[9].

---

[7] MORÁN ALONSO, N. "Ecobarrio".Madrid, 9.6.2008, citant la definició de RUDIN, D. FALK, N. (1999) "Building the 21st century home. The Sustainable Urban Neighbourhood." Architectural Press. (http://habitat.aq.upm.es).

[8] Font: Diversos articles extrets de la documentació inclosa en el Dossier "Smart City:vivere meglio in città piú intel.ligenti" (disponibles en anglès) del "FORUM PA 2010": http://portal.forumpa.it/

[9] "¿Qué son las smart cities o ciudades inteligentes?". J. M. Hernández Muñoz, http://sociedadinformacion.fundacion.telefonica.com:
"- Eficiencia y gestión energética: Màlaga, Amsterdam.
- Entornos de negocio y 'economía del conocimiento': Luxemburgo, Dubai, Malta, Kochi.
- Transporte y movilidad urbana: Singapur, Brisbane, Estocolmo, Maastricht.
- e-Gobierno y participación ciudadana: Tampere, Turku, Alburquerque.
- Medio-ambiente: Copenhague, Vancouver, Melbourne, Montpellier.
- Urbanismo (también energías y entornos de negocio): Masdar, Sondgo.
- Turismo y actividad cultural: París, Londres, Salzburgo, Brujas, Sidney, Zurich, etc.
- Sanidad y atención personal: París, Granada, (...)."

En qualsevol cas, a dia d'avui no hi ha un "registre oficial" de ciutats *smart*, ni cap autoritat o ens, públic o privat, que s'encarregui de donar un segell de validesa a una ciutat per tal d'esdevenir *smart*. En aquest sentit hem de tenir en compte que es tracta d'un procés obert, on els canvis i els passos endavant, a vegades significatius i a vegades petits però constants, es van produint de forma incessant.

Són diversos els fòrums, grups de treball i iniciatives, tant públiques com promogudes des del sector privat empresarial, que en els darrers anys focalitzen el seu interès en el fenomen de les Smart Cities i en les experiències i iniciatives que es duen a terme en diversos països. Sens perjudici que, si resulta oportú, es faran comentaris o valoracions més concretes al respecte, a efectes il·lustratius en citem algun, per incloure diversos llistats de ciutats, amb detall de les "experiències Smart City" dutes a terme o planificades[10]:

A nivell de la UE destaca el Projecte "European Smart Cities"[11], que novament recorre als "eixos" citats (economia, mobilitat, medi ambient, persones, manera de viure, governança), i estableix fins i tot un rànquing de ciutats smart europees, en funció de la seva posició segons el "benchmarking" (estàndard de comparació) predefinit. Prendrem com a referència aquest estudi, per posar alguns exemples d'experiències Smart Cities en l'apartat corresponent del nostre estudi. En aquest Projecte s'estudien 70 ciutats europees, sense que això impliqui, ni de bon tros, que siguin les úniques ciutats a les que es pugui considerar com a Smart Cities. Pel que fa a Espanya, s'hi va incloure Pamplona, Oviedo i Valladolid.

Pel que fa a Catalunya, diverses ciutats han endegat projectes relacionats amb les Smart Cities, entre d'altres, Barcelona, Sabadell, Figueres, Sant Vicenç dels Horts, Sant Cugat del Vallès, Viladecans o Tarragona. Les ciutats catalanes han apostat en els darrers anys per involucrar-se en el desenvolupament de projectes relacionats, entre d'altres, amb l'Open data[12]; sensorització de places d'aparcament; la gestió eficient i sostenible en els camps de la il·luminació urbana, l'aigua, la mobilitat,

[10] Alguns altres són: - SETIS "European Initiative on Smart Cities": http://setis.ec.europa.eu/about-setis/technology-roadmap/european-initiative-on-smart-cities
[11] Tota la documentació citada es troba a: http://www.smart-cities.eu
[12] Pel que fa a exemples d'Open Data, també cal citar el portal de la Generalitat de Catalunya: http://www20.gencat.cat/portal/site/dadesobertes

l'energia o la gestió i recollida de residus; medició de magnituds mediambientals (temperatura, humitat, pluja...); la medició del trànsit de vehicles a través de sensors; la reducció de consum energètic en vivendes; l'ús de bicicletes i de vehicles elèctrics; les xarxes de fibra òptica i les xarxes inalàmbriques "Wi-Fi", etc. [13]

Diverses ciutats catalanes també s'han involucrat en els darrers anys en l'organització i participació en diversos fòrums i grups de debat sobre el desenvolupament d'experiències d'Smart City.[14]

Un altre Projecte que voldríem destacar és el Projecte "Smart Cities"[15], ja que s'hi fa servir un concepte que pot tenir certa rellevància en relació amb la protecció de dades (o millor, pot ser un instrument per protegir la privacitat). Es tracta del concepte de "personas" (paraula en castellà, utilitzada així en el document original en anglès)[16], que es refereix no a "persones físiques identificades o identificables", sinó que es tracta d'arquetips, models de persones que reuneixen una sèrie de característiques concretes. A aquest arquetip se li atribueix un nom, edat, professió, interessos i aficions... en definitiva, un "perfil", incloent les seves capacitats d'interactuar amb TICs..., però sense fer referència a cap persona "real". A banda que aquest concepte pugui ser objecte de major estudi, als efectes del que ens interessa, és a dir, del

[13] A banda d'exemples que citarem en altres apartats, esmentem les següents referències:
Barcelona: Sobre diverses accions previstes: http://smartbarcelona.cat ; "SMARTGEO: TIC/SIG i smart cities", a www.gencat.cat (Departament de Territori i Sostenibilitat) ; sobre l'Open Data: http://w20.bcn.cat/opendata/ ; consultar el document "Compromís ciutadà per la sostenibilitat 2012-2020", a: http://w110.bcn.cat ; sobre la xarxa wifi: http://www.bcn.cat/barcelonawifi.ca
Sabadell: Sobre el servei Open Data: www.sabadell.cat
Figueres: Instal·lació de sensors per recollir dades sobre la circulació de vehicles, l'enllumenat o la gestió de residus (www.figueres.cat)
Sant Vicenç dels Horts: Participació en el Projecte "Sanvi Sens" (www.smartcities.es; http://www.i2cat.net/es/projecte/sanvi-sens-0).
Sant Cugat del Vallès: Participació en el Projecte europeu "3e-houses", de reducció de consum energètic (www.upc.es) ; Projecte pilot de carrer intel·ligent integral (http://smartcity.santcugat.cat).
Viladecans: Veure diversos projectes a: http://europa2020.cviladecans.cat i www.smartcityviladecans.com

[14] "2nd Smart City Expo World Congress", Barcelona, 13-15.11.2012 (http://www.smartcityexpo.com/ca/congress); "I Congrés Mediterrani d'Eficiència Energètica i Smart Green Cities", Tarragona, 7-8.11.2012 (www.tarragona.cat); Jornada: "Una ciutat intel·ligent per a una societat del benestar" (S. Vicenç dels Horts, 24.11.2011); Jornada: "Estrategia Smart City para los municipios de Cataluña", Viladecans, 27.3.2012 (www.viladecans.cat ; www.smartcityviladecans.com); "Sabadell Smart Congress", 8-9.4.2013 (www.sabadellsmartcongress.com);

[15] "North Sea Region Programme", projecte d'un grup d'investigació que rep suport de la "European Regional Development Fund." Font: http://www.smartcities.info

[16] Concepte creat per Alan Cooper, expert en software. Sobre aquest concepte i les seves aplicacions, veure: "Making customer groups real – using Personas". www.smartcities.info

tractament de dades personals en Smart Cities, i de la millor protecció possible dels principis de la protecció de dades, es podria reflexionar sobre la possibilitat d'utilitzar "personas" o arquetips en diferents experiències Smart Cities (com a mínim, en la seva fase d'estudi i disseny[17], en què es podria treballar amb aquests arquetips, i no amb dades personals "de persones reals"). Fins i tot, un cop posada en marxa una determinada experiència d'Smart City, i recordant la idea que les persones han de poder utilitzar, en alguns casos, "diferents identitats digitals", no descartem que determinats serveis d'Smart City puguin dur-se a terme sense utilitzar la identitat "real", sinó un arquetip. Tornarem sobre aquesta qüestió més endavant.

En qualsevol cas, és clar que el progressiu desenvolupament de les iniciatives urbanes intel·ligents podria suposar una interconnexió de serveis i infraestructures cada vegada més important. Si les ciutats tendeixen a oferir més serveis als habitants de nuclis urbans, si aquests serveis han de ser "intel·ligents" en els termes apuntats, és fàcil inferir que es tendirà a un major ús de les TIC, qualitativament i quantitativament. Les TIC poden aportar rendibilitat d'esforços, eficiència energètica, optimització de recursos, factors, en definitiva, que encaixen especialment en el model Smart Cities.

Sense voler focalitzar en les TIC tota la rellevància que des de la perspectiva de la protecció de dades pot tenir el desenvolupament de les Smart Cities, és evident que les tecnologies que s'apliquen –o poden arribar a aplicar-se- als serveis i infraestructures de les Smart Cities poden arribar a tenir un clar impacte en la privacitat dels ciutadans, principals beneficiaris, al mateix temps, dels esmentats serveis i infraestructures.

Farem esment d'algunes tecnologies (RFID, NFC, geolocalització, xarxes de sensors i comptadors intel·ligents...) l'ús de les quals amplien de forma rellevant les possibilitats de millora i eficàcia en la gestió i prestació de serveis en àmbit municipal. El potencial que això representa, unit a la dinàmica emprenedora de moltes ciutats que volen esdevenir *smart,* més enllà del factor "moda", [18] que sembla inevitable en el tema que

[17] Aquest grup d'investigadors posa l'exemple del municipi de Karlstad, a Suècia, en què s'utilitzen aquests "prototips" per dissenyar un producte o servei, en el context de les Smart Cities. No s'afecta, així, a dades personals "reals", cosa que des de la perspectiva del principi de minimització, entre d'altres, sembla força interessant.

[18] Tot i el desenvolupament, en els darrers anys, d'aquest concepte d'Smart City, val a dir que el tema no és nou, doncs ja a l'any 1994, la Carta de Ciutats i Viles Europees cap a la Sostenibilitat, (Carta d'Aalborg), apuntava en aquesta direcció. La Carta d'Aalborg es va

ens ocupa, fa que les "experiències Smart City" hagin de tenir especialment en compte quin tractament de dades personals es farà (si cal fer-ne algun), i com afectarà a la privacitat dels ciutadans l'ús d'aquestes tecnologies en el desenvolupament de les Smart Cities.

3.2. Altres conceptes relacionats

Smart grids (xarxes intel·ligents) i ***Smart metering*** (comptadors intel·ligents).

Les xarxes intel·ligents s'utilitzen per optimitzar la xarxa de distribució d'energia elèctrica, bàsicament, de forma que es busca un ús sostenible i eficient del recurs (aigua, gas, electricitat, són serveis que es poden veure optimitzats a través de la utilització de xarxes intel·ligents). Es tracta, doncs, d'un sistema que permet la comunicació bidireccional entre el consumidor final, ja sigui una persona física o jurídica, i les companyies subministradores del servei. La informació que s'obté en aquest procés de comunicació, permet a les companyies subministradores realitzar un ús més eficient dels recursos.

Segons la Recomanació de la Comissió Europea de 9 de març de 2012[19], relativa als preparatius de desplegament dels sistemes de comptador intel·ligent, la xarxa intel·ligent és:

"Xarxa energètica millorada amb l'addició de comunicacions digitals bidireccionals entre el proveïdor i el consumidor, comptadors intel·ligents i sistemes de seguiment i control".

En relació amb les xarxes intel·ligents, ens interessa especialment, dins el marc europeu, citar els treballs duts a terme des de la Comissió Europea, en concret, des de la Comissió d'Europea (Direcció Gral. d'Energia).[20] A banda del que es dirà de la Recomanació de 9.3.2012, citada, fem esment que des d'aquesta D.G. s'ha difós el document "Guidelines for conducting a cost-benefit analysis of Smart Grid projects"

aprovar a la Conferència Europea sobre Ciutats i Viles sostenibles (maig de 1994), sota el patrocini de la Comissió Europea, organitzada pel Consell Int. per a Iniciatives Ambientals.

[19] DOUE L/73 de 13.3.2012

[20] Es pot trobar la diversa documentació citada, a la web: http://ec.europa.eu/energy/gas_electricity/smartgrids/smartgrids_en.htm

(autor: Joint Research Centre), on es donen pautes a seguir per realitzar l'anàlisi de cost-benefici d'aquestes xarxes. Si bé la privacitat i la protecció de dades no és, francament, un dels eixos principals d'aquest document, es fa esment que, entre les àrees "d'impacte social" que pot tenir el desenvolupament d'aquestes xarxes, hi ha la privacitat i la seguretat, que l'anàlisi de cost-benefici de les xarxes ha de procurar que en el desenvolupament d'aquestes s'asseguri la privacitat de les dades i la ciber-seguretat, i que s'hauria d'incloure els costos addicionals estimats per implementar mesures de prevenció. Com a mínim, doncs, és clar que la perspectiva de la protecció de dades està present en els objectius dels organismes de la UE implicats en la progressiva implantació de les xarxes intel·ligents[21]. Del conjunt de documents que citem de la D.G. d'Energia, també volem esmentar el "Set of common functional requirements of the SMART METER"[22]. Resulta particularment interessant el fet que s'hi estableixen una sèrie de "funcionalitats per la seguretat i la privacitat" en l'àmbit de les xarxes intel·ligents (partint de la base que aquestes comporten tractaments de dades respecte els quals hi ha certs dubtes de com s'han de dur a terme, o dels riscs que presenten), que considerem que podrien extrapolar-se a d'altres anàlisis de privacitat des del disseny o avaluacions de l'impacte sobre la privacitat (Privacy impact assesments o PIAs) referides a d'altres experiències Smart City. Entre d'altres funcionalitats, es fa referència a que cal que les comunicacions de dades entre subministradors d'energia i operadors sigui segura, que es valori si la seguretat i la privacitat es tenen en compte en el disseny de la xarxa, valorar les notificacions que cal fer d'atacs a la seguretat de les dades, controlar els accessos a la informació.... En definitiva, són qüestions que estan presents en el "disseny" de les xarxes intel·ligents, i que no deixen de ser elements que reconeixem com a propis d'una anàlisi relacionada amb molts altres tractaments de dades personals.

El concepte de xarxa intel·ligent s'ha de posar en relació, necessàriament, amb el concepte de "comptador intel·ligent" (smart metering), ja que és a través d'aquests

[21] Trobem referències més explícites a la necessitat d'assegurar els drets de privacitat dels ciutadans, i d'aplicar estàndards de seguretat adequats, per evitar les conseqüències d'un tractament incorrecte de dades tractades en les xarxes intel·ligents, així com la necessitat de tenir en compte la Directiva de 1995 de protecció de dades i la Directiva 2002/58/CE sobre comunicacions electròniques en el desenvolupament de xarxes intel·ligents, en el document de la DG. d'Energia de la Comissió Europea: "Smart Grid Mandate: Standardisation Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment", de març de 2011.

[22] Document d'octubre de 2011, de la D.G. d'Energia, esmentada.

comptadors, principalment, que es recull informació sobre el consum d'energia per part dels usuaris.

Cal subratllar que l'ús i desenvolupament a Europa dels "comptadors intel·ligents [23] ha estat motiu d'atenció especial per part de la UE, així com dels operadors de protecció de dades (principalment, Supervisor Europeu de Protecció de Dades "SEPD", el Grup de Treball de l'Article 29 "GT29", i Grup de Treball en Protecció de Dades i Telecomunicacions "Grup de Berlín"). En aquest Document de Treball es fa especial atenció a diversos textos i recomanacions emanats dels citats operadors.

Segons la Recomanació de 9 de març de 2012, citada, un sistema de comptador intel·ligent és:

"Sistema electrònic que pot mesurar el consum d'energia, afegint més informació que un comptador convencional, així com transmetre i rebre dades mitjançant comunicacions electròniques".

Des del moment en què el consumidor final sigui una o més persones físiques (un particular, un nucli familiar...), si la informació obtinguda conté dades de caràcter personal, i si aquestes dades són objecte de tractament per part de tercers –altres persones físiques o jurídiques, públiques o privades-, cal tenir en compte les obligacions i principis de la normativa aplicable de protecció de dades personals.

Certament, el tractament de dades personals en el consum energètic per part dels consumidors finals (que poden ser tant persones físiques, grups familiars, com empreses i altres persones jurídiques), no és nou. Amb la utilització de comptadors d'energia tradicionals ja es podia mesurar un consum associat a persones físiques, amb la qual cosa ja es feia un cert tractament de dades personals. Ara bé, els comptadors intel·ligents permeten recollir i tractar aquesta informació amb un grau de detall molt major. Això, unit al fet que en el context de les Smart Cities un dels elements clau és el consum sostenible de recursos energètics per part dels ciutadans, fa que des de la perspectiva de la protecció de dades sigui necessari fer especial atenció a aquesta qüestió.

[23] Pel que fa al desenvolupament normatiu a nivell d'Estats de la UE, se'n fa un estudi força detallat i actualitzat, en el Document: "European Smart Metering Landscape Report 2012", AA.VV, (Viena, Octubre 2012). Font: www.smartregions.net

En qualsevol cas, partirem de la base, com explicita el Considerant 7 de la Recomanació 9.3.2012, que els drets i obligacions de la Directiva de protecció de dades de 1995 "són plenament aplicables als comptadors intel·ligents que tracten dades personals, en particular en l'ús de serveis de comunicacions electròniques disponibles al públic per a les relacions contractuals i comercials amb els clients."

Segons el Considerant 2 de la mateixa Recomanació, els Estats membres de la UE estan obligats a garantir la utilització de sistemes de comptador intel·ligent que contribueixin a la participació activa dels consumidors en el mercat del subministrament d'electricitat i gas (...). Per tant, sembla inevitable la progressiva implantació d'aquests sistemes, i el tractament de dades subsegüent, també en el marc de les Smart Cities.

El desenvolupament de les xarxes i comptadors intel·ligents és una clara prioritat normativa de la UE. Això es demostra pel fet que hi ha diversos textos amb diferent valor normatiu que s'hi relacionen, entre d'altres:

- Projecte de Directiva sobre eficiència energètica i de derogació de les Directives 2004/8/CE i 2006/32/CE[24]. Respecte d'aquest projecte, el SEPD ha advertit en una carta adreçada al Comissari per l'Energia de la Comissió Europea que, si bé (el Projecte) no té un impacte directe en la protecció de dades, cal tenir present que les xarxes i comptadors intel·ligents "tenen una particular importància pels drets a la privacitat i la protecció de dades personals", per la qual cosa caldrà reflexionar a llarg termini.[25]

- Comunicació de la Comissió (...) sobre la Inversió en el desenvolupament de tecnologies amb baixa emissió de carboni (Pla EETE), i Comunicació de la Comissió (...) "Energia 2020. Estratègia per a una energia competitiva, sostenible i segura".[26]
La primera d'aquestes Comunicacions estableix que:

"2.2 Eficiencia energética – Iniciativa «Ciudades Inteligentes»

[24] COM (2011)370 final.
[25] www.edps.europa.eu
[26] Documents COM (2009) 519 final i COM (2010) 639 final, respectivament.

La eficiencia energética es la forma más sencilla y más barata de garantizar la reducción de las emisiones de CO2. En los sectores del transporte, la construcción y la industria, las oportunidades tecnológicas disponibles deberán convertirse en oportunidades comerciales.
Esta nueva iniciativa europea – Ciudades Inteligentes – tiene como finalidad crear las condiciones necesarias para poner en marcha la comercialización a gran escala de las tecnologías orientadas a mejorar la eficiencia energética.
La iniciativa apoyará a las ciudades ambiciosas y pioneras (por ejemplo, las ciudades del Pacto de los Alcaldes) que conviertan sus edificios, redes de energía y sistemas de transporte en edificios, redes y sistemas del futuro, demostrando conceptos y estrategias de transición hacia una economía con baja emisión de carbono. Las ciudades y regiones que participen tendrán que poner a prueba y demostrar que es factible ir más allá de los actuales objetivos energéticos y climáticos de la UE, – por ejemplo, tender a una reducción del 40 % de las emisiones de gases con efecto invernadero mediante una producción, distribución y uso de la energía sostenibles, antes de 2020.
Se calcula que la inversión pública y privada total que necesitará Europa en los próximos 10 años será de 11 000 millones de euros. De aquí al año 2020, la iniciativa «Ciudades Inteligentes» habrá situado a unas 25 o 30 ciudades europeas a la vanguardia de la transición hacia un futuro con baja emisión de carbono. Estas ciudades serán los centros a partir de los cuales las redes inteligentes, una nueva generación de edificios y las soluciones para el transporte con baja emisión de carbono, se convertirán en realidades a escala europea que transformarán nuestro sistema energético."

Però les xarxes intel·ligents no només s'implementen a través de comptadors intel·ligents a efectes de mesurar i controlar consums d'energia com gas, electricitat... entre d'altres, als domicilis dels ciutadans, sinó que es relacionen també de forma directa amb altres "experiències Smart City". Per exemple, els serveis telemàtics de "road pricing" (taxes per ús de carreteres o vies públiques), presenten similituds, als efectes que ens interessen en el nostre estudi, amb les xarxes i comptadors intel·ligents: ús de "medidors" (o comptadors) que s'instal·len en els vehicles que circulen per aquestes vies, o que s'instal·len en punts fixes, comunicació de dades (també personals) a un sistema central que les processarà, o els riscs per la privacitat i la protecció de dades.[27]

Smart data (Dades intel·ligents)

Vinculat amb la PbD ("privacy by design", a la que ens referirem més endavant abastament) i amb els seus postulats, s'estudia la possibilitat d'utilitzar la intel·ligència artificial per protegir la privacitat i els drets dels ciutadans, a través de les "dades intel·ligents", que es podrien "autoprotegir" en funció dels requeriments del propi

[27] Així s'explicita en l'Informe de 16.2.2011 del Grup d'Experts 2 del Grup especial sobre xarxes intel·ligents ("Smart Grids Task Force"), a què ens referirem amb més detall en l'apartat 4.2 del nostre Document.

interessat i titular de la informació personal tractada. Diversos autors parlen de tres components de les dades intel·ligents, que serien: assegurar les dades de les persones; fixar regles d'accés a les dades; respondre en conseqüència a peticions d'accés a aquesta informació (seguint les "instruccions" que hauria donat o predefinit el titular). D'alguna manera, es pretén que la dada intel·ligent pensi per sí mateixa, i prengui decisions en funció del nivell preestablert d'autoprotecció.

El desenvolupament de les "smart data", força treballat en el plànol teòric[28], té una possibilitat d'aplicació pràctica en molts aspectes del tractament de dades personals[29]. Sobretot, pensem, en l'àmbit de les dades tractades per un tercer a través de pàgines web o Internet, per exemple (en què es donaria potser certa possibilitat de control a l'usuari, fins i tot en front de les condicions de tractament preestablertes pel responsable de la pàgina). En qualsevol cas, cal veure les connexions pràctiques que això podria tenir en aplicacions o experiències Smart City que impliquen una "cessió" de dades per part de l'usuari que vol (o "ha de") participar-hi.

Internet of things *"IoT"* (Internet de les coses o dels objectes).

El desenvolupament de les Smart Cities es vincula, com s'ha apuntat, amb les TIC. Dins d'aquesta vinculació, es pot establir una relació directa entre les Smart Cities i l'anomenat IoT, entès com la interconnexió en xarxa d'objectes d'ús quotidià. Diversos objectes d'us quotidià (telèfons mòbils, llibres, electrodomèstics, vehicles, roba, aliments, mobiliari urbà, etc), poden complir diferents "funcions", si se'ls dota de suficient capacitat (amb sensors de diferents tipus, etiquetes de radiofreqüència -tecnologia d'identificació per radiofreqüència o RFID-, NFC -*Near Field Communication,* és a dir, comunicació de camp proper-, codis de barres, etc, a les que anirem fent referència en aquest Document de Treball). Els exemples són molt diversos, com ara accedir a informació addicional sobre els productes que volem comprar –caducitat, procedència...-, o sobre l'estat del trànsit o la situació d'un mitjà de

[28] "Smart Data: The Need, the Goal, the Challenge" AA.VV. Universitat de Toronto, març de 2012; "Smart Data: Make the data "think" for itself. Data protection for the 21st century". AA.VV. Ambdós textos disponibles a: www.ipsi.utoronto.ca.

[29] De la mateixa manera que, pensem, caldria estudiar possibles interaccions entre el desenvolupament d'experiències Smart Cities i la utilització cada vegada més sovintejada del "Cloud Computing". Sobre això, sens perjudici d'aprofundir-hi més endavant, ens remetem al document del Grup de Treball de l'Article 29, citat: "Opinion 5/2012 on Cloud Computing".

transport determinat, sistemes de medició d'energia, control d'electrodomèstics a distància, localització de vehicles, etc.

La utilització d'aquests "objectes intel·ligents" en el marc de les Smart Cities obre un ventall de possibilitats enorme, i així s'ha posat de manifest des de les autoritats europees.[30]

Com s'explica en la nota de premsa sobre la consulta pública (juliol 2012) de la Comissió Europea sobre la IoT [31]:

"Son numerosos los ejemplos de esta evolución de los dispositivos en red: un automóvil podría informar sobre el estado de sus diferentes subsistemas, de tal modo que pueda hacerse un diagnóstico y una reparación a distancia mediante sensores de comunicación integrados; las personas en desplazamiento podrían recibir en sus teléfonos inteligentes información sobre el estado de la puerta de entrada o las persianas de su domicilio, o incluso el contenido del frigorífico, gracias a sensores instalados en sus hogares; un automóvil podría dar indicaciones sobre cómo sortear un atasco; dispositivos personales podrían transmitir a una central información actualizada sobre el estado de pacientes que reciben asistencia sanitaria a distancia."

Segons la Comissió Europea en la seva Comunicació de 18.6.2009:

"La conexión entre los objetos se efectúa habitualmente asignándoles un identificador y un medio para que se conecten a otros objetos o a la red. La cantidad de información en el mismo objeto suele ser limitada, y el resto reside en algún otro lugar de la red. En otras palabras: acceder a la información sobre un objeto implica establecer una comunicación en red. Se plantean las siguientes preguntas inmediatas:

– ¿Cómo está estructurada esta identificación? (denominación del objeto)
– ¿Quién asigna el identificador? (autoridad responsable de la asignación)
– ¿Cómo y dónde puede obtenerse información adicional sobre el objeto, incluida su historia? (mecanismo de direccionamiento y depósito de información)
– ¿Cómo se garantiza la seguridad de la información?
– ¿Qué partes interesadas son responsables de cada una de las cuestiones anteriores y cuál es el mecanismo de rendición de cuentas?
– ¿Qué marco ético y jurídico se aplica a las diferentes partes interesadas?

Los sistemas de IO que no hayan tratado adecuadamente estas cuestiones podrían acarrear graves consecuencias negativas, como las siguientes:
– El mal tratamiento de la información podría dar lugar a la revelación de datos personales o comprometer la confidencialidad de datos empresariales."

[30] Són d'especial interès la Resolució del Parlament Europeu, de 15 de juny de 2010, "Internet de los objetos" (DOUE C236 E/24, de 12.8.2011), així com la Comunicació de la Comissió al Parlament Europeu, al Consell, al Comitè Econòmic i Social Europeu i al Comitè de les Regions "Internet de los objetos-Un plan de acción para Europa", COM (2009) 278 final, de 18.6.2009. També cal tenir en compte la Resolució del Parlament Europeu de 15.6.2010, sobre la Internet de los Objetos, DOUE C/236, de 12.8.2011.

[31] http://europa.eu/rapid/press-release_IP-12-360_es.htm. Els resultats encara no estan disponibles: http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=IoTGovernance

Partint de la premissa que la IoT s'aplicarà cada vegada més per al desenvolupament d'aplicacions i serveis municipals de les Smart Cities[32], i com es desprèn dels documents citats, i d'altres, caldrà fer especial atenció a qüestions com l'assegurament de la privacitat de les persones, l'aplicació de mesures de seguretat adequades, la confiança que el ciutadà–consumidor posarà en la utilització d'aquests sistemes, l'atribució de responsabilitats a efectes de la Directiva de protecció de dades de 1995 i altra normativa interna (LOPD), etc.

En aquest sentit (no només des de la perspectiva de la protecció de dades, lògicament), la Comissió Europea estableix a la Comunicació citada diverses línees d'acció. En una d'elles, la Comissió es remet expressament a les directrius establertes en la Recomanació de la Comissió de 12 de maig de 2009, sobre l'aplicació dels principis relatius a la protecció de dades i la intimitat en les aplicacions basades en identificació per radiofreqüència (RFID).[33]

Tant en aplicacions de RFID com en utilització de la IoT, es considera especialment rellevant que els Estats vetllin perquè els operadors facin avaluacions d'impacte sobre la protecció de dades i la intimitat (PIAs) que avaluïn, entre d'altres, si una aplicació en concret pot utilitzar-se per fer seguiment de les persones, per a quines funcions està prevista una aplicació concreta, qui es responsabilitza del seu ús, quines mesures de seguretat s'apliquen, com s'informa als ciutadans[34], etc.

Aquests i d'altres elements que conformarien les PIAs en el context de l'RFID o l'IoT, podrien ser en bona part aplicables al context d'altres exemples de les Smart Cities.

---

[32] De la web de l'Ajuntament de Santander: El proyecto de referencia en esta categoría es SmartSantander**,** que está desplegando 20.000 dispositivos IoT (*Internet of Things*), la mayor parte de ellos en el área urbana de Santander y sus alrededores. Las infraestructuras creadas permitirán validar nuevas alternativas tecnológicas, y evaluar de forma práctica servicios basados en la red desplegada para monitorizar lugares y servicios como los autobuses urbanos, los aparcamientos públicos, las playas y el puerto, los parques municipales, los servicios de recogida y tratamiento de basuras, etc

[33] DOUE L/122, de 16.5.2009.

[34] En aquest sentit la Recomanació citada, de 12.5.2009, es refereix a una "política de información concisa, exacta y fácil de comprender para cada una de sus aplicaciones", que haurà d'incloure, com a mínim, informació sobre la identitat i domicili dels operadors, la finalitat de l'aplicació, les dades tractades, si es controla la localització de les etiquetes, els riscos per a la privacitat, entre d'altres.

Tecnologies diverses: NFC, RFID, Geolocalització, Wireless sensor netwok:

La gran majoria d'experiències d'Smart City utilitzen les TIC i, en concret, tecnologies que, com es posa de manifest al llarg d'aquest Document de Treball, poden ser d'una enorme utilitat per al seu desenvolupament, però alhora fan necessari que s'avaluïn els riscos que presenten per a la privacitat i la protecció de dades.

S'ha fet referència a la tecnologia **NFC**, que podem traduir per "Comunicació de Camp Proper". Aquesta tecnologia s'utilitza en molts exemples de "targetes intel·ligents", que en moltes ciutats s'utilitza per finalitats de transport o turístiques (tipus "Oyster Card" a Londres, o l'Amsterdam Card[35]). S'utilitza també en les anomenades "smart tags", utilitzades en comerç, "targetes de proximitat" o "contactless", especialment utilitzades com a sistema de pagament, com ara per pagar un bitllet de transport públic, per exemple, a la ciutat de Hèlsinki[36]. Les targetes intel·ligents incorporen un xip NFC que emmagatzema certa informació, i quan és llegit per un lector NFC permet fer un anotació, carregar una despesa en un compte...). Als efectes que ens ocupen, es tractaria de conèixer en cada cas quina informació s'emmagatzema, i quines prevencions cal aplicar (transparència per a les persones usuàries, mesures de seguretat, protecció de la informació davant de pèrdues o robatoris, accessos previstos, etc).[37]

També cal fer referència a la tecnologia **RFID** (*Radio frequency identification*). Segons la Recomanació de la Comissió de 12.5.2009, sobre l'aplicació dels principis relatius a la protecció de dades i la intimitat en les aplicacions basades en la identificació per radiofreqüència, aquesta consisteix en:

"el uso de ondas electromagnéticas radiantes o del acoplamiento de campo reactivo en la porción del espectro correspondiente a las radiofrecuencias para comunicarse en ambas direcciones con una etiqueta a través de diversos sistemas de modulación y codificación a fin de leer unívocamente la identidad de una etiqueta de radiofrecuencia u otros datos almacenados en ella;

[35] https://oyster.tfl.gov.uk/oyster/entry.do; http://www.iamsterdam.com/. Sobre la NFC, també es pot trobar documentació a: www.nfc.forum.org.

[36] Veure: http://www.forumvirium.fi/en/news/helsinki-commuters-use-rfid-to-get-transit-updates-and-post-messages

[37] En relació amb la plena actualitat de l'aplicació de tecnologia NFC a les Smart Cities, veure la notícia "Barcelona instal·larà panells intel·ligents per interactuar amb els mòbils", a www.elperiodico.cat, de 4 de febrer de 2013.

«etiqueta RFID» o «etiqueta»: un dispositivo RFID con capacidad para producir una señal radioeléctrica o un dispositivo RFID que reacopla, retrodispersa o refleja (dependiendo del tipo de dispositivo) y modula una señal portadora procedente de un lector o grabador;"

La RFID no deixa de ser una tecnologia que permet la traçabilitat d'un objecte, animal o persona, que pot contenir determinada informació. Un camp en el que en els darrers anys s'ha utilitzat la RFID, tot i no formar part de l'Smart City, és el camp de la medicina i el tractament i l'assistència als pacients[38]. Un exemple de RFID en Smart Cities podria ser el de gestió de residus, a través de RFID integrada en contenidors d'escombraries o en productes de supermercats, de manera que es pot saber si un producte es diposita al contenidor adequat[39].

No sembla, a dia d'avui, que proliferin els exemples de RFID "associat a persones físiques" en l'àmbit de les Smart Cities. Ara bé, també és cert que una de les aplicacions esteses de RFID es refereixen al comerç (RFID en peces de vestir, objectes diversos...) i en termes amplis la millora de l'atenció al client en el comerç no deixa de ser un element "smart". En qualsevol cas, si en el futur prolifera l'ús de RFID en vinculació directa amb Smart Cities, caldria estar, des de la perspectiva de la protecció de dades, al que exposa la Recomanació de la Comissió de 12 de maig de 2009, citada (garantir que la indústria –en el nostre cas, les Smart Cities "autoritats i administracions públiques" i indústria implicada- elaboren les corresponents PIAs, informació i transparència suficient en l'ús de la RFID, seguiment i campanyes de sensibilització adequades, entre d'altres). També caldria tenir en compte els advertiments del Grup de l'Article 29 en el Dictamen 9/2011, de 11.2.2001, relatiu a la proposta revisada de la Indústria per a un marc d'avaluació de l'impacte sobre la protecció de dades i la intimitat en les aplicacions basades en RFID.

Pel que fa a la **Geolocalització**, és el conjunt de tecnologies que permeten el coneixement de la pròpia ubicació geogràfica. També denominada "georeferenciació", aquesta tecnologia permet el posicionament i defineix la localització d'un objecte o persona en un sistema de coordenades determinat. Entre els dispositius que permeten utilitzar la geolocalització, destaquen els telèfons intel·ligents que integren receptors de GPS (Global Positioning System, o Sistema de Posicionament Global), la utilització

[38] Un entre molts exemples: http://www.hidglobal.es/etiquetas-rfid-medicina
[39] Exemple extret de "SmartSantander".

dels quals és un element present en moltes experiències Smart City.[40] Les aplicacions de geolocalització permeten, a través de diversos dispositius, l'obtenció d'informació sobre la pròpia localització en temps real, així com la localització de diferents tipus d'informació en el mapa, amb total precisió.

Segons la citada "Guia de seguridad y privacidad de las herramientas de geolocalización", de l'Observatori INTECO, es poden distingir principalment tres categories d'usos comuns per a la geolocalització:

"1) La localización física de un objeto o individuo en un sistema de coordenadas (proceso de **georreferenciación**), para posteriormente acceder a información específica. Un ejemplo de esto sería la utilización de un sistema de navegación mediante GPS.

2) La búsqueda de información y su localización física en un sistema de coordenadas (proceso de **geocodificación**). Un ejemplo de esto sería la utilización de un servicio de mapas para buscar museos en una ciudad determinada.

3) La adición de información geográfica a un contenido generado (proceso de **geoetiquetado**), usualmente como paso posterior a un proceso de georreferenciación. Un ejemplo de esto sería la creación de una fotografía, incluyendo en sus metadatos las coordenadas del lugar en que fue tomada. "

En definitiva, la geolocalització ens permet usos com ara localitzar llocs que volem visitar en una determinada ciutat, mantenir i consultar un registre històric de llocs que hem visitat o sobre els que hem fet alguna consulta, o mantenir una agenda de llocs recomanats en funció dels nostres interessos o aficions. De fet, ja es troben al mercat diverses Apps disponibles per disposar d'aquests i altres serveis[41].

Des de la perspectiva de la protecció de dades, en el mateix informe d'INTECO s'apunta que:

"La extensión de estas tecnologías y su demanda, no obstante, lleva asociada la problemática de la naturaleza de la información – frecuentemente privada o sensible – asociada a ellas. Por ello, es importante tomar especial conciencia de los aspectos relacionados con la seguridad y la privacidad, de forma que sea posible ejercer un uso responsable de las herramientas de geolocalización, y asegurar su pleno disfrute."

[40] Informació extreta de l'Informe: "Guia de seguridad y privacidad de las herramientas de geolocalización": Observatorio INTECO, març de 2011.
[41] Exemples extrets de: http://bitelia.com/2012/11/geolocalizacion-usos-utiles

Per exemple, a través de geolocalització (georreferenciació) es pot comprovar la localització física d'una persona amb un telèfon mòbil, i accedir a informació específica vinculada amb aquesta persona. També es permet l'addició d'informació de geolocalització a un determinat contingut, com podria ser una fotografia. Aquest procés de "geoetiquetat" podria permetre disposar d'informació –metadades-, com ara el lloc o l'hora en què va ser presa la fotografia, amb la qual cosa es podria localitzar determinats individus sense, podem imaginar, el seu coneixement (o situar-los en un lloc i hora determinats). Això s'ha de tenir en compte, entre d'altres, des de la perspectiva del deure d'informar els usuaris d'uns determinada aplicació Smart City que utilitzi geolocalització, de la informació que, sense saber-ho, el propi individu pot estar generant i posant a disposició de tercers.[42]

Aplicat a les Smart Cities, la geolocalització podria permetre la localització de vehicles, llocs d'interès turístic, equipaments o mobiliari urbà, i fins i tot persones. Les aplicacions, doncs, són moltes. Com apunta el Grup de l'Article 29 en el seu Dictamen 13/2011, sobre serveis de geolocalització en els dispositius mòbils intel·ligents:

"El valor de la información aumenta cuando está ligada a una localización y toda localización puede ligarse a cualquier tipo de información: datos financieros, de salud, o sobre el comportamiento de los consumidores."

La vinculació és clara amb exemples d'Smart Cities: mapes de navegació, serveis geogràfics personalitzats (punts d'interès a una ciutat) control de persones (malalts, víctimes i agressors en casos de violència de gènere, com a mesura cautelar en àmbit penal o per a persones que compleixen una condemna, menors...) rastreig de persones o llocs, sistemes electrònics de venda de bitllets, "teletacs" i peatges, geolocalització d'adreces IP.... amb tot el que això podria comportar, no ho oblidem, de creació de perfils. Novament, algunes qüestions que afecten principis de protecció de dades han de ser objecte de reflexió: avaluar que cal el consentiment de l'nteressat, com a punt de partida, informar adequadament, fixar clarament els "límits" d'ús de la geolocalització, definir molt bé les responsabilitats (operadors, gestors, ajuntaments, empreses instal.ladores dels dispositius en vehicles, per exemple...). Entre d'altres qüestions, ens sembla interessant l'apunt del Dictamen 13/2011, citat, en el sentit

[42] Recordem, en aquest sentit, l'especial preocupació que ha tingut des de la perspectiva de la protecció de dades la utilització d'algunes aplicacions d'imatges i geoetiquetat com Google Street View, exemple citat, juntament amb d'altres (Panoramio o Flickr Maps), en l'informe d'INTECO, esmentat.

d'afavorir les bones pràctiques que portin a la utilització de tecnologies de protecció de la intimitat (Privacy enhancing technologies o "PET") adreçat als proveïdors d'aplicacions de geolocalització, cosa que ens sembla plenament aplicable a les experiències Smart Cities que utilitzen aquesta tecnologia:

"La aplicación que desee utilizar datos de geolocalización informará claramente al usuario sobre los fines para los que quiere utilizarlos y solicitará su consentimiento inequívoco para cada una de las posibles finalidades distintas. El usuario elegirá activamente el nivel de la geolocalización (por ejemplo, a escala de un país, ciudad, código postal o con la mayor precisión posible). Una vez que el servicio de localización se active, un icono estará permanentemente visible en cada pantalla indicando dicha activación. El usuario podrá retirar su consentimiento en cualquier momento y sin tener que abandonar la aplicación y también podrá suprimir, fácil y permanentemente, cualquier dato de localización almacenado en el dispositivo."

Com s'ha apuntat, hi ha un potencial risc per la privacitat de les persones, a arrel de la utilització de dispositius de geolocalització. D'entrada, tot i que sembli una obvietat, pel mer fet de l'increment de la posada a disposició dels usuaris d'aquestes aplicacions. El fet que les aplicacions de geolocalització tractin dades de posició georreferenciada d'una persona, pot portar al coneixement per part de tercers dels itineraris, consums, desplaçaments, horaris, relacions socials, hàbits d'oci o lleure, etc, d'aquest usuari. Des d'aquesta perspectiva, el propi usuari es podria estar convertint, sense ser-ne gaire conscient, en un "distribuïdor" de la seva pròpia informació personal, fent-la accessible a tercers. Tornem a citar com a exemple les "fotografies georeferenciades": si hi ha un traspàs, volgut o no, d'aquesta informació, un nombre indeterminat –i probablement ampli de tercers- podria accedir a aquesta informació. Així, una foto captada amb un smartphone pot ser codificada amb paràmetres de latitud i longitud, i quan l'usuari envia la foto online, pot estar exposant més dades personals de les que imagina[43].

També podem imaginar com a exemples de futur la complementació de sistemes actuals de "teletacs", pagament de peatges o serveis de lloguer de bicicletes amb algun dispositiu instal·lat als vehicles o bicicletes, que permetés la seva

[43] Així s'apunta en els articles disponibles a: www.tendencias21.net: "La geolocalización de los smartphones amenaza la privacidad", i "La geolocalización a través del móbil, nuevo mercado emergente".

geolocalització. En el cas que això es portés a la pràctica (cosa que, d'entrada, caldria fonamentar en una finalitat legítima i, entenem, en el consentiment de l'usuari), el risc potencial per la privacitat sembla inqüestionable. Tot i que és un simple exemple de futur, cabria plantejar-se la proporcionalitat de poder localitzar en tot moment una bicicleta de lloguer, per exemple, per evitar pèrdues o robatoris, si això implica directa o indirectament un tractament de les dades (i una geolocalització) de l'usuari que en fa ús en un determinat moment.

Tot això, en definitiva, planteja reptes des de la perspectiva de la privacitat i la protecció de dades personals. Entre d'altres, caldrà fer atenció als riscos que pot suposar la manca (o insuficiència) de mesures tècniques de seguretat prou robustes per protegir la informació, la utilització d'informació amb finalitats de "profiling" sense coneixement ni consentiment de l'interessat per a finalitats de màrqueting o publicitat, etc. L'ús d'aquesta tecnologia en el context que ens ocupa haurà de ser analitzat des de la perspectiva dels diferents principis de protecció de dades.

Respecte la **Wireless sensor network** *(X*arxes de sensors sense fils), és una altra tecnologia que també podem relacionar directament amb el desenvolupament d'Smart Cities[44]. Es tracta de crear una xarxa distribuïda de nodes de sensors que poden mesurar diversos paràmetres d'interès per a una gestió més eficient de la ciutat. Totes aquestes dades s'envien sense fils i en temps real als ciutadans o a les autoritats competents.

Per exemple, a través de sistemes de monitorització, els ciutadans poden conèixer la concentració de la contaminació en cada carrer de la ciutat o poden obtenir alertes al seu mòbil o d'altres dispositius sobre nivells de contaminació. També permet optimitzar el reg de parcs i la il·luminació dels carrers. Es poden obtenir informacions i alertes sobre fuites d'aigua, mapes de soroll o de contaminació per zones, etc. Fins i tot, els contenidors d'escombraries poden enviar, mitjançant una xarxa de sensor, una alerta quan estan a punt d'omplir-se. La utilització d'aquests sensors també pot permetre, en el context de les Smart Cities, controlar el trànsit, rebre informació de llocs d'aparcament, etc.

[44] Informació obtinguda de: http://www.libelium.com/smart_cities.

A títol d'exemple, citem la ciutat de Santander, com una de les "pioneres" en la utilització de sensors (es preveu el desplegament de 20.000 dispositius per poder transmetre informació útil als usuaris). Aquesta ciutat forma part, junt amb altres tres ciutats (Guilford, Lübeck i Belgrat)[45], d'un projecte de desenvolupament d'Smart Cities a través de xarxes de sensors. Aquest és un Projecte aprovat per la Comissió Europea en el 7è Programa Marc d'Investigació (7PM), concretament, en l'àmbit de l'Internet del futur.[46]

Open data

Les "dades obertes", enteses com "tota la informació que els organismes públics (...) generen, recullen o sufraguen"[47] que posteriorment es difon i es posa a disposició de la ciutadania, suposen un flux informatiu important que s'ha incrementat considerablement en els darrers anys. Posem com a exemples la informació geogràfica, estadístiques, informació meteorològica, dades procedents d'investigacions finançades amb fons públics, o llibres digitalitzats en biblioteques públiques, entre d'altres. Els experts apunten la tendència cap a un tractament progressiu de quantitats ingents d'informació oberta, és a dir, de "Big data" [48], concepte que es refereix als arxius o conjunt de dades el contingut dels quals supera o excedeix la capacitat de les eines habituals de software per a recollir, emmagatzemar, tractar i analitzar informació.[49]

El potencial de la utilització d'informació oberta per al desenvolupament i implantació d'experiències d'Smart Citiy és clar. A banda dels exemples citats, que podem relacionar clarament amb els eixos propis de les Smart Cities, en trobem d'altres, com ara la utilització d'aplicacions ("Apps"[50]) que els ciutadans poden descarregar-se en

[45] Es pot trobar informació completa sobre aquest Projecte en les quatre ciutats citades a: http://www.smartsantander.eu; http://cordis.europa.eu; http://portal.ayto-santander.es.
[46] Decisió núm. 1982/2006/CE del Parlament Europeu i del Consell (DOUE L 412, de 30.12.2006).
[47] Comunicació de la Comissió al Parlament Europeu (...) "Datos abiertos. Un motor para la innovación, el crecimiento y la gobernanza transparente" (COM (2011) 882 final).
[48] "Big Data for Smart Cities: How do we go from open data to big data for smart cities". www.smartcities.es/tag/open-data.
[49] Segons el McKinsey Global Institute, a "Big data: The next frontier for innovation, competition and productivity" (www.mckinsey.com).
[50] Respecte diverses qüestions relacionades amb la privacitat en el disseny d'Apps per a telèfons mòbils, ens remetem al document: "Mobile Privacy Disclosures. Building Trust Through

dispositius mòbils per obtenir informació molt diversa (estat del trànsit, contaminació, qüestions mediambientals, meteorologia, transports, turisme...), etc.

Com es posa de manifest des de la Unió Europea[51], la "informació oberta" comporta importants possibilitats de reutilització d'aquesta informació en nous productes i serveis, així com importants possibilitats de millora de l'eficiència de les administracions públiques. La reutilització d'informació, la transparència i la millora de la gestió pública són, doncs, les aplicacions fonamentals de la informació oberta. [52]

Hi ha diverses normes que podem relacionar amb les dades obertes, amb la difusió d'informació per part del sector públic i, en definitiva, amb l'accés per part dels ciutadans a aquesta informació. A nivell estatal, caldria tenir en compte les previsions de la Llei estatal 11/2007,de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, que remet a les previsions de la LOPD, en allò que afecta al tractament de dades personals[53]. Pel que fa a Catalunya, cal tenir present la Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya, que té per finalitat, entre d'altres, garantir que l'ús dels mitjans electrònics promogui una administració pública oberta, transparent, accessible, eficaç i eficient (article 3.a) de la llei citada). Per l'especial afectació que pot suposar per a la difusió d'informació del sector públic, també cal tenir present l'esborrany del Projecte de llei de transparència, accés a la informació pública i bon govern, actualment en procés de tramitació al Congrés dels Diputats[54]. Pel que fa a la reutilització de la informació del sector públic,

---

Transparency", de la Federal Trade Commission (FTC), USA, de febrer de 2013 (http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf).

[51] En la Comunicació de la Comissió Europea, citada.

[52] De la Comunicació de la Comissió Europea, citada: "El impulso hacia la utilización de datos abiertos está cobrando fuerza en varios Estados miembros, los cuales están adoptando este concepto por razones de transparencia, eficiencia administrativa y potencial económico de la reutilización.(...). El Reino Unido ha creado el portal data.gov.uk que reúne información procedente de organizaciones gubernamentales a todos los niveles. Otros Estados miembros están creando portales similares, por ejemplo Francia a través de ETALAB. Los portales de datos también existen a nivel regional, como dadesobertes.gencat.cat en Cataluña y dati.piemonte.it en Piamonte, Italia."

[53] Una de les finalitats de la Llei 11/2007 és: "Crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos" (art. 3.3).

[54] Segons el Projecte de Llei: "Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 11 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 12. A este respecto, cuando la

a nivell estatal ens hem de referir a la Llei 37/2007, de 16 de novembre, que preveu expressament que la reutilització de documents que continguin dades de caràcter personal es regirà per la LOPD (article 4.6).

Des de la perspectiva de la protecció de dades interessa subratllar que part de la informació "oberta" que posteriorment és objecte d'accés públic o de reutilització, por ser o haver estat, en origen, dada personal. La normativa esmentada és conscient d'això i, com s'ha apuntat, inclou referències i remissions a la normativa de protecció de dades. En aquest sentit, i en relació amb el procés de revisió actualment obert en relació amb la normativa europea sobre reutilització d'informació pública el SEPD, ha considerat que cal establir clarament l'aplicabilitat d'aquesta Directiva a les dades personals, i exigir als organismes del sector públic una avaluació de qualsevol informació del sector públic que inclogui dades personals que puguin estar disponibles per a la seva reutilització[55].

Per tot l'apuntat, no s'hauria de donar per fet que la "informació oberta" i la informació reutilitzable és innòcua per a la privacitat dels ciutadans. En el marc de les Smart Cities es podria donar el cas, per exemple, d'informació oberta que en principi no afecta persones concretes, però que si es sotmet a un procés de "data mining" (mineria de dades), o si es refereix a un barri molt concret d'una ciutat, es pot arribar a relacionar amb persones concretes sense esforços desproporcionats. Això fa que sigui necessari vetllar adequadament per la privacitat, i analitzar la normativa citada, en relació amb les Smart Cities, des de la perspectiva de la protecció de dades personals.

Profiling (creació de perfils): El desenvolupament de les Smart Cities pot comportar, al menys parcialment, la creació de perfils de consumidors (*consumer profiling*) i d'usuaris de diferents prestacions, productes o serveis oferts –independentment que els ofereixi un Ajuntament o la companyia subministradora d'algun d'aquests serveis-.

información contuviera datos especialmente protegidos, la publicidad solo se llevará a cabo previa disociación de los mismos." (art. 4.3). (BOCCGG Serie A, núm. 19-1, de 7.9.2012).

[55] Veure el Projecte de Directiva de modificació de la Directiva 2003/98/CE relativa a la reutilització de la informació del sector públic (COM (2011) 877 final). Respecte aquest Projecte, destaquem les consideracions del Dictamen del Comitè Econòmic i Social Europeu (DOUE C 191, de 29.6.2012), i especialment del Dictamen del SEPD, de 18.4.2012.

Des de fa anys els actors en matèria de protecció de dades (Autoritats de protecció de dades, organismes de la UE i el Consell d'Europa, els propis Estats...) han posat de manifest que el "profiling" pot representar un risc gens menyspreable per a la protecció de dades i la privacitat.[56]

El "tractament" que suposa fer un perfil de les persones, té unes connotacions que han preocupat, tradicionalment, els operadors de la protecció de dades. El Projecte de Reglament de protecció de dades de la UE, fa especial atenció de la creació de perfils, i de com pot afectar els drets del ciutadà, i deixa clar que s'ha de reforçar el dret d'accés a la pròpia informació i a ser informat adequadament, especialment quan un tractament es basa en elaboració de perfils (entre d'altres, Considerants 21 i 51). L'article 21.2 del Projecte de Reglament UE disposa, entre d'altres, que:

"A reserva de las demás disposiciones del presente Reglamento, una persona solo podrá ser objeto de una medida del tipo contemplado en el apartado 1 (relatiu a l'avaluació per perfils) si el tratamiento:

a) se lleva a cabo en el marco de la celebración o la ejecución de un contrato, cuando la solicitud de celebración o ejecución del contrato presentada por el interesado haya sido satisfecha o se hayan invocado medidas adecuadas para salvaguardar los intereses legítimos del interesado, como el derecho a obtener una intervención humana; o

b) está expresamente autorizado por el Derecho de la Unión o de un Estado miembro que establezca igualmente medidas adecuadas para salvaguardar los intereses legítimos del interesado; o

c) se basa en el consentimiento del interesado, a reserva de las condiciones establecidas en el artículo 7 y de garantías adecuadas.
(...)."

A través de títols de transport intel·ligents (amb tecnologia NFC, per exemple), per utilitzar determinat transport públic urbà, o a través de la informació relativa al consum d'energia en un domicili, es pot fer perfils de desplaçaments, hàbits, costums d'una persona, o fins i tot de qüestions com ara quantes persones poden viure en un domicili, quins horaris fan, forma de vida etc..

Sobre això, ens sembla especialment rellevant tenir en compte la Recomanació CM/Rec (2010)13, del Comitè de Ministres del Consell d'Europa, sobre la protecció de

[56] Prova de la preocupació per aquest tema, és la "Uruguay Declaration on profiling", de la darrera 34ª Conferència Int. d'Autoritats de Protecció de dades i Privacitat, en la que s'afirma, entre d'altres, que per crear confiança, les entitats públiques i privades han d'assegurar que informen a la societat, de la manera més extensa possible, de les seves operacions de creació de perfils.

les persones respecte el tractament automatitzat de dades de caràcter personal en el context de la creació de perfils[57], que fa referència, específicament, a algunes de les tecnologies que comentem (RFID, geolocalització...), en els següents termes:

"Tomando nota de que esta recopilación y tratamiento pueden tener lugar en diferentes situaciones con diferentes fines y hacer referencia a diferentes tipos de datos, tales como datos sobre el tráfico y las preguntas de los usuarios de Internet; datos sobre los hábitos de compra, actividades, estilo de vida y comportamiento de los usuarios de los dispositivos de telecomunicaciones, incluidos datos de localización geográfica, así como datos provenientes en particular de las redes sociales, los sistemas de videovigilancia, los sistemas biométricos y los sistemas de identificación por radiofrecuencia (RFID) que prefiguran la "Internet de los objetos"; tomando nota de que conviene evaluar las diferentes situaciones y objetivos de una forma diferenciada;"

Per això, ens sembla especialment important que, en matèria de "profiling", com una eina vinculada al desenvolupament d'experiències Smart City, es tinguin en compte els límits legals que la normativa (actual i futura) imposa, a banda dels advertiments i recomanacions existents.

D'aquesta interessant Recomanació del Consell d'Europa, podem extraure elements útils per al nostre estudi, en el context de les Smart Cities: entre d'altres, que cal que els Estats posin mitjans per evitar la "invisibilitat" de la creació de perfils (per exemple, quan un usuari d'un comptador intel·ligent, o d'un títol de transport intel·ligent, desconeix que "algú" analitzarà els seus desplaçaments, o les hores de major consum energètic, i en farà un ús també desconegut); la necessitat de preservar les "esferes de vida diferents i independents de cada persona", en el sentit que, per exemple, per poder utilitzar Apps d'Smart City per gaudir de determinats serveis a la seva ciutat, una persona pugui "controlar" quina informació dóna, pugui utilitzar fins i tot una "identitat" pròpia però diferent a la utilitzada en altres serveis, o que no se li exigeixi més informació de la deguda (principi de qualitat); que cal preservar els menors d'edat de mesures de "profiling", i també la utilització de dades sensibles en aquest context.

En definitiva, dins del concepte d'Smart City hi tenen cabuda un seguit de conceptes i tecnologies que han de ser objecte d'atenció especial, en base als principis de protecció de dades. Singularment, el principi de minimització, així com la promoció d'un correcte disseny des de la privacitat, i de la utilització de tècniques favorables a la

[57] http://conventions.coe.int

privacitat o PET ("Privacy Enhancing Technologies")[58], a les que també ens referim en aquest estudi, que poden permetre, per exemple, utilitzar tècniques d'anonimització o la pesudoanonimització en determinades experiències Smart City, o en relació amb determinats accessos (per exemple, podria ser legítim que una empresa aliena a la prestació del servei d'energia elèctrica faci perfils de consum dels usuaris, si ho fa amb informació anonimitzada o utilitzant prototips o "personas", salvant així la privacitat dels consumidors[59]).

L'aplicació d'aquestes i d'altres tecnologies als "productes i serveis" que les Smart Cities ofereixen al ciutadà, comporta necessàriament, des de la perspectiva de la protecció de dades, no només aplicar els principis de la normativa de protecció de dades (consentiment, informació adequada als afectats, exercici de drets, etc...) sinó en bona part "repensar" alguns d'aquests principis, o com a mínim, aplicar-los de manera que es tinguin en compte les característiques específiques de les dites tecnologies.

Com a exemple d'aquesta consideració general, citem el que s'anomena com el "dret al silenci dels xips" [60]. Aquest "dret" implicaria que una persona ha de poder abstraure's, "desconnectar-se" -"oposar-se", en terminologia LOPD-, de la utilització d'aquestes tecnologies, i de l'ús de les seves dades a través d'aquestes tecnologies. En definitiva, aquest dret ha d'aportar capacitació i control a l'usuari. Aquesta consideració, que en termes abstractes és clara, cal veure fins a quin punt es pot respectar en termes pràctics: podrà un ciutadà reclamar el seu dret al "silenci dels xips", i per tant negar-se a que les seves dades siguin utilitzades en relació amb la prestació d'un servei, sense haver de renunciar a la utilització d'aquest servei? Si es vincula el subministrament de gas o electricitat a la instal·lació al domicili de comptadors intel·ligents, quins efectes pot produir una denegació del consentiment de l'interessat? I en cas que la prestació del servei no requereixi el consentiment, quins

[58] Així es posa de manifest en el document de CRID (Centre de Recherches Informatiques et Droit) "Rapport sur les lacunes de la Convention nº 108 pour la protéction des personnes à l'égard du traitement automatisé des données à caràctère personnel face aux développements technologiques", disponible a la pàgina web del Consell d'Europa. Del mateix CRID, i en relació amb la creació de perfils, citem l'estudi "L'application de la Convention 108 au mécanisme de profilage", de varis autors, entre d'altres, Y. Poullet i J.M. Dinant.

[59] Fins i tot amb la utilització d'arquetips o "personas", concepte que comentem en l'apartat 3.1 del nostre estudi.

[60] Adam Greenfield: "Everyware: The Dawning Age of Ubiquitous Computing". Aquest concepte ha estat objecte d'atenció de la Comissió Europea en la Comunicació citada, de 18.6.2009. També s'hi refereix expressament el Parlament Europeu en la Resolució, citada, de 12.8.2011.

efectes pot tenir un exercici del dret d'oposició? En definitiva, és aquest "dret", simplement, una manifestació més del dret a l'autodeterminació informativa, o és quelcom nou, que cal definir adequadament?.

Serveixi aquesta referència, per il·lustrar que en el context de les Smart Cities i de l'ús d'aquestes i d'altres tecnologies, probablement caldrà formular qüestions relatives als principis i garanties de la normativa de protecció de dades des d'una perspectiva diferent a la "tradicional".

Un altre exemple il·lustratiu ens l'aporta el propi concepte de privacitat: cada vegada més autors analitzen el pas des de la privacitat cap a "les privacitats", en el sentit que cal repensar el concepte tradicional, en funció del que comporten les dites tecnologies.[61] És a dir, en l'entorn que examinem, els ciutadans deixen diferents rastres i traces, en funció del producte, aplicació o servei que volen utilitzar, comprar, etc. La persona no exposa la seva "personalitat" en bloc, sinó que podríem dir que pot gestionar "diverses personalitats". Aquest idea no és nova, ni neix a partir de la IoT, però sí que pot tenir aplicacions interessants en el context d'aquestes i d'altres tecnologies, relacionades amb les Smart Cities. Sens perjudici de futures aportacions i reflexions, d'entrada podríem considerar aquest concepte com una oportunitat –des de la perspectiva de la protecció de dades-, en el sentit de reforçar l'autodeterminació informativa, és a dir, que el ciutadà pugui gestionar els diferents nivells de privacitat a la seva conveniència, en funció d'un o altre entorn, servei, prestació... etc. (Si l'Ajuntament m'ofereix un servei, puc considerar acceptable que tracti més dades que les que voldrà tractar una companyia que em subministra per exemple l'electricitat? Podré decidir quin grau de privacitat exposo en cada cas, en funció de la confiança que em mereix el responsable, o en funció de la tecnologia utilitzada, o del suport utilitzat –telèfon, aparell subministrat pel responsable...-? Per contra, els responsables estaran disposats o fins i tot obligats a informar de manera "reforçada", és a dir, en el sentit que la possible mancança o "ignorància tecnològica" del ciutadà no minvi el seu control sobre la pròpia informació?).

[61] Recollim l'expressió "from privacy to privacies", utilitzada per R. Van Kranenburg a "The Internet of Things: A critique of ambient technology and the all-seeing network of RFID". http://www.theinternetofthings.eu

Tornem a recuperar en aquest punt el concepte de "personas" o arquetips que hem esmentat anteriorment. D'entrada, pot ser habitual la seva utilització per al disseny d'un exemple d'Smart City, sense haver de tractar dades personals (per exemple, si es tracta de dissenyar una App d'informació destinada a famílies que tenen fills menors, no seria necessari el tractament de dades personals si el grau de detall de l'arquetip inclou un perfil de comportament, de freqüència amb la que l'arquetip -un pare o mare amb fills menors- utilitzarà el servei, els seus objectius o interessos, les seves motivacions per utilitzar aquell servei, la seva capacitat o aptituds per entendre i utilitzar certes TIC o el propi servei que es vol oferir, etc.)

Però no només és en aquesta fase de disseny, probablement, que es podria plantejar utilitzar aquests arquetips, sinó també quan el servei Smart City ja està disponible per als ciutadans. Per exemple, el responsable del tractament de dades d'un ciutadà determinat que utilitza un servei, podria en un primer moment, legítimament, recollir i tractar un mínim de dades de la persona, per tal de donar-lo d'alta com a usuari d'un servei (de mobilitat urbana, d'informació turística, de subministrament d'un servei o producte...), però a partir d'aquí es podrien utilitzar arquetips per a gestionar d'altres finalitats o usos secundaris al servei, com ara avaluar el servei, incloure millores, oferir altres productes, realització de perfils de consum, etc. És a dir, a partir d'una primera recollida i tractament de les dades mínimes imprescindibles (ens remetem a les consideracions fetes en relació amb el principi de qualitat) a l'usuari se li podria atorgar un "arquetip" a través del qual es desenvoluparia la seva relació amb el responsable del servei Smart City. La utilització d'arquetips evitaria que, per a aquestes altres finalitats (que poden derivar de la "finalitat principal" que legítimament permet un tractament de dades) es tractessin dades personals, minimitzant el risc per als drets de l'afectat. Això evitaria problemes deguts a deficiències en la recollida del consentiment, en la informació que se li ha de prestar a l'interessat quan es tracten les seves dades, en l'aplicació de mesures de seguretat, etc., doncs realment no s'estarien afectant ni tractant dades personals dels usuaris d'aquell servei. Òbviament, aquesta solució implicaria protegir adequadament el vincle amb la identitat real del subjecte, és a dir, amb les dades personals utilitzades en un primer moment: o bé es trenca el vincle i la informació ja no és "dada personal" en absolut, o bé es manté el vincle degudament protegit. Una o altra opció dependrà de la finalitat perseguida. En definitiva, el que plantegem és que, en la línea del que és l'anonimització de dades personals per a

d'altres usos (sistema abastament emprat en molts contextos[62]), s'analitzi també la utilització d'arquetips com a alternativa a la utilització de dades personals, en diferents fases de desenvolupament i aplicació d'experiències Smart Cities.

En definitiva, estudiant les possibilitats que dóna, de cara a minimitzar el tractament de dades personals, el fet que una persona física "real i concreta" pugui pertànyer a un o altre arquetip, o fins i tot que una pugui formar part de diferents arquetips, es permetria a l'individu gestionar i controlar millor la seva relació amb administracions públiques, empreses prestadores de serveis Smart City, i, sobre tot -des de la perspectiva que ens interessa-, la informació personal que cedeix i que després serà tractada per tercers. Com dèiem, així com una persona física ha de tenir un cert marge d'actuació a l'hora d'utilitzar diverses identitats digitals (i això no deixa de ser una manifestació del dret a l'autodeterminació informativa), es podria avaluar la possibilitat que també pogués relacionar-se amb empreses o administracions suministradores d'exemples Smart City a través d'arquetips.

Relacionem aquesta qüestió amb la pràctica, especialment recomanable, d'utilitzar pseudònims, que pot suposar una major protecció de la informació personal en alguns contextos. La utilització d'un pseudònim, o de diversos (per relacionar-se amb diversos responsables o utilitzar diferents serveis), pot afavorir el control per part de l'usuari sobre la informació que dóna en cada cas, i la utilització que en faran altres. El pseudònim permetria establir una "barrera de protecció" de les dades personals i permet, al mateix temps, la relació individualitzada entre el responsable del servei o prestació Smart City i la persona física.[63]

4. L'APLICACIÓ DELS PRINCIPIS DE LA PROTECCIÓ DE DADES EN EL CONTEXT DE LES SMART CITIES

[62] El concepte d'anonimització és especialment rellevant en matèria de protecció de dades. Una prova més de la importància d'aquests conceptes, és que en "l'informe Albrecht" sobre el Projecte de Reglament UE (2012/2011 (COD), de 16.1.2013), es fan constants referències als conceptes d'anonimització i de pseudoanonimització.

[63] Prova de la importància de l'ús de pseudònims, és que en l'"Informe Albrecht" al Projecte de Reglament UE es presenta una esmena per introduir la definició d'aquest concepte en l'article 4 del Reglament, amb la següent redacció: ""pseudonym" means a unique identifier which is specific to one given context and which does not permit the direct identification of a natural person, but allows the singling out of a data subject". És a dir, el pseudònim permet establir una barrera de protecció de les dades personals, i permet la relació individualitzada entre el responsable del servei o prestació Smart City i la persona física.

En aquest apartat farem referència a un seguit de principis, presents tant en la normativa europea (Directiva de protecció de dades de 1995, principalment, sense oblidar el punt de partida que suposa per a la protecció de dades en el marc europeu el Conveni 108 del Consell d'Europa[64]) com en les normes estatals de regulació del dret a la protecció de dades (LOPD i RLOPD, en el nostre cas). El que interessa, més que no pas descriure aquests principis, prou definits en la dita normativa, és posar de manifest els punts que poden plantejar dubtes, problemes, o, com a mínim, que mereixen una reflexió, quan parlem d'Smart Cities.

Atès que al llarg d'aquest Document de Treball ja s'han anat apuntant algunes qüestions de reflexió, en part posades de manifest pels experts en protecció de dades en els documents consultats, per no ser redundants no insistirem en reflexions ja fetes.

D'entrada, convé deixar clar que bona part de les aplicacions de les Smart Cities no comporten un tractament de dades personals. Certament, quan ens referim als "eixos" de les Smart Cities, se'n deriven molts exemples, alguns dels quals no comporten tractament de dades de caràcter personal, entre d'altres:

Pantalles amb informació dinàmica en transports públics; aprofitament energètic en edificis intel·ligents; clústers empresarials (barris on es prioritza determinada activitat comercial o indústria); desenvolupament d'un barri amb energies sostenibles; aplicacions de mobilitat intel·ligent a través de TIC, per tal de fer-les més eficients (semàfors, vies urbanes, xarxes de transport...); informació del sector públic que, sense incloure dades personals, es reutilitza i es difon a través de diversos canals, i que es pot referir a l'estat del trànsit, meteorologia, contaminació per barris, localització d'equipaments culturals, entre d'altres.

Cal fer avinent que l'estudi dels supòsits o exemples d'Smart City que no impliquen cap tractament de dades personals és aliè a l'objecte d'aquest document. Dins d'aquest capítol -no afectació a informació personal- situem també, en principi, aquelles ciutats que, per tal de recollir informació mediambiental, per exemple, situen

[64] Convenció per a la protecció de les persones pel que fa al tractament automatitzat de dades de caràcter personal, feta a Estrasburg el 28 de gener de 1981 (BOE núm. 274, de 15.11.1985).

"nodes" o sensors en diferents punts de la ciutat. Evidentment, ens estem referint només al supòsit que aquestes tecnologies es facin servir només per captar "informació" (volum de trànsit, contaminació, llocs d'aparcament disponibles, etc.) i difondre-la al públic en general..., sense cap possibilitat de fer cap seguiment de persones (enregistrar matrícules de vehicles, seguiment de vehicles o persones, etc).[65] Per exemple, seria diferent que "s'anunciïn" llocs d'aparcament en un panell informatiu, que si una persona s'instal·la una "App" al seu ordinador o en d'altres dispositius per localitzar els llocs d'aparcament disponibles en una zona determinada; en aquest segon cas, com a mínim, hi pot haver un tractament de dades associades a la IP o a un número de telèfon. En qualsevol cas, cal tenir en compte les consideracions fetes en altres apartats d'aquest estudi, com ara les relatives al tractament de dades que pot generar l'IoT.

4.1 Principi de legitimitat i consentiment.

Qualsevol tractament de dades personals ha de resultar legítim, i per ser-ho, ha de donar correcte compliment als principis i obligacions establerts en la normativa de protecció de dades. El primer que cal plantejar-se, doncs, a l'hora de dur a terme una experiència d'Smart City que impliqui el tractament d'informació personal és si aquest resulta legítim, en base al que disposa la normativa sobre protecció de dades. En concret, l'article 7 de la Directiva de protecció de dades de 1995 configura els principis relatius a la legitimació del tractament de dades en els següents termes:

"Els Estats membres han d'establir que el tractament de dades personals només es podrà efectuar si:
a) l'interessat hi ha donat el consentiment de manera inequívoca,
b) és necessari per a l'execució d'un contracte en què l'interessat és una de les parts o per a l'aplicació de mesures pre-contractuals adoptades a petició de l'interessat, o
c) és necessari per al compliment d'una obligació jurídica a què estigui subjecte el responsable del tractament, o
d) és necessari per protegir l'interès vital de l'interessat, o
e) és necessari per al compliment d'una missió d'interès públic o inherent a l'exercici del poder públic conferit al responsable del tractament o a un tercer a qui es comuniquin les dades, o
f) és necessari per a la satisfacció de l'interès legítim que persegueix el responsable del tractament o la tercera o terceres persones a qui es comuniquin les dades, sempre que no prevalgui l'interès o els drets i llibertats fonamentals de l'interessat que requereixin protecció

[65] Dins d'aquesta "salvetat", posem de manifest que la videovigilància, present en els Smart Cities, evidentment pot comportar un tractament de dades personals. Ens remetem, sobre aquesta qüestió, a la normativa corresponent i la Instrucció 1/2009 d'aquesta Autoritat.

d'acord amb l'apartat 1 de l'article 1 d'aquesta directiva."

Des del moment que un exemple d'Smart City comporta un tractament de dades personals, cal analitzar si les dades es recullen per al compliment d'una finalitat legítima, i si aquesta recollida i el tractament posterior es fa d'una forma legítima. En concret, si es disposa del consentiment de les persones afectades, si escau.

Especialment caldrà analitzar de forma acurada la legitimitat per realitzar, legítimament, un determinat tractament de dades, en experiències Smart City que utilitzin o puguin arribar a utilitzar, ni que sigui potencialment, dades personals a les que la normativa de protecció de dades atorga un grau reforçat de protecció (article 7 LOPD i article 8 de la Directiva de protecció de dades de 1995). Citem (a banda d'altres exemples ja comentats, com ara la iniciativa E-call, gestió d'emergències, etc) a tall d'exemple, les experiències Smart City relacionades amb la mobilitat i utilització de transports públics per part de persones invidents[66]. A través de sensors de geolocalització i una brúixola, aquesta aplicació permet a les persones invidents saber on es troben i els facilita l'accés al transport públic. Ara bé, quines dades personals es recullen i tracten en experiències d'aquest tipus? Quin ús posterior se'n fa? Quines mesures de seguretat reforçades caldria plantejar en aquest cas? [67] Sense oblidar que, en aquests casos (aplicacions de localització de persones amb alzheimer) el correcte compliment del principi de consentiment també pot ser problemàtic, i incidir en la legitimitat del tractament de les dades personals corresponents.

L'article 6 de la LOPD configura el consentiment inequívoc del titular de les dades com l'eix que legitima un tractament de dades, llevat que la llei disposi una altra cosa, en definitiva, que es donin les circumstàncies legals que habiliten un tractament de dades sense haver de disposar del consentiment. Especialment, caldrà tenir en compte les previsions sobre diferents tipus de consentiment requerit, en funció de la informació personal tractada (art. 7 LOPD). Ara bé, tractant-se d'administracions públiques, que tenen encomanda per lleis la consecució de l'interès públic, la mateixa LOPD habilita

[66] Exemple extret de l'estudi de la Universitat d'Almería respecte la utilització d'una App que facilita l'accés a persones invidents als autobusos urbans. Font: http://cms.es/UAL.
[67] Es fan extensibles aquestes consideracions a d'altres exemples, com ara la investigació duta a terme per la Universitat Carlos III de Madrid sobre el desenvolupament de sistemes basats en localització per satèl·lit emprades per localitzar persones que pateixen alzheimer, o dones maltractades. Font: http://www.uc3m.es.

el tractament quan es tracti de "l'exercici de les funcions pròpies de les administracions públiques en l'àmbit de les seves competències" (art. 6.2).

En el context de les Smart City, podem trobar molts exemples i iniciatives que es duen a terme des del sector públic. En aquests casos, quan una Administració pública recull dades personals dels ciutadans per tractar-les en el context de l'exercici de les funcions que li són pròpies, caldria partir de la base que no seria necessari disposar del consentiment previ de l'afectat. El tractament pot ser legítim sense el consentiment previ dels afectats.

A tall d'exemple, citem la instal·lació de sistemes de geolocalització en vehicles de cossos policials, en serveis d'emergència (bombers...) o serveis de transport públic, com ara els autobusos o els taxis que circulen per una ciutat. En aquests casos, sempre que la instal·lació trobi la seva justificació en l'adequada prestació del propi servei (en el sentit que conèixer la situació i recorreguts de la flota de vehicles suposa la millora del propi servei –reducció de temps d'espera en víctimes d'accidents, millora en els temps d'atenció de trucades d'emergència...-, o bé perquè augmenta la seguretat dels propis treballadors[68] i de terceres persones, etc), podria resultar legítima una recollida i tractament de les dades sense consentiment. Per contra, altres supòsits d'utilització de la geolocalització a través de dispositius mòbils intel·ligents (com ara smartphones) o a través de targetes intel.ligents, de forma generalitzada per als usuaris d'un serveis públic, que sigui "prescindible", és a dir, no justificable en la pròpia prestació del servei o en l'exercici de la funció pròpia de l'Administració pública, podria requerir el consentiment previ dels afectats.

Podem trobar altres exemples en determinades mesures preses per una administració pública municipal *smart* per millorar el trànsit de vehicles a determinades zones de la ciutat (regulació i optimització del trànsit, estalvi d'energia, reducció d'accidents i de contaminació atmosfèrica...), les quals podrien no requerir el consentiment dels afectats, en cas de trobar-se el tractament suficientment emparat per previsions normatives que no facin necessari disposar del dit consentiment. Així, es podria

[68] Pel que fa estrictament a l'àmbit laboral, especialment, pel que fa a la problemàtica del consentiment com a fonament del tractament legítim de les dades dels treballadors, ens remetem a les consideracions fetes pel Grup de l'Article 29 en els Dictàmens 8/2001, sobre el tractament de dades en el context laboral, i el Dictamen 13/2011, sobre els serveis de geolocalització en dispositius mòbils intel·ligents).

considerar que en l'exemple de l'enregistrament de matrícules de vehicles per motius de seguretat difícilment podrà basar-se en el consentiment –sempre que hi hagi la suficient habilitació legal-, mentre que si la finalitat fos, per exemple, participar en un estudi sobre la circulació de determinats tipus de vehicles (per exemple, vehicles de baix consum, vehicles elèctrics... per una zona urbana determinada), pot ser qüestionable argumentar que un ciutadà hagi de suportar el tractament de la seva informació personal (i, potser, la creació de perfils) sense el seu consentiment.

En alguns supòsits el tractament s'haurà de dur a terme en base a l'existència del consentiment de les persones afectades, bé perquè es tracti de dades especialment protegides (dades relatives a la ideologia, creences, afiliació sindical, raça, salut o vida sexual) o per altres motius, com pugui ser l'especial afectació que el tractament pot implicar per a les dades del ciutadà. No hem d'oblidar en aquest sentit que el dret a al protecció de dades té un caràcter instrumental respecte a l'exercici d'altres drets de les persones, de manera que un tractament inadequat op excessiu pot acabar afectant altres drets o llibertats (dret de reunió, llibertat de circulació etc.)

Posem per exemple un projecte de gestió intel·ligent de la mobilitat urbana que impliqués la instal·lació en els vehicles de dispositius de seguiment o monitorització, per exemple, per detectar una situació de perill per a la conducció (somnolència del conductor, alteració del ritme cardíac...). Projectes com aquest podrien combinar això amb la instal·lació de sensors i càmeres intel·ligents instal·lats en la infraestructura viària –semàfors, interseccions...-, per gestionar i fer més àgil la circulació de vehicles a les ciutats, o fins i tot, en cas d'accident, activar trucades d'emergència –tipus E-Call, esmentat.[69] No sembla que en aquests casos, o similars, es pogués procedir al tractament de dades d'un usuari sense disposar del seu consentiment, pels motius indicats (tipus sensible de dades tractades i afectació a altres drets i llibertats de la persona afectada).

Quan calgui el consentiment aquest haurà de ser entenedor (o informat) i lliure (en els termes que ho ha plantejat el Grup de l'Article 29 en el seu Dictamen 15/2011 sobre la

[69] Exemple il·lustratiu, inspirat en el "Proyecto MARTA (Mobilidad y Automoción con Redes de Transporte Avanzada), citat en el document "Smart Cities: un primer paso hacia la internet de las cosas". Fund. Telefónica, Ariel, 2011. Veure, també, l'article: "El Proyecto MARTA permitirá la gestión más inteligente de la movilidad urbana", a www.idi.mineco.gob.es

definició del consentiment), i específic per a les diferents finalitats del tractament.[70] Les persones afectades han de conèixer de forma clara abans de donar el seu consentiment, les implicacions del tractament, D'altra banda, "el consentiment ha de ser lliure". Sobre això, caldrà reflexionar sobre si un ciutadà estarà de fet en disposició de consentir de forma lliure en relació amb una aplicació d'Smart City sense la qual no pugui gaudir d'un servei, com ara el subministrament d'energia, o sense la qual no pugui circular pel centre d'una ciutat.

Diverses ciutats europees han condicionat l'accés amb vehicles motoritzats a determinades zones, amb sistemes de "road princing". Per exemple, l'"Area C" de la ciutat de Milà[71], en la que s'estableix una reglamentació d'accés a determinats espais: determinats vehicles (elèctrics, motocicletes...) hi tenen accés lliure, mentre que la resta de vehicles estan supeditats a un pagament, i hi ha diferents tarifes, per exemple, per a residents a la zona o en funció del nombre de vegades que es circula per la zona. Aquest model, que és similar al d'altres ciutats, implica necessàriament un tractament de dades personals –per exemple, a efectes del pagament d'una taxa-, que no sembla que pugui dependre de la capacitat d'elecció del titular de les dades.

Altres exemples de prestació del consentiment que podrien resultar problemàtics, o que com a mínim poden ser objecte de debat, es refereixen al consentiment de menors que són "objecte" (més que no pas usuaris actius) d'aplicacions de geolocalització –Apps de control parental- que informen de forma continua sobre emissions d'alerta si el menor surt d'un perímetre determinat, o informant els pares a través d'Internet. En un sentit ampli, aquestes aplicacions, per bé que inicialment s'incardinen en una esfera merament privada, podrien arribar a posar-se a disposició en el context de les Smart City, com un servei, per exemple, que oferís una administració municipal. La privacitat del propi menor, i la discussió –fins i tot ètica- de l'excés de control en aquests casos hauria de ser tinguda en compte en aquest cas, tant des de la perspectiva de la legitimitat del propi tractament, com des de la perspectiva del principi de consentiment (prenent com a referència, sobre tot, la

[70] Com apunta el Grup de l'Article 29 en el seu Dictamen 13/2011, citat:
"El consentimiento debe ser específico para los diferentes fines para los que se procesen los datos, por ejemplo para elaborar perfiles y orientaciones de comportamiento. Si la finalidad del tratamiento de los datos cambia de forma sustancial, el responsable del tratamiento deberá obtener la renovación del consentimiento específico."

[71] http://www.comunemilano.it

frontera dels 14 anys que, en principi, marca la normativa en relació amb el consentiment dels menors). [72]

Cal ser conscients que el progressiu desenvolupament d'exemples d'Smart City ha de portar a una reflexió prèvia sobre la necessitat o no de disposar del consentiment de les persones afectades.

Finalment, i sens perjudici de l'anàlisi que requerirà cada cas concret, apuntem que, pel que fa a possibles comunicacions o cessions de dades (arts. 11 i 21 de la LOPD) en diverses experiències Smart City, un punt d'atenció fonamental serà avaluar en cada cas si es compta amb una norma amb rang de llei que habilita la comunicació o, per contra, cal disposar del consentiment de les persones afectades. El principi general de l'article 11 de la LOPD estableix que és necessari aquest consentiment a menys, bàsicament, que la cessió o comunicació de les dades estigui autoritzada en una llei (norma amb rang legal). Atès que en el context de les Smarts Cities ens trobarem amb molts supòsits de prestació de serveis per les administracions públiques (locals i supralocals), pel que fa a la comunicació de dades entre administracions públiques ens remetem a la previsió de l'article 21.1 de la LOPD[73].

4.2 Principi de finalitat.

Un primer tractament legítim no comporta que també ho sigui qualsevol altre tractament que es faci a partir d'aquella informació o qualsevol cessió de les dades a tercers, per a finalitats diferents[74]. El principi de legitimitat exigeix que les dades no siguin tractades per a finalitats "incompatibles" amb la finalitat legítima per a la qual van ser recollides. En el marc de les Smart Cities cal posar especial atenció, doncs, a que la legitimitat que permet un tractament per part d'un ajuntament, per exemple, o d'una empresa que subministra un determinat servei, no suposa "en cascada" la

[72] Tot i que probablement ja s'escapa més del context Smart City, també és interessant plantejar-se els problemes referits al consentiment dels treballadors quan és una empresa la que utilitza geolocalització, per exemple, dels vehicles. Al respecte, ens remetem als comentaris fets en el Dictamen 13/2011, del Grup de Treball de l'Article 29.

[73] "Les dades de caràcter personal recollides o elaborades per les administracions públiques per a l'exercici de les seves atribucions no han de ser comunicades a altres administracions públiques per a l'exercici de competències diferents o de competències que tractin matèries diferents, excepte quan la comunicació tingui com a objecte el tractament posterior de les dades amb finalitats històriques, estadístiques o científiques."

[74] Tal com ha posat de manifest el Tribunal Constitucional en la STC 292/2000 (F.J.13).

legitimitat per a tractaments secundaris, que potser no són necessaris o, simplement, no són volguts per l'interessat.

En el terreny dels comptadors intel·ligents, cal pensar que s'estaran obtenint i tractant dades que afecten a un nucli familiar, a l'interior d'un domicili, amb tot el que això té d'afectació per la privacitat. Cal analitzar l'habilitació per utilitzar aquesta informació amb finalitats diferents de la principal[75]. Per exemple, que l'empresa que subministra el servei disposi d'habilitació, no implica que aquesta habilitació s'estengui a finalitats o usos derivats de la principal (com ara per fer estudis de qualitat, creació de perfils de consum, oferir serveis relacionats amb el subministrament d'altres energies, "serveis de valor afegit", cedir les dades a d'altres empreses...). L'empresa prestadora del servei pot tenir habilitació per recollir i tractar dades per al subministrament, facturació o manteniment del servei, controlar impagaments o fraus, però això no legitima qualsevol altre tractament de dades.

Encara en relació amb el tractament de dades per a finalitats legítimes, podem posar altres exemples: una ciutat implanta un sistema de seguretat i videovigilància per tal de millorar la seguretat viària i ciutadana, a través del qual es poden enregistrar les matrícules dels vehicles que circulen per determinades zones. El sistema permet la lectura automàtica de matrícules així com la identificació de la marca, model i color dels vehicles. La tecnologia emprada també ofereix la possibilitat de creuar les dades obtingudes dels vehicles amb bases de dades policials, a fi de detectar vehicles "sospitosos", per exemple, d'haver estat robats o de trobar-se relacionats amb la comissió d'algun delicte. A partir de l'exemple que proposem[76], i des de la perspectiva del principi de legitimitat que examinem, podem formular les següents qüestions: quina és la finalitat legítima prevista? Si ho és la mera regulació del trànsit (prioritzar determinades vies d'accés a la ciutat, per exemple, o estudiar quin itinerari és més recomanable en hores punta en una zona amb alta densitat de centres escolars), no sembla que el tractament per a finalitats de controls o anàlisis rutinàries en matèria de seguretat pública (analitzar les matrícules per detectar cotxes "sospitosos") pugui resultar habilitada sense una base legal pròpia.

[75] Com apunta el SEPD, es podria establir una "granularitat" del consentiment, en funció –afegim- que les diferents finalitats siguin indispensables o no per prestar el servei.
[76] Exemple extret, a efectes il·lustratius, de la informació disponible a la web: http://www.esmartcity.es , en relació amb el sistema implantat a la ciutat francesa de Cannes per una determinada empresa.

Caldria plantejar, també, els riscos que es poden generar, en el sentit de que la capacitat de correlacionar la informació extreta de diferents sensors (instal·lats per a finalitats concretes en un entorn de Smart Cities), per obtenir i tractar una informació per a finalitats que no serien les que en principi haurien justificat l'obtenció i el tractament de les dades. És a dir, en un context de sensors instal·lats a les ciutats smart, que recullen informació de tot tipus i de manera "invisible" o imperceptible pels ciutadans, es podria generar en determinats casos una potencial vigilància continuada dels ciutadans. Aquest "seguiment" (o, d'alguna manera, aquest perfil en el que l'objecte és "el que fa" l'usuari), podria generar que, en cas de necessitat, determinades informacions que, a priori, no identifiquen cap persona concreta, puguin passar a ser dades personals, modificant la configuració de certs dispositius (p. ex. càmeres que inicialment per la seva configuració no permetien identificar persones, però que arran la modificació de la seva configuració sí que ho permeten). Això permetria fer un seguiment acurat del que fa una persona. Seguiment que, en línia amb el risc que apuntem, no estaria en absolut previst com a finalitat legítima inicial.

Aquesta reflexió enllaça especialment amb els exemples que hem esmentat en l'entorn de la seguretat pública: Caldria que qualsevol tractament amb finalitats policials de la informació generada en el marc d'experiències d'Smart City en principi amb altres finalitats, tingués la suficient habilitació en una base legal pròpia.

Caldria revisar aquestes possibilitats des de la perspectiva del principi de finalitat que tractem.

Serveixi també d'exemple el tractament de dades realitzat per un ajuntament, vinculat a la utilització de "smart cards", per exemple, per desplaçar-se per una ciutat amb finalitats de turisme. En aquest casos, podem entendre com a legítima la recollida i tractament de dades identificatives i bancàries (número de targeta a efectes de cobrament...). Ara bé, seria legítim fer un tractament dels llocs visitats per un turista, fent-lo identificable, amb finalitats d'oferir determinats serveis addicionals, sense una habilitació adequada? Creiem que no, llevat que es pugui considerar aquest tractament com a "indispensable" per al funcionament del sistema, i que forma part de la finalitat que habilita el tractament, això és, la prestació de determinat servei.

Finalment, apuntem un altre exemple que, creiem, caldria analitzar des de la perspectiva del principi de finalitat, entre d'altres. Es tracta de les xarxes inalàmbriques "Wi-Fi". Diverses administracions públiques, principalment en àmbit local, així com entitats privades, ofereixen accés a xarxes, habitualment Internet. La facilitat d'accedir a Internet o a informacions pròpies d'aquesta entitat (ajuntaments...) que ofereix l'accés a aquestes xarxes, és sens dubte un exemple de Smart City, ja que permet oferir als ciutadans serveis amb valor afegit (fer tràmits, gestions, obtenir informació...). Dit això, cal tenir present que la navegació que es pugui fer pot resultar monitoritzada per part del proveïdor d'aquest accés a xarxes –sigui públic o privat-. Aquesta monitorització, d'existir, hauria de respondre a una finalitat legítima, a banda que, entre d'altres, caldria informar adequadament l'usuari sobre aquesta possible monitorització.

4.3 Principi de qualitat. Principi de minimització.

El principi de qualitat (article 6 de la Directiva de protecció de dades de 1995 i article 4 de la LOPD) exigeix que qualsevol tractament de dades afecti, només, a les dades "adequades, pertinents i no excessives" en atenció a la finalitat legítima a la que es vol donar compliment en cada cas. En concret, i pel que fa al cas que ens ocupa, segons l'article 4 de la LOPD, les dades personals només es poden recollir -en el context que analitzem, per part d'una empresa o administració o autoritat pública que vulgui oferir un servei Smart City als ciutadans-, i només es poden tractar posteriorment quan siguin adequades, pertinents i no excessives, en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut. S'afegeix que les dades objecte de tractament no es poden utilitzar per a finalitats incompatibles amb les que varen habilitar la recollida, sense que es consideri incompatible el tractament posterior de dades amb finalitats històriques, estadístiques o científiques.

Per bé que no es pot generalitzar i trobar una base comuna per diferents supòsits d'Smart City en quant a les dades que poden resultar ajustades al principi de qualitat, sí cal partir de la base que el compliment d'aquest principi ha de ser especialment respectat en l'entorn de les Smart Cities. D'entrada, per la quantitat d'exemples que proliferen dia a dia en aquest context, i que en bona mesura poden comportar tractament de dades, i de l'altra, pel fet que determinades tècniques i sistemes que, com anem comentant, estan força presents en l'entorn de les Smart Cities (NFC,

RFID, portals d'internet, smartphones, sensors i comptadors intel·ligents, videocàmeres....), per sí mateixes, tendeixen a permetre un ingent tractament de dades personals.

Una concreció del principi de qualitat és l'anomenat "principi de minimització", el qual no es troba explicitat en la Directiva de protecció de dades de 1995, però sembla que podria quedar incorporar més explícitament en el Projecte de Reglament que es debat actualment al sí de la UE, citat. Concretament, l'article 5.c) del Projecte de Reglament disposa, entre d'altres, que les dades personals han de ser:

"adecuados, pertinentes y limitados al mínimo necesario en relación a los fines para los que se traten; solo se tratarán si y siempre que estos fines no pudieran alcanzarse mediante el tratamiento de información que no implique datos personales;

En qualsevol cas, la premissa d'utilitzar les mínimes dades imprescindibles per a cada tractament, així com la de fer els mínims tractaments possibles (per exemple, en atenció a les diferents fases del que genèricament considerem "tractament" de dades, si per dur a terme determinada actuació cal recollir dades, sense que ningú aliè al responsable les tracti, no serà necessari cedir-les) ha de tenir plena aplicació en l'àmbit de les Smart City.

El "contrapunt" al principi de minimització és el "data mining" o mineria de dades: a tall d'exemple, des del moment que en el context de les Smart Cities es posen a disposició dels usuaris unes Apps amb geolocalització per a diferents usos –tema ja apuntat-, per bé que aquests siguin legítims i aïlladament la informació tractada resulti proporcionada a la finalitat perseguida, no podem descartar que mitjançant tècniques de mineria de dades s'acabi fent un ús de dades personals excessiu i per tant desproporcionat. En un cas concret[77], es va poder comprovar que observant la ubicació de les metadades emmagatzemades en fotos publicades a través d'un compte amb pseudònim de twitter pel seu titular, es va poder localitzar el domicili d'aquesta persona. A partir d'això, per les referències creuades amb els registres d'aquesta ubicació de la ciutat, es va poder trobar el seu nom, lloc de treball, i identitat de familiars. Serveixi l'exemple d'advertiment del fet que, a partir del desenvolupament d'un servei d'Smart City que utilitza geolocalització, es pot estar

[77] Relatat a l'article "La geolocalización de los smartphones amenaza la privacidad" de www.tendencias21.net.

facilitant una mineria de dades dels usuaris i de tercers que pot posar en risc la seva privacitat.

Podem posar un altre exemple de minimització en el context dels comptadors intel·ligents: aquests comptadors permeten un seguiment, si es vol, continu dels consums en un domicili. Ara bé, per facturar el subministrament d'energia, hi ha cap necessitat de fer lectures de consum contínues? Clarament, sembla que no. El lapse entre lectures por ser major i per tant, menys intrusiu, segons la finalitat. Aquest serà un punt a tenir en compte (una altra cosa seria la realització de pautes de consum, que poden donar informació molt més "interessant" amb lectures constants, ara bé, des de la perspectiva de la protecció de dades, novament, caldria recórrer aquí al tractament d'informació agregada, probablement).

En qualsevol cas, per avaluar les dades personals que pot ser pertinent tractar resulta determinant aclarir per a quines finalitats (i usos secundaris) es tracten les dades[78]: si les dades es recullen per fer ús d'un lloguer de bicicletes, o per fer ús d'una targeta intel·ligent per utilitzar el transport públic (metro...), les dades a tractar, fins i tot el període de conservació d'aquestes dades, seran diferents si la finalitat és la de cobrar el servei, comunicar-se amb els usuaris, controlar el frau, etc, d'aquelles necessàries per fer un estudi sobre la qualitat del servei o el grau de satisfacció dels usuaris, a banda que, en aquest darrer cas, el tractament podria fer-se probablement amb informació anonimitzada.

Alguns casos no permeten, creiem, l'anonimització de les dades (per exemple, si un cotxe circula amb un dispositiu tipus "teletac" de cobrament electrònic de peatges, calen les dades del propietari per realitzar la facturació del servei; igualment, els sistemes d'"Ecovia", www.ecoviat.com[79], en què els vehicles acreditats com de baixa emissió, poden circular per determinades vies, o el carril bus-VAO[80]). Això obliga a un mínim tractament de dades difícilment anonimitzable, (tipus de vehicle, requeriments

[78] En relació amb el principi de qualitat i minimització, el Grup de Berlín destaca que no s'ha de fer el mateix tractament de dades per a totes les finalitats o usos i afegeix que, per exemple, les empreses de transport haurien de facilitar alternatives per poder "viatjar anònimament", sense que això els suposi un perjudici. Ens remetem als documents del Grup, citats en l'apartat de "Mesures de Seguretat".
[79] En aquesta web, l'usuari pot donar-se d'alta adjuntant informació d'una sèrie de documents del vehicle i dades personals.
[80] www.gencat.cat/especial/carrilbusvao/cat/vehicles.htm

tècnics, propietari...). Ara bé, en aquests o altres exemples (altres casos de "road pricing", o lloguer de bicicletes en el cas de Barcelona o Londres, etc [81]), l'anonimització sí és possible per a usos o finalitats secundàries.

Cal destacar que sobre els diferents exemples d'aplicació d'Smart City al trànsit en carreteres, en diversos països trobem informació relativa al tractament que es fa de dades personals, per a quines finalitats, etc. A banda d'algun exemple citat, destaquem com a iniciativa "positiva" el document que l'Autoritat de protecció de dades d'Ontario ha elaborat conjuntament amb l'Autoritat de trànsit, en què s'explica "com circular de forma anònima per determinades carreteres".[82]

A banda d'alguns exemples als que ens referim al llarg del treball, com ara els comptadors intel·ligents, i sobre els quals no tornarem a incidir, ens referirem a:

"Smart cards" o targetes intel·ligents, títols de transport o referents a d'altres equipaments de l'Smart City: permeten utilitzar les xarxes de transport públic i algunes afegeixen la possibilitat de fer servir altres equipaments, com ara museus, etc. Des del moment que aquests títols de transport són "personalitzats", és evident que hi ha un tractament de dades personals que ens pot donar informació sobre els moviments d'una persona, les persones amb que va acompanyat o, en el cas de serveis diferents al transport, sobre les seves aficions, hàbits, estil de vida etc.

En aquests casos els Ajuntaments (i/o empreses responsables) generalment posen a disposició dels usuaris, turistes... qüestionaris que cal emplenar, a través de les seves web, per tal de rebre aquestes targetes. Es sol·liciten i tracten dades identificatives, algunes permeten triar el transport, simplement, però d'altres permeten -o sol·liciten- fins i tot informació sobre si l'usuari que demana la targeta té algun tipus de minusvalidesa o necessitats especials...[83] (segurament aquests casos podrien ser un exemple de "possibilitat de minimització" ja que, en principi, no sembla justificable el

[81] Entre d'altres, posem l'exemple de la iniciativa "TOLL2GO", per la circulació de camions per la xarxa de carreteres d'Àustria i Alemanya, que comporta la instal.lació d'aparells de seguiment als vehicles: www.toll-collect.de. Citem aquest exemple com a "positiu", ja que en la pàgina web citada s'inclou una clàusula informativa força entenedora de quin tractament de dades personals es farà.
[82] "407 Express Toll Route: How you can travel the 407 anonymously", 1998, disponible a la web d'aquesta Autoritat, ja esmentada.
[83] www.southampton.gov.uk/smartcities

tractament d'aquestes dades sensibles, a menys que pugui ser rellevant, per exemple, per a la determinació de la tarifa, i que es demostri que clarament és necessari tractar aquesta informació per tal que l'usuari faci un ús del servei o transport).

D'altra banda, cal tenir en compte que en aquells supòsits que una mateixa targeta pugui servir com a sistema d'identificació en diferents serveis, aquest fet, per si sol, no hauria de comportar un tractament indiscriminat de la informació necessària per a la prestació de cadascun dels diferents serveis.

Pel que fa al cobrament electrònic de peatges (englobem els exemples tipus Teletac, Via-T,...), en general, en aquests casos, hi haurà sensors instal·lats a la zona de peatge, probablement videovigilància, (per al control d'infraccions), i cal instal·lar un receptor/emissor al vehicle, que facilitarà el cobrament electrònic del peatge. A banda de les dades mínimes per facturació, etc, la "minimització" podria aplicar-se a temes com ara evitar monitorització o perfils de rutes, moviments del vehicle, hàbits de desplaçament..., com també evitar utilitzar aquesta informació amb altres finalitats.

Serveixi com a exemple la informació de la xarxa de transports de Londres[84], en concret, la referida a la tarifa per utilitzar el vehicle en determinades zones, en què s'informa que l'usuari no necessita tiquets ni passis especials per entrar a determinades zones, sinó que les càmeres instal·lades a la zona capten la matrícula del vehicle. Es comprova en una base de dades si la persona ha pagat la taxa, si està exempta de pagar-la... la informació es conserva unes hores, i si tot està conforme (pagament fet, si escau, o exempció...) automàticament s'esborren totes les dades -imatges del vehicle- de la base de dades.

En alguns casos la utilització d'aquestes vies o de determinades tarifes pot estar supeditada a que el vehicle estigui ocupat per un determinat nombre d'ocupants. En aquesta casos no sembla justificat haver d'enregistrar una imatge de tots els ocupants, si més no en el cas dels vehicles que compleixin amb el nombre d'ocupants establert a la normativa corresponent.

En aquesta línea, també volem posar l'exemple dels sistemes "E-call". Es tracta de sistemes de gestió de trucades d'urgències que passen per col·locar sensors en un

[84] Tfl: "Transport for London": www.tfl.gov.uk/roadusers/congestioncharging/6718.aspx

vehicle, que en cas d'accident desencadenen una trucada d'emergència de forma automàtica[85]. En aquest context hauria de jugar una especial importància la transparència del sistema per a l'usuari, com també el seu control sobre aquest tipus de dispositius. D'altra banda ens podríem plantejar qüestions com ara, quines són les dades mínimes i necessàries perquè un sistema com aquest sigui efectiu.

Aquests i d'altres exemples podrien ser objecte d'una anàlisi més detallada sobre els usos concrets que comporten, quines dades cal tractar, quin temps de conservació és l'adequat, per a quins usos es pot tractar la informació de forma anonimitzada, etc.

Un element al qual també hauríem de fer especial atenció com a manifestació del principi de qualitat, és el que es refereix al manteniment i conservació de dades. Segons disposa l'article 4.5 de la LOPD:

"Les dades de caràcter personal han de ser cancel·lades quan hagin deixat de ser necessàries o pertinents per a la finalitat per a la qual han estat recollides o registrades. No han de ser conservades de manera que permetin identificar l'interessat durant un període superior al necessari per a les finalitats d'acord amb les quals hagin estat recollides o registrades."

Sobre això, incidim en diversos exemples que hem anat desgranant en aquest treball: en el marc de la mobilitat viària, les dades tractades pel pagament de taxes per accedir un nucli urbà no haurien de ser conservades, probablement, més enllà de la constatació del pagament per part de l'usuari, o com a màxim durant el període de validesa de la taxa satisfeta . No descartem que la informació generada pugui ser útil, per exemple, per tal que una administració municipal pugui replantejar (ampliar, limitar...) la zona on és pertinent cobrar la taxa, però aquest seria un cas en què es podria tractar la informació personal, probablement, de forma agregada, és a dir, sense identificar la persona (matrícula, propietari...). Per tant, la informació personal no podria ser conservada per a aquestes finalitats identificant la persona.

Finalment, fem referència a la informació que un telèfon mòbil podria anar "acumulant" i emmagatzemant sobre les recerques que ha fet l'usuari per localitzar diferents llocs d'interès, a través de la geolocalització. El fet que diversos serveis o Apps permetin

[85] Ens remetem a la Comunicació de la Comissió Europea "E-Call: el momento de implantarlo" COM (2009)434 final; Document de treball del Grup de l'Article 29 sobre les conseqüències per la intimitat en la iniciativa eCall, de 26 de setembre de 2006.

mantenir un "històric" de llocs visitats o consultes fetes, pot resultar útil a l'usuari, però ens hauríem de preguntar si té sentit que, per defecte, s'acumuli i mantingui emmagatzemada aquesta informació *sine die*. La determinació de quin hagi de ser el període de conservació adequat en cada cas, hauria de quedar en mans de l'usuari que, en qualsevol cas, hauria de tenir prou disponibilitat per eliminar aquests tipus de registres de consultes fetes anteriorment.

El Grup de Berlín apunta en diversos documents que cal fer especial atenció als períodes de conservació de les dades (per exemple, si les dades permeten un viatge turístic durant tres dies per una Smart City, més enllà de pocs dies no té sentit que l'autoritat del transport d'aquella ciutat conservi dades del turista, a menys que s'asseguri que se'n farà un mer ús estadístic de recorreguts efectuats en transport públic o de museus o llocs d'interès visitats -l'exemple és nostre-).[86]

També caldria reflexionar sobre quines són les capacitats d'interoperabilitat dels diferents sistemes, ja que això podria comportar certs riscos. En l'entorn de les Smart Cities, es poden generar tractaments en relació amb diferents conjunts de dades, els quals no són especialment rellevants si els considerem de manera aïllada (el conjunt de dades tractat en relació amb un exemple de Smart City pot no incloure informació sensible, per exemple, o pot no incloure un nombre important de dades de diferents categories...). Ara bé, si aquests conjunts de dades es processen en un mateix entorn, es poden generar efectes no desitjats –nous tractaments no habilitats ni ajustats als principis de protecció de dades-.

4.4 Principi d'informació o transparència.

El deure d'informació és un altre dels eixos fonamentals de la protecció de dades. Aquest principi implica que el responsable d'un fitxer o tractament de dades té l'obligació d'informar la persona física titular de les dades, entre d'altres, de quin tractament es farà i què implica aquest tractament, a qui es cediran les dades, per a

[86] Per exemple, amb la utilització de la citada "Iamsterdam Card", targeta intel·ligent que permet utilitzar mitjans de transport i visitar determinats llocs d'interès, en cada museu visitat es pren nota del número de targeta, i cal marcar –amb la targeta citada- cada entrada i sortida d'un transport públic. Val a dir que la targeta funciona amb un número aleatori, -no amb el nom i cognoms de la persona-. Ara bé, si aquests tipus de targes turístiques s'han pagat amb una targeta bancària, fins a quin punt es pot relacionar la informació i "personalitzar" els recorreguts fets o els llocs visitats? Amb quina finalitat? I amb quin grau d'informació a l'usuari?

quina finalitat, on ha d'adreçar-se per obtenir informació sobre el tractament i, si escau, exercir els drets que atorga la normativa de protecció de dades (accés, rectificació, cancel·lació i oposició, drets ARCO). Així, el principi d'informació és clau en el context de l'autodeterminació informativa, per exercir els drets ARCO. En això radica bona part de la transcendència del dit principi. L'article 5 LOPD configura els elements sobre els quals cal informar l'usuari, en els següents termes:

"1. Els interessats als quals se sol·licitin dades personals han de ser prèviament informats de manera expressa, precisa i inequívoca:
a) De l'existència d'un fitxer o un tractament de dades de caràcter personal, de la finalitat de la recollida de les dades i dels destinataris de la informació.
b) Del caràcter obligatori o facultatiu de la resposta a les preguntes que els siguin plantejades.
c) De les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.
d) De la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.
e) De la identitat i la direcció del responsable del tractament o, si s'escau, del seu representant.
Quan el responsable del tractament no estigui establert en el territori de la Unió Europea i utilitzi en el tractament de dades mitjans situats en territori espanyol, ha de designar, llevat que aquests mitjans s'utilitzin amb finalitats de tràmit, un representant a Espanya, sens perjudici de les accions que es puguin emprendre contra el mateix responsable del tractament.
(...)."

En el marc del que disposa la Directiva de protecció de dades de 1995, la LOPD, i de les concrecions del Projecte de Reglament de protecció de dades[87], és especialment rellevant constatar que els elements que "tradicionalment" configuren la informació que el responsable d'un tractament de dades ha de donar, haurien de ser revisats quan parlem de determinats casos d'Smart City.

El Projecte de Reglament UE citat (art. 11, en connexió amb l'art. 14) exigirà al responsable aplicar "polítiques transparents i fàcilment accessibles" en relació amb el tractament de dades personals i l'exercici dels drets de l'interessat.

El futur marc de protecció de dades europeu pretén atorgar major rellevància, encara, a la "transparència", en el sentit d'accessibilitat i claredat en la informació que el responsable ha de donar als interessats respecte el tractament de les seves dades: un exemple, dels molts amb que podem il·lustrar la importància que la transparència pot tenir en les Smart Cities, és el referit als "smart parkings", o sistemes d'aparcament

[87] Per bé que es tracta d'un text no definitiu, cal tenir en compte la rellevància atorgada en el Projecte de Reglament UE a la transparència en la informació –art. 11-, a la portabilitat de les dades –art. 18-, o a l'elaboració de perfils –art. 19-, com a "nous drets" en el context dels drets del titular de les dades personals, qüestions que hauran de ser tingudes en compte en el context de les Smart Cities.

intel·ligents[88]. Sistemes com aquests funcionen a través de la distribució de nodes en el paviment dels carrers d'una ciutat, en concret, de zones d'aparcament. En principi, aquests nodes no recullen informació del cotxe o del conductor, sinó que informen sobre si una plaça d'aparcament està o no ocupada, informació que s'envia a través d'una App que una persona es descarrega al seu mòbil, o a una pàgina web que es pot consultar. Ara bé, l'usuari que accedeix al web de l'empresa o servei municipal que gestiona el servei de pàrquing intel·ligent, sap quin rastre pot deixar la seva consulta a la web o el fet que es descarregui l'App al seu mòbil? Quina informació "transparent i assequible", doncs, haurà de donar el responsable per tal de complir adequadament amb les exigències del principi d'informació, no només en el context actual de l'article 5 LOPD, sinó amb vistes a les exigències de la nova normativa UE?.

Pel que fa a un dels exemples analitzats abastament en aquest treball, com són els comptadors intel·ligents, se'ns presenten diverses consideracions, respecte el deure d'informar:

- La informació sobre el tractament de dades hauria de referir-se a tots els usos previstos, diferenciant clarament els "necessaris" per a la prestació del servei (facturació, detecció de fraus o avaries, etc), dels que no ho són (usos secundaris).
- Caldria informar adequadament l'usuari sobre les dades que l'empresa subministradora ha de tractar sense consentiment, i aquelles dades (o tractaments) que requereixen el consentiment de l'usuari.
- S'hauria d'informar sobre els períodes de conservació, en funció de les finalitats?.
- Caldria informar sobre la possibilitat de portabilitat de les dades, per al cas que l'usuari decideixi canviar de companyia subministradora?.
- Atès que el propi usuari tindrà un rol actiu sobre la seva informació (consultes a les pròpies dades, facturació...) se l'hauria d'informar sobre la manera segura d'accés, consulta i tractament de les pròpies dades –possibilitat o no de rectificació o cancel·lació de dades, etc-?.
-També creiem que caldrà treballar especialment, en relació amb l'ús de xarxes i comptadors intel·ligents, en la redacció de qüestionaris, formularis o altres impresos de recollida de dades (art. 5.2 LOPD), ja que entendre quines dades són o no

[88] Per exemple, com el projecte fet en col·laboració amb l'Ajuntament de Birmingham: http://blog.ferrovial.com , que citem a títol il·lustratiu.

necessàries, quines mesures de seguretat s'apliquen, etc, pot implicar certa dificultat de comprensió per part dels usuaris.

-Convé fer atenció, també, al fet que la companyia subministradora d'energia –principal responsable del tractament- no estigui establerta a la UE, o pugui cedir dades a tercers fora de l'àmbit de la UE, als efectes de donar informació adequada i comprensible per a l'usuari sobre els responsables del tractament de les dades.

D'altra banda, novament recorrem a l'exemple d'experiències Smart City que utilitzen aplicacions de geolocalització: es deriva del que hem dit anteriorment, que és força improbable que els usuaris d'aplicacions Smart City que utilitzen aquesta tecnologia siguin conscients del seu grau de control sobre la pròpia geolocalització, i dels drets que els emparen i que els atorga la legislació de protecció de dades. Per tenir capacitat real d'exercir drets ARCO, cal que l'usuari hagi rebut suficient informació sobre les conseqüències d'aquest tractament.

El responsable de tractaments de dades aparellats als exemples citats d'aplicacions amb geolocalització ha de donar a l'usuari una informi clara i entenedora sobre aquests. Podria ser exigible (a banda del que en qualsevol tractament exigeix l'article 5 de la LOPD) que l'usuari conegui quines dades de localització es recullen i tracten, que se li informi de com pot triar el nivell i abast de la geolocalització (limitar, bloquejar, activar o desactivar la geolocalització), o de com pot eliminar dades de localització emmagatzemandes; també en el cas que es condicioni la circulació en vehicles pel centre d'una ciutat al pagament d'una taxa, i els usuaris hagin d'instal·lar un dispositiu al seu vehicle que en fa un seguiment, de manera que l'usuari "emet informació" sobre els moments en què es troba –el vehicle- en aquella zona, i ha de saber com desactivar-ho quan surt de la zona en qüestió; si el responsable conserva dades de localització l'usuari aquest hauria de saber-ho, per tal de tenir la possibilitat d'actualitzar, rectificar o cancel·lar dades, si escau, o d'oposar-se a determinats tractaments que puguin no estar relacionats directament amb l'exemple citat. Un altre exemple: si en el futur un sistema d'utilització de bicicletes urbanes gestionades per un Ajuntament, tipus "bicing" a Barcelona, o "Barclays Cycle Hire" a Londres[89] permetés la geolocalització de la bicicleta en tot moment i, amb això, per bé que indirectament, la geolocalització de l'usuari, creiem que això plantejaria exigències especials en relació amb la informació que sobre això n'hauria de rebre l'usuari.

[89] Informació disponible a: https://web.barclayscyclehire.tlf.gov.uk .

En aquesta línea, en relació amb tecnologies NFC, targetes bancàries contactless, etc, atès que, com hem exposat, en l'entorn de les Smart Cities l'usuari esdevé un "distribuïdor" de la seva pròpia informació personal, fent-la accessible a tercers a vegades amb cert risc i desconeixement, els advertiments de seguretat podrien formar part de la informació que el responsable ha de donar a l'usuari?.

Pel que fa al deure d'informació en relació amb altres exemples que hem tractat en aquest document, en alguns casos també seria interessant plantejar-se si el responsable ha d'explicar amb cert detall (i de manera entenedora i adaptada a la capacitat de comprensió de l'usuari, insistim), sobre les dades que, un cop tractades en el context de la finalitat principal, poden ser objecte d'anonimització o tractament agregat.[90] Aquesta consideració és extensible a diversos exemples, com ara els serveis de pàrquing intel·ligent, l'ús d'Apps per rebre informació diversa, les consultes realitzades pels ciutadans a pàgines web d'informació, serveis de lloguer de bicicletes... Alguns d'aquests casos poden generar, legítimament, un interès per part del responsable (un ajuntament, per exemple), per realitzar un estudi estadístic sobre la seva viabilitat, grau de satisfacció dels usuaris, possibilitats de millora..., podria ser convenient, doncs, que com a part del deure d'informació l'usuari sabés en quina mesura les seves dades poden ser tractades a efectes estadístics posteriorment.

Per exemple, si una smart city es planteja fer estudis de mobilitat a partir de la participació de ciutadans en un sistema de detecció de pàrking intel·ligent (l'usuari s'instal·la una App al seu mòbil, on rep alertes sobre una plaça disponible en determinat carrer) per millorar el trànsit en determinades zones o franges horàries, sembla que aquests estudis han de ser viables, sempre que s'anonimitzi prèviament la informació personal que s'hagi pogut tractar de l'usuari que utilitza el sistema de pàrking intel·ligent. Alternativament, podríem plantejar com a raonable, des de la perspectiva del principi d'informació que comentem, que l'estudi utilitzi dades personals desagregades –permetent la identificació- amb el consentiment de l'afectat? No podem descartar aquesta possibilitat, per bé que ens sembla un clar exemple de necessitat de reforçar la informació prèvia que caldria donar a l'usuari.

[90] El Grup de Berlín alerta sobre el dret dels afectats de ser informats adequadament sobre el tractament de dades per a "usos secundaris", als efectes de poder donar el seu consentiment explícit (opt-in) o retirar-lo (opt-out).

També creiem que pot ser problemàtic (i per tant, objecte d'atenció) establir un grau adequat d'informació a l'interessat en aquells casos en què hi ha diversos "responsables, encarregats, i tercers" implicats, per exemple, en el context de les xarxes i comptadors intel·ligents, en què hi pot haver implicada l'administració pública, l'empresa subministradora, empreses del mateix grup en el mateix o altres països, tercers que subministren "serveis de valor afegit" (a què es fa sovint referència en els documents citats sobre xarxes i comptadors intel·ligents, però que no es concreten, cosa que seria convenient), etc. La mateixa consideració la podem fer en aquells casos en què els usos derivats de la finalitat principal, no s'expliquen suficientment.

Finalment, volem insistir en relació amb el principi d'informació en un darrer punt de debat. Si una cosa caracteritza la majoria d'exemples d'Smart City és el necessari ús de determinades tecnologies per part dels usuaris. Algunes d'aquestes tecnologies poden ser força desconegudes pel titular de les dades (geolocalització, traçabilitat, RFID, targetes contactless, NFC...). Així, ens haurem de plantejar si un usuari, un ciutadà sense especials coneixements tècnics, tindrà facilitat per comprendre el tractament de dades que el seu ús pot comportar. Més encara, podríem considerar, atès que l'ús d'aquestes tecnologies podria presentar especials riscos per la seguretat de la informació (qüestió sobre la que tornarem en referir-nos a les mesures de seguretat), que el deure d'informació no només ha d'incloure els elements de l'article 5 LOPD, sinó també una mínima informació a l'usuari (pràctiques recomanades o consells de seguretat) sobre mínimes mesures de seguretat per protegir la informació? Cabria considerar que les "polítiques transparents" que probablement exigirà el futur Reglament UE al responsable han d'incloure uns mínims consells de seguretat per a l'usuari d'una targeta contactless, per tal d'evitar que la informació personal que s'hi conté sigui objecte de captació o tractament indegut per tercers? Podria exigir-se al responsable donar aquesta informació, tenint en compte l'exigència –força genèrica- de l'article 14.1.h) del Projecte de Reglament UE, de donar "qualsevol altra informació que resulti necessària per garantir un tractament de dades lleial", tenint en compte les circumstàncies específiques en què es recullen les dades? (Per exemple, les circumstàncies en què a través de tecnologia NFC es recullen les dades de l'usuari, o el flux informatiu que es produeix en acostar un dispositiu mòbil a un node situat en punts de la ciutat per obtenir informació, certament pot escapar de la comprensió de

molts usuaris, i advertir l'usuari dels riscos podria formar part d'aquesta "lleialtat" exigible.

4.5 Exercici de drets per part de les persones interessades.

Com s'ha apuntat, l'exercici de drets per part del titular de dades personals és una manifestació del dret a l'autodeterminació informativa.

Els drets ARCO (accés, rectificació, cancel·lació i oposició), es troben configurats en la LOPD, a partir de la Directiva de protecció de dades de 1995 (Títol III de la LOPD, desplegat al Títol III del RLOPD). També cal que fem especial atenció a les previsions del Projecte de Reglament UE sobre l'exercici d'aquests drets (arts. 15 a 21), amb l'avinentesa, com sempre, que es tracta d'un text no definitiu.

Partim de la base que qualsevol tractament de dades en el context de les Smart Cities ha de generar la possibilitat real de que els usuaris afectats exerceixin els seus drets. Més enllà de consideracions generals aplicables a l'exercici d'aquests drets en relació amb qualsevol tractament de dades, en l'àmbit que ens ocupa fem les següents consideracions particulars:

El dret d'accés (arts. 27 a 30 RLOPD) no ha de veure's limitat per una deficient transparència de qui és el responsable del tractament, o dels tercers que tracten les dades. Això pot no representar especials dificultats quan un Ajuntament, per exemple, a través de la seva pàgina web, facilita una aplicació perquè una persona es doni d'alta en un servei de cobrament electrònic de taxes per utilització de determinades vies urbanes o interurbanes, si se l'informa adequadament sobre l'exercici de drets, però pot ser més problemàtic en casos en què hi ha diverses empreses prestadores implicades, com ja hem exposat en aquest treball (un Ajuntament, l'empresa prestadora del servei, l'empresa que fa l'aplicació per obtenir una targeta intel·ligent; el responsable prestador del servei és diferent al responsable de tractar les dades per altres finalitats....). O també, pot ser dificultós per a un usuari identificar qui és el responsable de tractar les seves dades, quan s'instal·la una App a un dispositiu propi, per gaudir d'un determinat servei: l'Ajuntament que ofereix el servei? L'empresa que desenvolupa l'App? Altres operadors de telefonia intervinents?.

En qualsevol cas, caldrà tenir en compte l'existència d'un responsable i, si escau, d'encarregats del tractament, als efectes de saber qui ha d'atendre en cada cas l'exercici[91] del dret d'accés (consideració que fem extensible a d'altres drets ARCO), i més tenint en compte la brevetat dels terminis legals imposats per atendre els drets.

També apuntem que la LOPD exigeix que l'accés a les pròpies dades es doni en forma "llegible i intel·ligible". En el cas, per exemple, de mesures molt detallades del consum energètic a través de comptadors intel·ligents (mesures cada 30 minuts, per exemple, i durant un llarg període de temps, que poden servir per crear perfils de consum), en el cas que l'afectat sol·liciti l'accés, com s'hauria d'atendre aquest accés? Seria suficient indicar el fet objectiu que es realitzen lectures molt concretes i sovintejades de consum? Caldria indicar el lapse de temps en què es fa la mesura? Caldria afegir la informació sobre el perfil efectuat? Quina seria, en aquest cas, la manera "lleial" i completa d'atendre el dret d'accés?[92]

Respecte els drets de rectificació i de cancel·lació de les dades (l'exercici dels quals es regula de forma agrupada als arts. 31 a 33 RLOPD), hi ha un punt comú a tots dos que cal destacar: com s'infereix del que apuntem en aquest treball, l'usuari d'alguns exemples d'Smart City pot tenir cert grau de dificultat a l'hora d'entendre i tenir clar quines dades personals es tracten, ja que en molts d'aquests casos estem passant del "tradicional formulari" amb dades identificatives i de contacte per rebre informació d'un determinat servei o activitat, a connectar el nostre smartphone a un node o sensor, operació que probablement generarà un flux informatiu bidireccional que és difícilment comprensible o identificable per a molts ciutadans. Podem fer extensible aquesta consideració a la informació tractada en els comptadors intel·ligents, per bé que els comptadors "tradicionals" ja permeten tractar informació personal i, si escau, exercir el dret de rectificació o de cancel·lació. Constatat això, podem avançar que en alguns casos podria ser complicat per a l'usuari complir amb l'exigència de l'article 32.1 RLOPD, segons el qual, quan s'exerciten aquests dos drets, en la sol·licitud cal indicar

[91] Qüestió que aquesta Autoritat ha tractat amb deteniment en la seva Recomanació 1/2010, sobre l'encarregat del tractament en la prestació de serveis per compte d'entitats del sector públic a Catalunya.

[92] Partint de la base que la recol·lecció sistemàtica i per defecte de corbes de consum es podria considerar desproporcionat, segons apunten, per exemple, les Recomanacions de la CNIL, esmentades.

a quines dades es refereix l'interessat. Aquesta qüestió, ens sembla, hauria de ser objecte d'especial reflexió.

Específicament respecte la rectificació de dades, aquest dret es refereix a dades "inexactes o incompletes" (art. 16.2 LOPD, art. 31 RLOPD i art. 16 del Projecte de Reglament UE). A banda de supòsits que no ofereixen major dubte (rectificar dades errònies incloses en un formulari web per fer ús del servei de lloguer de bicicletes o del pagament d'una taxa per circulació amb vehicles...), creiem difícil establir, en la pràctica, "inexactituds i incorreccions" de dades de geolocalització, per exemple, o de dades de perfils de consum energètic. D'entrada, serà fàcil que l'usuari arribi a detectar-ho? I després, com podrà justificar-ho davant el responsable? Considerem que pot ser especialment dificultós per a l'interessat aportar "documentació justificativa" que acrediti la pertinença de la rectificació (art. 32.1 RLOPD). En qualsevol cas, només si el ciutadà té realment la possibilitat, mitjançant el dret d'accés, de coneixer quina informació seva s'està tractant, podrà arribar a exercir aquests drets.

Fem extensible aquest darrer advertiment (ex. art. 32.1 RLOPD) respecte possibles cancel·lacions de dades, en les que també s'exigeix aquesta acreditació per part de l'interessat.

Encara en relació amb la cancel·lació de dades, a tall d'exemple podríem imaginar determinades Apps que, a través dels smartphones o d'altres dispositius, donessin a un visitant esporàdic d'una ciutat una sèrie d'informacions sobre llocs turístics d'interès. Fins a quin punt, podríem preguntar-nos, aquesta persona és conscient de la informació (del "rastre", especialment si s'utilitza geolocalització)[93] que anirà deixant a arrel de la utilització d'aquest servei, o de si un tercer mantindrà algun tipus d'informació un cop la visita a la ciutat ha conclòs, o quin possible ús es farà d'aquella informació? Això pot afegir dificultats pràctiques a l'hora de cancel·lar dades per part d'aquest visitant esporàdic.

Aquestes consideracions són extensibles a molts altres exemples, com ara el formulari que emplenarà una persona a una web municipal per obtenir una targeta que li permeti circular amb el seu vehicle per una ciutat que no tornarà a visitar en força temps, o les

[93] Hi incideix especialment el document "On locational privacy, and how to avoid losing it forever", de A. Blumberg i P. Eckersley, Electronic Frontier Found. 2009. Font: www.eff.org.

dades de medició de consum d'una determinada energia preses amb comptadors intel·ligents, en relació amb una persona que ha ocupat una vivenda de lloguer durant un temps (la companyia subministradora podria mantenir i fer ús de la informació generada, vinculant la informació a una persona física que ja no ocupa aquell habitatge?). O en l'exemple esmentat d'enregistrament de matrícules de cotxes en una ciutat, amb la possibilitat de creuar la informació amb fitxers policials per detectar "matrícules sospitoses", quan temps es mantindrà aquesta matrícula en els dits fitxers? Amb quina finalitat? De tot això pot dependre que l'usuari pugui cancel·lar o no les seves dades personals.

També mereix una especial atenció el dret d'oposició, com ja ha quedat apuntat. Aquest dret permet a l'interessat oposar-se a un tractament de dades, amb motius personals i fonamentats, quan aquell tractament no requereix el seu consentiment (quan el tractament es basa en el consentiment l'interessat pot retirar-lo en qualsevol moment, atès que estem davant d'un dret personalíssim).[94] Cal plantejar fins a quin punt un usuari es podrà oposar a un tractament de dades, si el servei o prestació Smart City fa ineludible aquest tractament.

En alguns casos, si el gaudi d'un servei (circular per determinada via, pagar un peatge o taxa de determinada forma, rebre informació turística o d'esdeveniments culturals a través de determinades webs o Apps...) és "opcional" per al ciutadà – és a dir, té altres alternatives-, des del moment que aquest ciutadà "tria" el servei Smart City, pot ser més conscient del tractament de les seves dades (ell mateix s'informa sobre el servei i opta per comunicar una sèrie de dades). Per contra, en aquells casos en què un servei Smart City no depengui del previ consentiment de l'afectat (per exemple, pensem que en un futur proper l'única via de pagament d'un determinat transport públic sigui a través d'una targeta intel·ligent) pot ser difícil articular, a la pràctica, una oposició al tractament de dades.

[94] En relació amb això, també apuntem que la retirada del consentiment (art. 6.3 LOPD) en alguns exemples d'Smart City pot ser problemàtic: Per exemple, l'empresa subministradora podria condicionar el subministrament a que l'interessat "consenti" el tractament de dades per a finalitats secundàries, aparellades a la principal? D'entrada ens inclinem a considerar que no, i a més, no sembla que en aquest cas, com a mínim, es pugui derivar algun perjudici per al consumidor del servei en el cas que retiri el seu consentiment.

A banda de l'exercici dels drets ARCO, cal tenir en compte altres qüestions que també relacionem amb l'autodeterminació informativa, és a dir, amb el control que l'afectat ha de tenir sobre la seva informació personal:

Pel que fa a l'anomenat "silenci dels xips", per bé que no és un exercici del dret d'oposició ni per tant es troba subjecte als mateixos requisits que aquest, podem considerar que també comporta una certa "oposició" d'un interessat a que la seva informació sigui tractada de determinada manera, un cert "posicionament" d'aquest sobre el tractament de les seves dades o, dit d'una altra manera, una voluntat de mantenir-se al marge del tractament que es pot derivar d'un exemple determinat d'Smart City. És a dir, si el futur proper és que un ciutadà es pugui desplaçar per la ciutat apropant el seu smartphone a dispositius instal·lats per la ciutat per tal d'obtenir informació, aquesta serà la seva única alternativa? En cas que la resposta sigui afirmativa, podrà controlar, silenciar, limitar o seleccionar la informació personal que generaran les seves consultes (vegades que es consulten determinats museus, transports, punts d'informació turística...)? Es podrà oposar a que el servei Smart City li sol·liciti la seva localització geogràfica? Resultaria abusiva aquesta sol·licitud? Això seria aplicable a d'altres exemples que hem anat citant, com ara el pagament de bitllets de metro a través de targetes contactless, NFC... Quin marge de control (o d'oposició, en terminologia de protecció de dades) té l'usuari, per exemple, sobre el fet que el responsable del tractament faci un seguiment dels seus desplaçaments en metro al llarg d'un període determinat? En aquest darrer exemple, novament, limitar o condicionar aquest dret d'oposició podria ser abusiu? (Més encara, com apuntàvem, si en un futur la única via de pagament dels desplaçaments en metro, per seguir l'exemple, passa per aquests sistemes).

També s'estan implantant en algunes ciutats els anomenats panells intel·ligents ("digital signage"), no només en espais oberts sinó en centres comercials, centres poliesportius, parades de metro i altres transports, és a dir, espais públics i privats. Aquests panells intel·ligents permeten adreçar missatges i donar informacions als ciutadans, que, mitjançant sensors de diferents tipus, es poden anar adaptant a les circumstàncies que es donin en cada moment. La progressiva instal·lació d'aquests panells, sens perjudici de la seva utilitat, també haurà de ser valorada des de la

perspectiva del "dret a no ser molestats", i d'aquest "silenci" que les persones, probablement, tenen dret a reclamar en el seu entorn físic.[95]

Finalment, cal no oblidar les previsions del Projecte de Reglament UE sobre "nous drets", com són el dret a la portabilitat de les dades (art. 18 del Projecte)[96] i l'elaboració de perfils (art. 20). Simplement apuntar que atès que en el marc de les Smart Cities és evident que es tractaran dades personals per via electrònica en molts casos, els responsables hauran d'afrontar els casos en què l'usuari sol·liciti la portabilitat, sense que això pugui suposar un greuge o perjudici en el gaudi del servei en qüestió. Pel que fa a l'elaboració de perfils, qüestió abastament citada en relació amb les Smart Cities, els responsables hauran de tenir en compte que, segons el Projecte de Reglament, el "profiling", limitat per defecte (art. 21.1[97]), s'hauria de basar en el consentiment de l'interessat, o produir-se en el marc de la celebració o execució d'un contracte, principalment.

4.6 Mesures de seguretat.

Segons la normativa de protecció de dades (art. 9 de la LOPD i Títol VIII del RLOPD), en el marc del que disposa la Directiva Europea de 1995[98], el responsable del fitxer i, si s'escau, l'encarregat del tractament, han d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries que garanteixin la seguretat de les dades de caràcter personal i n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposats, tant si provenen de l'acció humana o del medi físic o

[95] Sobre el concepte de "digital signage" i les seves implicacions per a la privacitat, ens remetem a l'article de R. Miralles, "Digital signage i privacitat", de la Revista "+KDades" de l'Autoritat Catalana de Protecció de Dades, núm. 16, disponible a la web: www.apd.cat.

[96] Tot i que, pel que es desprèn de l'"Informe Albrecht", del Parlament Europeu, sobre el Projecte de Reglament UE (Ref.: 2012/0011 (COD), de 16.1.2013), es podria configurar la portabilitat com una manifestació del dret d'accés tradicional, i no com un "nou dret".

[97] Art. 21.1: "Toda persona física tendrá derecho a no ser objeto de una medida que produzca efectos jurídicos que le conciernan o le afecten de manera significativa y que se base únicamente en un tratamiento automatizado destinado a evaluar determinados aspectos personales propios de dicha persona física o a analizar o predecir en particular su rendimiento profesional, su situación económica, su localización, su estado de salud, sus preferencias personales, su fiabilidad o su comportamiento."

[98] Veure l'article 17 de la Directiva 95/46/CE en relació amb les obligacions del responsable i, si escau, de l'encarregat del tractament, en relació amb les mesures de seguretat aplicables. Veure també els articles 30 a 32 del Projecte de Reglament UE, citat.

natural. A això cal afegir que, en funció de la informació personal tractada en cada cas, i de la seva especial sensibilitat (article 7 LOPD), caldrà aplicar unes mesures més o menys reforçades i exigents –de nivell bàsic, mitjà o alt-, als diferents fitxers o tractaments de dades personals que generi el tractament de dades.

En relació amb els diversos exemples d'Smart Cities que es puguin produir, seria convenient analitzar si hi ha mesures de seguretat especialment adients, o si n'hi ha d'altres l'aplicació de les quals convindria reforçar. En alguns dels textos analitzats en aquest treball es fan consideracions al respecte.[99]

D'entrada, en relació amb l'aplicació de les mesures de seguretat, és rellevant determinar qui és el responsable d'un tractament de dades i, si escau, els encarregats del tractament. En alguns exemples d'Smart City, com ara el referit a la utilització de comptadors intel·ligents, es detecta certa problemàtica a l'hora de concretar quins són els agents implicats i, per tant, quines han de ser les responsabilitats de cadascú, pel que fa a l'aplicació de les dites mesures. Per tant, en aquest i en altres casos caldrà definir adequadament els "responsables", els encarregats", o els "tercers que poden oferir altres serveis", etc, per tal de determinar el grau de responsabilitat que els serà exigible, en relació amb la seguretat dels diferents tractaments de dades personals efectuats.

Cal tenir en compte les referències a la millora de mesures de seguretat ja existents, o fins i tot la implementació de mesures de seguretat "ad hoc", que s'apunten en els següents textos del Grup de Treball de Berlín, esmentat[100]:

-Document de treball: "E.Ticketing in public transport" (setembre 2007).
- Carta de Granada sobre privacitat en el món digital (abril 2010).
- Document de treball: "Privacy by design and smart metering: Minimize personal information to maintain privacy."[101] (setembre 2011).

[99] En diversos documents citats en aquest treball es fan mencions relatives a la seguretat de les dades. Entre d'altres, l'apartat 7 de l'Informe de 16.2.2011, del Grup d'experts 2 del Grup especial sobre xarxes intel·ligents ("Smart Grids Task Force"), esmentat, detalla les ESO (European Standardization Organizations) i estàndards de seguretat existents i que poden ser convenients en relació amb les xarxes intel·ligents.

[100] Consultables a la web: http://www.berlin-privacy-group.org

- Document de treball: "Event data recorders (EDR) on vehicles. Privacy and data protection issues for governments and manufacturers." (Abril 2011).
- Posició comú: "Online profiles on the Internet". (maig 2000).
- Memorandum de Sofia: "Report and guidance on road pricing". (març 2009).
- Posició comú sobre: "Privacy and location information in mobile communications services". (novembre 2004).

Des de la perspectiva de la seguretat, des del moment que un usuari utilitza una targeta intel·ligent per al pagament d'un transport públic, per exemple, o realitza el pagament del bitllet amb l'ús de targetes amb RFID o NFC, que poden incorporar dades personals (podríem imaginar que dades identificatives, com a mínim, incloent el número de targeta de crèdit), aplicar mesures de seguretat adients per protegir la informació d'accessos i utilització fraudulenta per tercers. Això és extensible a les targetes intel·ligents que es poden utilitzar en relació amb l'atenció mèdica o farmacèutica, per exemple, per rebre atenció mèdica en un centre de salut o bé per comprar medicaments en una farmàcia. En el cas que aquestes targetes intel·ligents incorporin dades personals de l'usuari d'un servei mèdic o farmacèutic, caldrà aplicar mesures de seguretat adients per protegir la informació, que pot ser informació sensible.

Cal incidir en la utilització de targetes de crèdit amb tecnologia NFC (incorporació de xips NFC), per realitzar diversos tipus de pagaments, en el nostre cas, relacionats amb serveis o prestacions Smart City. Com s'ha posat de manifest, es detecten riscos per la seguretat de la informació personal que es conté en aquests tipus de dispositius. No només en cas de robatori o sostracció física, sinó també a través de la utilització de determinats dispositius que, amb la proximitat amb la targeta contactless que conté les dades personals (identificatives, dades bancàries...) permetrien "descarregar" i llegir aquestes dades. El fet que, fins i tot amb desconeixement de l'usuari, un tercer pugui obtenir les dades referides, és evidentment un risc de seguretat que cal tenir en compte, per tal de desenvolupar sistemes de protecció de la informació en front d'aquestes intrusions. Hi ha mecanismes que permeten obtenir i llegir el compte

[101] Sobre les Smart Metering, ens remetem a les consideracions d'aquest document, ja que en bona part són coincidents amb altres consideracions que ja hem comentat abastament en aquest treball.

corrent, el nom i cognoms del titular, i la data de caducitat de la targeta de crèdit contactless utilitzada, sense coneixement de la persona interessada, amb el risc que això suposa d'utilització posterior fraudulenta d'aquestes dades (compres per Internet, etc) [102]. Des del moment en què en exemples d'Smart City s'utilitzin targetes de crèdit que incorporen aquestes dades, caldrà fer atenció a aquests riscs i a la seva prevenció.

Insistim en la idea abans apuntada, ara des de la perspectiva de la seguretat, que l'usuari de diversos exemples d'Smart City pot esdevenir un portador i distribuidor de la seva pròpia informació personal, fent-la accessible a tercers a vegades amb cert risc i desconeixement, cosa que ha d'incrementar les mesures específiques de seguretat aplicades als exemples citats, més enllà de les previsions generals de la normativa (RLOPD).

Pel que fa a les aplicacions o serveis d'Smart City amb suport de geolocalització, qüestió a la que ens hem referit repetidament, hi ha diverses recomanacions de seguretat per al seu ús que els experts han anat manifestant[103], entre d'altres, la de configurar les opcions de localització de forma adequada a les necessitats de l'aplicació que es vol utilitzar (i, per defecte, podríem afegir, configurar les opcions menys "intrusives" per a l'usuari), controlar les actualitzacions de les aplicacions, en el sentit que, amb desconeixement de l'usuari, aquestes actualitzacions no modifiquin les condicions inicialment establertes, vigilar la vinculació de dades que estableixen algunes aplicacions de geolocalització amb les xarxes socials[104], o bé utilitzar xarxes segures o de confiança i recórrer al xifratge d'informació, quan aquesta així ho requereixi.

En relació amb les mesures de seguretat que podrien ser adients, recuperem també l'exemple relatiu a iniciatives "E-Call". En aquest cas, cal plantejar la conveniència de protegir el propi dispositiu que s'instal·la al vehicle (cosa que implicaria una seguretat

[102] Sobre això es pot consultar diversos vídeos disponibles a la xarxa, entre d'altres: "Barclays contactless cards users exposed to fraud"; "Always on-How to program your own NFC chips", així com notícies d'interès, entre d'altres: "Banc card details can be stolen with NFC" o "The risk inside your contactless smart oyster credit". (Veure DVD que adjuntem al document).
[103] Per exemple, la "Guia sobre seguridad y privacidad de las herramientas de geolocalización" d'INTECO, citada.
[104] Facebook, per exemple, està desenvolupament una aplicació per a smartphones, basada en la localització de contactes propers, és a dir, en el seguiment de la ubicació d'amics o contactes que l'usuari té en la xarxa social. (notícia apareguda a: www.valenciaplaza.com).

d'origen, és a dir, en la pròpia fabricació del dispositiu), a banda que la transmissió d'informació relacionada amb l'alerta, si escau, es faci de manera segura o xifrada.[105]

Si en el futur, en alguns exemples d'Smart City, com ara la mateixa E-call, o sistemes de pagament de peatges, o d'utilització de determinades vies reservades –tipus VAO-, etc, s'arribés a instal·lar en els vehicles algun tipus de "caixa negra", és a dir, un dispositiu que enregistrés determinades situacions (velocitat, pas per determinats punts, itineraris realitzats, localització, incidents, situació del propi conductor...), caldria també plantejar-se mesures específiques de protecció de la informació continguda, com ara evitar accessos indeguts, etc.

També caldria abordar la problemàtica específica que pot afectar a la informació generada pels comptadors intel·ligents. Entre d'altres, caldria que les consultes que han de poder fer els consumidors sobre el seu consum d'energia, es facin per Internet, a través del mòbil de l'usuari, etc, però en tot cas, de forma segura (amb connexions segures tipus https, evitant accessos de tercers, amb algun sistema d'autenticació, etc, en definitiva, protegir l'espai personal de consulta del propi usuari). Ara bé, probablement, el punt principal a debatre seria com es protegeix la informació personal des del mateix moment en què es genera i es recopila per part del comptador intel·ligent: com es transmet al responsable (xifratge de la informació, vies on-line segures...)?; qui pot accedir a la informació i quin grau d'identificació i d'autenticació cal exigir per a qualsevol persona que accedeixi a la informació (sistemes d'identificació i autenticació segurs, passwords)?; caldrà establir diferents rols d'accés, en funció de la informació que cal consultar (la informació que haurà de consultar la persona que emet la factura, no és la mateixa que la que hagi de consultar el comercial que pot valorar oferir un nou servei al client...)?; quin control d'accessos i traçabilitat és el més adient, per assegurar la gestió correcta de la informació i actuar contra accessos indeguts?; L'empresa subministradora vetlla perquè, en el cas que altres tercers pugin accedir a certa informació, es faci de forma agregada quan això no desvirtuï la finalitat perseguida?, etc. També caldria assegurar que els diversos "tercers" que poden accedir a les dades generades pels comptadors intel·ligents, aplicaran les mesures de seguretat adients. Sobre les mesures de seguretat en l'entorn dels comptadors intel·ligents, ens sembla especialment interessant l'estudi i

[105] Com s'apunta en el document citat del Grup de Treball de l'Article 29 sobre la iniciativa E-Call, de 2006.

recomanacions que ha fet l'Autoritat de Protecció de Dades francesa[106]. La CNIL recomana, entre d'altres, vetllar perquè els propis aparells o comptadors disposin de certificacions tècniques de seguretat; augmentar les mesures de protecció com major sigui el grau de detall de les dades de medició recollides; la realització d'anàlisis de riscos adequats; o que les violacions de dades es comuniquin als interessats, independentment que el Projecte de Reglament UE imposi finalment aquesta obligació.

5. ELS INSTRUMENTS PER A LA PROTECCIÓ DE LA PRIVACITAT: AVALUACIÓ D'IMPACTE SOBRE LA PRIVACITAT, TECNOLOGIES DE PROTECCIÓ DE LA PRIVACITAT, PRIVACITAT EN EL DISSENY I PRIVACITAT PER DEFECTE.

La normativa en matèria de protecció de dades ofereix als ciutadans afectats diferents instruments, per a la garantia dels seus drets davant els tractaments de dades que es puguin dur a terme en el context de les Smart Cities. N'hem vist alguns, com ara el dret d'informació o l'exercici dels drets ARCO, i n'hi ha altres com ara la creació i publicitat dels fitxers de dades de caràcter personal, actualment en procés de revisió, el requeriment d'informes, en alguns casos preceptius, de l'autoritat de control, en aquest cas l'Autoritat Catalana de Protecció de Dades, en el procediment d'elaboració de disposicions normatives que tinguin impacte en matèria de protecció de dades, la necessària implantació de mesures de seguretat o la possibilitat de presentar denúncies davant d'aquesta autoritat de control en cas de tractaments inadequats.

Ara bé, més enllà d'això, i tenint en compte les especials característiques d'aquest fenomen pels aspectes tecnològics inherents i especialment per l'amplia afectació que pot tenir per als ciutadans, tant pel nombre de ciutadans afectats com per la freqüència o quotidianitat amb que es poden veure sotmesos a un tractament d'aquest tipus, convé tenir presents altres instruments que poden permetre, en millor mesura, una protecció de forma preventiva o proactiva, és a dir, anticipant-se al moment en què pugui sorgir alguna incidència en el tractament de la informació personal afectada.

[106] Veure l'article: "La CNIL contrôle la sécurité des compteurs d'eau communicants"; les recomanacions fetes amb data 24 de gener de 2013, i la Délibération nº 2012-404 de 15 de novembre de 2012, tots els documents disponibles a la web: www.cnil.fr

Aquests plantejaments que encaixen en el que venim denominant com el model català de protecció de dades, englobarien instruments com ara l'avaluació d'impacte sobre la privacitat, la utilització de tecnologies de protecció de la privacitat, la privacitat en el disseny o la privacitat per defecte

Avaluació d'impacte sobre la privacitat (PIA)

D'entrada, l'anomenada avaluació d'impacte sobre la privacitat i la protecció de dades o PIA ("*Privacy impact assesment*" en la versió anglesa) hauria d'estar present per part de les autoritats (locals o supralocals) que pretenen desenvolupar experiències d'Smart City que afectin a dades personals.

Per PIAs, cal entendre el procés sistemàtic per avaluar l'impacte potencial dels riscos quan les operacions de tractament de dades puguin suposar riscos específics per als drets i llibertats dels interessats. El responsable o, si escau, l'encarregat del tractament, haurien de realitzar aquestes avaluacions.

El procés de PIA, pren especial rellevància en el desenvolupament de xarxes intel·ligents i ús de comptadors intel·ligents, com es desprèn de la Recomanació de 9.3.2012, citada (consideracions 4 a 6 de la Recomanació). En el marc d'aquesta Recomanació, la Comissió UE fins i tot preveu que els Estats haurien "adoptar i aplicar un "model" d'avaluació de l'impacte sobre la protecció de dades elaborat per la Comissió. Això és mostra de la repercussió que aquests sistemes tenen, clarament, en la protecció de les dades personals[107]. En qualsevol cas, la Recomanació marca un termini de 12 mesos (a partir de març de 2012) per fer aquest model de PIA, que a més es preveu que s'hagi de sotmetre a dictamen del Grup de l'Article 29.

Tecnologies de protecció de la privacitat (PET)

En segon lloc, en la configuració d'aquests serveis esdevé essencial la utilització de les anomenades "PET" ("*Privacy enhancing technologies*"), o tecnologies de protecció

[107] El SEPD es refereix específicament a aquest "model" de PIA previst, en el seu Dictamen de 8 de juny de 2012 sobre la Recomanació de 9.3.2012 que comentem. El SEPD considera molt adequat que es treballi en el disseny d'aquest model específic. Considerem un element de reflexió important considerar si es podria estendre l'experiència d'aquest "model" de PIA a d'altres experiències Smart Cities.

del dret a la intimitat (veure al respecte l'article 23 del Projecte de Reglament de protecció de dades de la UE). Respecte el concepte PET, com s'exposa en la Comunicació[108] de la Comissió al Parlament Europeu i el Consell "sobre el foment de la protecció de dades mitjançant les tecnologies de protecció del dret a la intimitat (PET)":

"...) en el proyecto PISA, que financia la UE, se entiende por PET un sistema coherente de medidas de TIC que protege el derecho a la intimidad suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin menoscabo de la funcionalidad del sistema de información. La aplicación de PET puede ayudar a diseñar sistemas y servicios de información y comunicación que reduzcan al mínimo la recogida y el empleo de datos personales y faciliten el cumplimiento de la normativa sobre protección de datos. En su Primer informe sobre la aplicación de la Directiva sobre protección de datos, la Comisión considera que «la aplicación de medidas tecnológicas adecuadas constituye un complemento fundamental de los medios jurídicos y debe constituir una parte de cualquier esfuerzo destinado a obtener un grado suficiente de protección de la intimidad». La utilización de PET debería dificultar o ayudar a detectar el incumplimiento de determinadas normas de protección de datos."

El foment de les PET en la pròpia indústria (que és un dels elements presents en la Comunicació citada), en l'àmbit de les Smart Cities, podria portar a "fomentar", o fins i tot "obligar" (aquest és un punt dubtós) a les empreses implicades en desenvolupar aplicacions d'Smart City, a incloure mesures de seguretat o utilitzar tecnologies especialment curoses amb la protecció de dades. La Comunicació citada ens dóna alguns exemple que creiem aplicables, en major o menor mesura, al tema que ens ocupa:

"En el dinámico contexto de las TIC, la eficacia en términos de protección de la intimidad, incluido el cumplimiento de la legislación sobre protección de datos, varía de una PET a otra y cambia con el tiempo. También la tipología de las PET es variada. Puede tratarse de una herramienta independiente, que el consumidor ha de comprar e instalar en su ordenador, o incorporada en la propia arquitectura de los sistemas de información. A continuación se mencionan varios ejemplos de PET:

- La anonimización automática de los datos tras un lapso de tiempo determinado obedece al principio de que los datos tratados deben guardarse en una forma que permita identificar al interesado únicamente durante el tiempo necesario para los fines iniciales para los cuales se facilitan los datos.
- Los instrumentos de cifrado que impiden el pirateo de la información transmitida por Internet responden a la obligación del responsable del tratamiento de datos de adoptar medidas adecuadas para proteger los datos personales frente al tratamiento ilícito.
- Los anuladores de *cookies*, que bloquean las *cookies* introducidas en un ordenador para que lleve a cabo determinadas instrucciones sin que el usuario tenga conocimiento de ello, responden al principio de que los datos deben tratarse de forma lícita y transparente y que ha de informarse al interesado del tratamiento que se realice.

[108] COM (2007) 228 final, Brussel·les, 2.5.2007.

- La Plataforma de Preferencias de Privacidad (P3P)[109], que permite a los usuarios de Internet analizar la política de los sitios web por lo que se refiere a la intimidad y compararla con las preferencias del usuario en relación con la información que desee facilitar, contribuye a garantizar que el interesado autoriza el tratamiento de sus datos con conocimiento de causa."

Tot i que cadascuna d'elles (o d'altres) requeriran un estudi més detallat respecte la seva possible aplicació a experiències Smart Cities, ens sembla que una d'elles, l'anonimització automàtica de dades (i ho relacionem amb l'adequada cancel·lació o bloqueig de dades, lògicament), pot ser plenament aplicable: si un ciutadà utilitza sistemes de targeta intel·ligent per cobrament electrònic de peatges, i el tractament principal és el cobrament corresponent, lògicament podem pensar que no hi ha possibilitat d'anonimització, però sí hi pot ser per a "finalitats aparellades", com ara fer un estudi de les franges horàries de major o menor utilització de la via, a efectes de regulació i millora del trànsit. o/ a banda de qüestions de facturació, el seguiment de les franges horàries de consum energètic en una vivenda, -sobre tot si, com sembla, es pretén fer estudis en funció del nombre d'habitants d'una llar, perfils....- l'anonimització sembla no només inevitable sinó exigible.

També caldria valorar les PET relativa a instruments de xifratge o, per exemple, -en el cas que una experiència Smart Cities posi a disposició del ciutadà una pàgina web a través de la qual inscriure's per rebre i utilitzar una targeta de transport intel·ligent-, es podria valorar la utilització de P3P, a banda, òbviament, d'assegurar el correcte compliment del deure d'informació a l'usuari.

Privacitat en el disseny (PbD)

La utilització d'aquestes tecnologies i les seves conseqüències és quelcom que cal plantejar des del mateix moment de la concepció del servei. Adquireix així especial rellevància el que es coneix com a la Privacitat en el Disseny o la Privacitat des del disseny ("*Privacy by Design*" (PbD)), per a tenir en compte l'aplicació de mesures i procediments tècnics i d'organització adequats per tal que un determinat tractament de dades satisfaci els requisits de la normativa de protecció de dades. La característica clau és que cal tenir en compte els efectes en la privacitat ja en el moment de "dissenyar" una determinada mesura d'Smart City. En relació amb la PbD cal fer

[109] "P3P" és un llenguatge estàndard que ofereix als usuaris una manera senzilla i automatitzada de controlar en major mesura l'ús que es fa de la seva informació personal en els llocs web que visita: http://www.w3c.es/Divulgacion/GuiasBreves/PrivacidadP3P

referència al treball "pioner" dut a terme des de l'Autoritat de Protecció de Dades d'Ontario (Canadà), en relació amb la definició dels "Set Principis Fundacionals de la PbD" [110], que esmentem breument a continuació[111]:

- Proactivitat i no reacció, prevenció i no correcció. Anticipar-se a la problemàtica que pot generar un tractament de dades. Compromís clar d'establir estàndards de protecció de dades, i buscar fórmules adequades de compliment.
- Privacitat com a configuració predeterminada. Cal definir abans de qualsevol tractament, qüestions com ara la finalitat específica de qualsevol fase del tractament, la minimització i possible anonimització de dades, limitacions d'ús, retenció i cessió...
-Privacitat integrada en el disseny. Integració en el disseny i l'arquitectura dels sistemes de tecnologies de la informació, i en les pràctiques de negoci. La protecció de dades no és un "annex", sinó forma part del nucli dur de la definició del sistema.
- Funcionalitat plena ("positive-sum, not zero-sum"), amb l'expressió "tothom hi guanya" (enlloc de l'esquema "el que un guanya l'altre ho perd"), es vol representar que tot suma per a la protecció de dades (com a exemple, la típica dicotomia entre seguretat i protecció de dades).
- Protecció de dades en tot el cicle de vida. El tractament de dades implica diverses fases (art. 3.c) LOPD), i el disseny les ha d'englobar totes. Així, cal assegurar la confidencialitat, integritat i disponibilitat de les dades en tot el cicle, incloent si escau la destrucció de les dades, així com els adequats controls d'accés.
- Visibilitat i transparència. Cada operació del tractament ha de ser transparent per a l'usuari (interessat, titular de la informació) i per a tots els intervinents.
- Respecte per la privacitat de l'usuari. El sistema PbD pivota sobre l'usuari, cal dotar-lo d'informació, capacitat de control (consentiment) i solucions amigables ("friendly"), dotant-lo d'un rol actiu en el tractament de les seves dades.

Sens perjudici d'una anàlisi més pormenoritzada[112], és clar que en el nostre estudi cal partir de la base de la plena aplicabilitat dels 7 principis esmentats a les experiències

[110] http://www.ipc.on.ca. Cal afegir que en la 32ª Conferència Internacional d'Autoritats de Protecció de dades (Jerusalem, octubre de 2010), es va reconèixer la PbD com un "component essencial de la protecció de la privacitat", i es van incorporar els anomenats "7 Principis fundacionals".

[111] Per a la traducció, es té en compte l'article "La protección inteligente de los datos personales: Privacy by Design (PbD)", de A. Brian Nougrères, RIPDP, nº 1, julio-diciembre de 2012, Bogotà. http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok6_-Ana-Brian Nougreres_FINAL.pdf

Smart Cities. Caldrà aplicar aquests principis tenint en compte les particularitats de cada tractament, entre d'altres, el nombre d'accessos i de responsables, encarregats i operadors implicats, les tipologies de dades, o la "voluntarietat" de l'interessat a l'hora d'utilitzar aplicacions d'Smart City.

Privacitat per defecte (PbDef)

Pel que fa a la Privacitat per Defecte ("*Privacy by Default*" (PbDef)), consisteix en l'aplicació de mecanismes per assegurar que, "per defecte", només es tractaran les dades personals imprescindibles i necessàries per a cada objectiu o finalitat específica de tractament. Aquest element té una relació molt directa, creiem, amb un dels principis de protecció de dades, com és el principi de qualitat, i més específicament el principi de minimització. De fet, en els textos consultats els experts fan menció reiterada, en relació amb els comptadors intel·ligents i el desplegament de xarxes intel·ligents, de la necessitat que es respecti el principi de minimització, és a dir, que "per defecte" es faci servir la mínima quantitat de dades, -i que aquestes es sotmetin al "mínim" tractament possible-, segons la finalitat (per exemple, no és el mateix el tractament de dades que haurà de fer la companyia subministradora d'un servei al consumidor final per donar el servei, que per facturar, o que per oferir si escau nous serveis al consumidor, etc).

També cal tenir present que el futur nou marc legal de protecció de dades a la UE, en procés de desenvolupament en el moment actual, vol donar carta de naturalesa a la PbD i a la PbDef.

Efectivament, en l'article 23 del Projecte de Reglament[113] del Parlament Europeu i del Consell, relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i la lliure circulació d'aquestes dades (Reglament general de protecció de dades), es preveu que:

[112] En relació, específicament, a l'aplicació de la PbD a les Xarxes Intel·ligents, ens remetem al document: "Achieving the Gold Standard in Data Protection for the Smart Grid" (juny 2010), de l'Autoritat de Protecció de Dades d'Ontario. www.privacybydesign.ca.
[113] COM (2012) 11 final; 2012/0011 (COD). Brussel·les, 25.1.2012,

"1. Habida cuenta de las técnicas existentes y de los costes asociados a su implementación, el responsable del tratamiento implementará, tanto en el momento de la determinación de los medios de tratamiento como en el del tratamiento propiamente dicho, medidas y procedimientos técnicos y organizativos apropiados, de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento y garantice la protección de los derechos del interesado.
2. El responsable del tratamiento implementará mecanismos con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada fin específico del tratamiento y, especialmente, que no se recojan ni conserven más allá del mínimo necesario para esos fines, tanto por lo que respecta a la cantidad de los datos como a la duración de su conservación. En concreto, estos mecanismos garantizarán que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas.
3. La Comisión estará facultada para adoptar actos delegados, (…)."

I no sembla descartable, vista la previsió de l'article 23.3 del Projecte de Reglament esmentat, que algun d'aquests "actes delegats" pogués referir-se, futurament, a l'aplicació de la PbD i la PbDef al desenvolupament de les xarxes i comptadors intel·ligents, o altres experiències d'Smart City

És clara la voluntat del legislador europeu d'incorporar la PbD i la PbDef a qualsevol tractament de dades personals. El responsable i, si escau, l'encarregat de tractar dades en el context de les Smart Cities, ja sigui en relació amb l'ús de recursos energètics (smart grids i smart metering), ja sigui en altres experiències d'Smart City, sempre que puguin afectar a dades personals (dels ciutadans, consumidors finals, dels usuaris de carreteres, persones físiques en definitiva...), haurà d'incloure aquesta perspectiva en el desenvolupament d'aquestes experiències.

6. LA NECESSITAT D'UN MARC NORMATIU ESPECÍFIC.

Més enllà de la normativa general en matèria de protecció de dades (fonamentalment la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD), i el seu reglament de desplegament aprovat pel Reial Decret 1720/2007, de 21 de desembre (RLOPD), de la qual es deriven els principis a què ens acabem de referir, no hi ha una normativa a nivell estatal que tracti de forma específica sobre la protecció de dades en l'àmbit d'aquestes aplicacions d'Smart City. Malgrat això, en aquest apartat ens referirem a una sèrie de normes (Directives que citarem), Recomanacions com la de 9.3.2012, citada, i Comunicacions de la UE, algunes ja

citades, que denoten d'entrada, l'interès i la necessitat de desplegar aquests sistemes per part dels Estats i les autoritats comunitàries[114].

Entre d'altres, destaquem la Comunicació de la Comissió "Smart Cities and Communities – European Innovation Partnership"[115], que crea un "partenariat", en el marc de l'estratègia que té com a horitzó l'any 2020, per mobilitzar els actors implicats en el cicle d'innovació que suposa el desenvolupament de les Smart Cities i les "comunitats intel·ligents". L'objectiu és accelerar a nivell UE el desenvolupament i implantació de tecnologies innovadores, per incrementar l'ús d'energies eficients i millorar la sostenibilitat del transport urbà. En relació amb això, la Comissió va endegar una consulta pública sobre el projecte "Smart Citites and Communities" (conclosa el 13.5.2011), del que destaquem l'informe elaborat per la Direcció General d'Energia, en el que s'inclouen informacions estadístiques sobre els objectius i àmbits ("eixos") de desenvolupament de les Smart Cities.[116]

Alguns dels textos que esmentem constaten la preocupació, en el marc de la UE, perquè la progressiva implantació de sistemes de xarxes i comptadors intel·ligents salvaguardin la privacitat i les dades personals de forma adequada. També els experts en matèria de protecció de dades alerten sobre la necessitat que es facin noves actuacions –normatives o complementàries- específiques per tal de protegir els drets dels ciutadans. Les valoracions són extenses, però és pertinent, com a mínim, apuntar aquest tema, ja que no només els sistemes de xarxes i comptadors, sinó també les diverses experiències d'Smart Cities, generen o poden generar un increment de tractaments de dades, que cal acotar, en el sentit d'aplicar-hi correctament els principis i obligacions de la protecció de dades.

Com s'ha apuntat, existeix un marc normatiu clar (i en procés de reforma) relatiu a la protecció de dades a la UE. Existeixen uns principis i obligacions ineludibles, d'aplicació per part de tot responsable que tracti dades personals a partir de la implantació d'experiències Smart Cities, sigui públic o privat.

[114] (D'especial interès, la Comunicació COM (2012) 202 final, de la Comissió al Parlament, el Consell (...) sobre "Redes inteligentes: de la innovación a la implantación", en què es posa de manifest la necessitat de treballar l'enfocament de protecció de la privacitat i les dades personals en la implantació d'aquests sistemes.
[115] C (2012) 4701 final, Brussel·les, 10.7.2012.
[116] També caldrà fer seguiment del "High Level Group" que es pretén endegar (previsió d'inici el 2014) en el sí d'aquesta iniciativa de "Smart Cities and Communities".

Ara bé, és necessari o convenient ampliar, completar o complementar el marc legal actual ("current legal basis", en terminologia anglesa), per tal de precisar l'aplicació, per exemple, del principi de minimització al tractament de dades en base a la finalitat?; Cal reforçar el deure d'informar els consumidors finals d'energia (gas, electricitat...) que tindran instal·lat un dispositiu a casa seva que tractarà determinades dades personals de consum, per tal que coneguin clarament els seus drets? Cal precisar l'abast del consentiment del ciutadà en determinades experiències Smart City? Fins a quin punt un consumidor final d'aigua o gas podrà "consentir", o oposar-se a la instal·lació de comptadors intel·ligents al seu domicili? Podrà retirar el consentiment, i amb quines conseqüències? En l'espai públic, caldria repensar les garanties de protecció de dades, per tal que el ciutadà conegui clarament quina experiència d'Smart City és innòcua per a la seva privacitat (no es tracten les seves dades) i quina no?.

En aquest sentit, citem com a exemple d'aquesta reflexió la Directiva 2009/73/CE, sobre normes comuns per al mercat interior del gas natural, així com la Directiva 2009/72/CE, sobre normes comuns per al mercat interior de l'electricitat (DOUE L 211, de 14.8.2009). Tot i que en aquests textos es fan mencions al tractament de dades de consum[117], el SEPD alerta que la base legal existent podria ser insuficient als efectes de fonamentar la legitimitat ex. art. 7 de la Directiva de 1995 de protecció de dades.[118] Es preveuen accessos a dades, utilització d'informació, etc. Tot el que pugui afectar a dades personals dels consumidors i accessos a aquestes dades, hauria d'estar adequadament previst pels corresponents textos normatius, sens perjudici de la inqüestionable aplicació de la Directiva de 1995 de protecció de dades i de la resta de normes aplicables a qualsevol tractament de dades.

[117] Considerant 50 de la Directiva 2009/73/CE, entre d'altres: "Un aspecto clave en el suministro a los clientes es el acceso a datos sobre el consumo objetivos y transparentes. Por ello, los consumidores deben tener acceso a sus datos de consumo, los precios asociados y los costes del servicio, de manera que puedan invitar a los competidores a hacer ofertas basándose en ellos. Por otra parte, también deben tener derecho a estar adecuadamente informados de su consumo de energía. (...)". L'article 21.10 de la mateixa Directiva disposa que: "10. El encargado del cumplimiento tendrá acceso a todos losdatos pertinentes y a las oficinas del gestor de la red de transportey a toda la información necesaria para el cumplimiento de su tarea."

[118] Punt 37 del Dictamen SEPD sobre la Recomanació de la Comissió Europea sobre el desenvolupament dels sistemes de comptadors intel·ligents, de 9.3.2012, que citem en aquest document.

No s'ha d'oblidar que els sistemes a gran escala de comptadors intel·ligents, generen un "consumer profiling", una creació de perfils dels consumidors finals. En aquest sentit, el SEPD adverteix que, en aquest context, el risc que suposa la mineria de dades -"data mining", entès com un tractament de dades de les persones que va més enllà del que inicialment podria fer pensar la finalitat objectiva del tractament, i que probablement escaparà del control i adequat coneixement de l'interessat-, és important, i cal controlar la possibilitat que només les parts autoritzades i no d'altres, tractin les dades adequades per a prestar el servei.

En la mateixa línea cal fer menció del Dictamen 12/2011 del Grup de l'Article 29, sobre medició intel·ligent, de 4 d'abril de 2011, on el Grup també exposa que cal reforçar el compliment dels principis i obligacions de la normativa de protecció de dades:

"Los contadores inteligentes permiten la generación, transmisión y análisis de datos sobre los consumidores en mucha mayor medida que el «contador tradicional» o «simple». Por lo tanto, permiten también al operador de red (también conocido como DSO, *Distribution Service Operator*), a los proveedores de energía y a otras partes recopilar información detallada sobre el consumo de energía y las pautas de utilización, así como adoptar decisiones relativas a consumidores individuales sobre la base de perfiles de utilización. Aunque se reconoce que estas decisiones generalmente benefician a los consumidores por el ahorro energético que traen consigo, también se está poniendo de manifiesto que puede producirse intrusión en la vida privada de los ciudadanos a través del uso de dispositivos instalados en sus hogares. Esto también implica un cambio en nuestra relación fundamental con los proveedores de energía, a los que tradicionalmente los consumidores han pagado por el gas y la electricidad suministrados. Con la introducción de los contadores inteligentes, el proceso es más complejo porque el interesado proporcionará a los proveedores información sobre sus hábitos personales."

Novament, com veiem, s'alerta sobre la creació de perfils dels consumidors, i la poca claredat respecte "qui i per a què" es podran utilitzar aquestes dades (no és el mateix el tractament –des de la perspectiva dels principis de qualitat i de finalitat que pot fer una empresa subministradora d'energia, que la que poden fer altres empreses que ofereixen serveis relacionats, ja que són un "tercer" que molt sovint no està prou identificat; en qualsevol cas, en aquests altres casos la finalitat haurà d'estar molt concretada, el tractament requerirà el consentiment de l'interessat –doncs ja no es tracta de la prestació "principal" d'energia o serveis-, i s'haurà d'informar adequadament a l'interessat.)

Hi ha qüestions, en definitiva, que afecten als principis de protecció de dades (exercici de drets, mesures de seguretat, deure d'informació, accés i tractament de dades de

consum per tercers, ajust del tractament a cada finalitat....) que, tal com demanen els experts (SEPD, Grup de l'Article 29, etc), haurien de concretar-se adequadament.

Com es fa referència en la Comunicació de la Comissió Europea "Energia 2020", citada, en què es fa referència a la "Iniciativa Ciutats Intel·ligents", la Comissió Europea (Direcció General d'Energia, a la que ja ens hem referit) ha creat un Grup especial sobre xarxes intel·ligents ("Smart Grids Task Force"), per debatre sobre la seva implementació a nivell europeu[119]. Aquest Grup especial s'estructura en diferents subgrups, dels que ens interessa especialment el "Grup d'Experts 2", centrat en estudiar l'impacte de les xarxes intel·ligents en la protecció de dades, i en elaborar recomanacions. Algunes d'aquestes recomanacions es relacionen amb l'aplicació de mesures de seguretat; amb la necessitat que els productes de xarxes intel·ligents, ja en la fase de disseny, incloguin estàndards apropiats de protecció de dades (inclús estudiar la implantació de nous estàndards de seguretat); amb la conveniència d'analitzar si el marc normatiu actual de protecció de dades (a la UE) és suficient, o caldria regular altres qüestions addicionals tendents, específicament, a protegir millor les dades personals de riscs aparellats a la utilització de xarxes intel·ligents; distingir adequadament el que és "dada personal" en aquest context; clarificar accessos i finalitats, valorar la problemàtica de TID en el marc de les xarxes intel·ligents, entre d'altres. Val a dir que aquestes són algunes de les qüestions que trobem presents –en certa manera "recurrent"-, també, en d'altres documents que analitzem en aquest treball (Grup de l'Article 29 i Grup de Berlín, SEPD...). Compartim la reflexió general que caldrà, partint probablement del marc ja existent de protecció de dades, especificar i explicar adequadament als ciutadans com s'apliquen els diferents principis i obligacions de la Directiva (i normativa derivada o complementària) als particulars tractaments de dades que poden sorgir en el context de les Smart Cities.

Finalment, és interessant considerar el paper i responsabilitat de cada Estat europeu en particular, a l'hora de treballar en actuacions normatives o complementàries -"guidelines", recomanacions, pautes per a les empreses del sector, operadors de serveis, Ajuntaments, etc...-, que puguin servir per a un correcte tractament de les dades en el context dels sistemes intel·ligents citats, extrapolables a d'altres experiències Smart Cities que comportin un tractament de dades personals.

[119] Es contenen diversos documents i estudis d'interès a la web: http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm

En concret citem un exemple, entre els diversos existents. Es tracta del procés de consulta pública que el Regne Unit (Departament d'Energia i Canvi Climàtic) ha dut a terme en relació amb l'"Smart Metering Implementation Programme".[120] En aquest procés el govern britànic ha analitzat diverses qüestions relatives a la protecció de dades en el marc de la implementació dels comptadors intel·ligents, que ens poden resultar molt útils a l'hora de reflexionar sobre les exigències derivades de l'aplicació dels principis de protecció de dades en les Smart Cities que volen implantar aquests sistemes de medició. Entre d'altres, es reflexiona sobre quin tipus de consentiment pot donar el consumidor final - persona física, quin accés a dades ha de tenir el propi consumidor[121], el subministrador d'energia, les empreses operadores, i "terceres parts". També es fa especial atenció a que el consumidor ha de rebre una informació acurada sobre el tractament que es generarà de les seves dades, quan, quines, i perquè es recolliran, qui les tractarà, quins drets poden exercir-se, on adreçar-se per exercir-los, etc. Es posa de manifest que no sempre caldrà tractar les mateixes dades (com a exemple "recurrent" que trobem en aquest i altres documents i dictàmens que hem analitzat per al nostre treball, és clar que no pot ser que es tractin les mateixes dades per a facturar, per a la bona gestió de la xarxa, que per a finalitats comercials, que per a oferir nous serveis als consumidors) o que cal aclarir qui són els "tercers" que podrien voler accedir a dades dels consumidors, i per a quines finalitats, etc..

7. CONCLUSIONS

Vistos els diferents punts, exemples, i documentació consultada, només ens queda apuntar algunes conclusions que, per tal d'evitar reiteracions, seran necessàriament breus, i sempre tenint en compte que no deixen de ser punts de partida per a una reflexió més detallada.

[120] Els documents es poden consultar a la pàgina: http://www.energy-uk.org.uk

[121] Aquesta Autoritat ha reflexionat en diversos Dictàmens sobre la capacitat que el titular de les dades personals pugui tenir un cert "marge d'actuació" en relació amb les dades tractades en el context de la seva Història Clínica Electrònica, o la carpeta personal de salut. De manera similar, podríem plantejar-nos si la progressiva implantació de comptadors intel·ligents deixarà marge "real" d'actuació al consumidor final, en el sentit de poden mantenir un cert marge de control sobre quines dades s'hi tracten, per a quines finalitats, qui hi pot accedir, etc.

1) Definir i situar adequadament el concepte d'Smart Cities i els elements principals que les configuren és rellevant als efectes de poder discernir quins casos poden comportar un tractament de dades personals i quins no, així com als efectes d'identificar les problemàtiques que es poden presentar en cada cas.

2) De la mateixa manera, és important estudiar els diferents conceptes relacionats amb les Smart Cities i les principals tecnologies emprades en aquest context, per tal d'identificar els punts d'interès o problemes que es poden generar des de la perspectiva de la protecció de dades.

3) Moltes experiències o exemples d'Smart Cities no impliquen, o no haurien d'implicar, el tractament de dades personals i, per tant, sens perjudici de la seva importància, interès, o major o menor implantació a les nostres ciutats, són alienes a aquest estudi, llevat que en el futur puguin generar algun tractament de dades de caràcter personal.

4) Pel que fa a la resta, el tractament de dades que generen les diferents experiències Smart City pot ser molt divers. És en aquests casos que cal analitzar els elements rellevants (tecnologies emprades, incidència en els diferents principis rectors en matèria de protecció de dades, instruments per millorar la garantia de privacitat, necessitat de precisar-ne el marc normatiu aplicable...), i establir correctament les interaccions entre tots aquests elements.

5) Pel seu impacte en la privacitat i la protecció de dades, cal fer especial atenció a la implantació de xarxes i comptadors intel·ligents, a les diferents tecnologies que podem agrupar en el desenvolupament de "l'Internet de les coses", i a d'altres tecnologies estudiades en aquest document, així com a l'especial problemàtica de la geolocalització d'objectes i persones, i a la possibilitat de generar perfils. Tot això pot comportar una especial afectació per a la vida quotidiana dels ciutadans, en concret, per a la seva privacitat i per al dret a la protecció de dades personals.

6) A través del desenvolupament de les Smart Cities, la persona física es converteix, progressivament -i sovint sense ser-ne gaire conscient-, en portadora i distribuïdora de la seva pròpia informació personal, fent-la accessible a tercers, de forma no sempre segura.

7) Convé estudiar la utilització de models o arquetips, així com la utilització de pseudònims, la gestió de diverses identitats digitals per part de l'usuari, així com el recurs a l'anonimització o pseudoanonimització de dades, en diferents fases del disseny i implantació d'exemples d'Smart Cities, per tal d'assegurar una major garantia per a la privacitat i la protecció de dades personals.

8) Tenint en compte això, tant el propi titular de la informació personal objecte de tractament com els diferents responsables implicats -administracions públiques, sector privat i empresarial, tercers intervinents en el desenvolupament i implantació dels diversos exemples d'Smart Cities-, així com les autoritats i operadors en matèria de protecció de dades, han de tenir presents els diferents principis, garanties i obligacions exigibles en matèria de protecció de dades i aplicar-los, cadascú des de la seva perspectiva i grau de responsabilitat.

9) Principis de legitimitat, consentiment i finalitat: qualsevol tractament de dades personals que pugui generar un exemple d'Smart City s'ha de fonamentar en una finalitat legítima. A partir d'això, cal establir una fonamentació clara de la legitimitat de cada tractament específic, i distingir la finalitat principal dels diferents usos derivats o secundaris, restringint, si escau, el tractament de dades en aquests usos. Cal distingir els supòsits en què hi ha necessitat de consentiment, d'aquells en què no és necessari. Pel que fa al consentiment, cal reflexionar sobre l'impacte que un ús opcional o obligat de serveis d'Smart City té per a la privacitat i la protecció de les dades d'aquest usuari. Cal fer especial atenció a la legitimitat i consentiment en determinats casos, com ara el tractament de dades sensibles, o de dades de menors.

10) Principi de qualitat i de minimització: per bé que no es pot generalitzar i trobar una base comuna pels diferents supòsits d'Smart City pel que fa a les dades que es poden tractar, cal donar a aquest principi una rellevància clau. Cal evitar o, al menys, controlar els tractaments que generen mineria de dades, elaboració de perfils o seguiment de pautes de consum, seguiment, monitorització o localització de vehicles i persones, en definitiva, els tractaments que podrien resultar abusius degut a la informació tractada. En la mesura del possible, cal estudiar la viabilitat de l'anonimització de les dades, sense desvirtuar la finalitat, en diversos exemples d'Smart City. I més enllà d'això, cal analitzar les capacitats d'interoperabilitat dels

diferents sistemes, ja que els diferents conjunts de dades, que no són especialment rellevants de manera aïllada, si es processen en un mateix entorn poden generar efectes no desitjats.

11) Principi d'informació: cal prioritzar la informació transparent, és a dir, accessible i entenedora en el marc de les Smart City, atenent a les particularitats de les tecnologies emprades i al nivell de comprensió de l'usuari. Cal plantejar si el deure d'informació que el responsable ha de complir, pot incloure determinades especificacions, com ara les relatives a les mesures i consells de seguretat a aplicar pel propi usuari depenent de la tecnologia implicada en el tractament, la possibilitat de gestionar les dades pròpies per part de l'usuari, la conservació de les dades o la seva portabilitat, entre d'altres. Tot això, en el context de la informació que pot ser exigible en el nou marc normatiu europeu, per garantir "un tractament de dades lleial".

12) Exercici de drets per les persones interessades: l'exercici dels drets ARCO, més enllà de la seva aplicació en qualsevol tractament de dades, presenta dificultats o dubtes específics en el context de les Smart Cities, que han de ser valorats. Entre d'altres, cal estudiar aquells casos en què pot ser dificultós, per a l'interessat, identificar les dades tractades; com es pot donar accés a les dades personals de l'interessat en forma llegible i intel·ligible; els casos en què l'usuari pot tenir dificultat per acreditar la pertinença de la rectificació o la cancel·lació. També cal tenir en compte les particularitats del dret d'oposició, així com l'anomenat silenci dels xips o el desenvolupament en el futur marc normatiu europeu dels "nous drets", com ara el dret a la portabilitat de dades o a no ser objecte de mesures basades en l'elaboració de perfils, en relació amb exemples diversos d'Smart Cities.

13) Pel que fa a les mesures de seguretat: cal incidir en els riscos particulars per a la seguretat de la informació personal tractada en el context de les Smart Cities, a causa de les particularitats de les tecnologies emprades (RFID i NFC, aplicacions o serveis amb suport de geolocalització, targetes contactless...), i valorar la pertinença de donar més i millor informació a l'usuari sobre les mesures de seguretat que pot o ha d'adoptar com a usuari, més enllà de les que ja ha d'aplicar el responsable.

14) Les avaluacions d'impacte sobre la privacitat (PIA), la utilització de tecnologies per a la protecció de la privacitat (PET), l'aplicació de la Privacitat en el disseny (PbD), o la

privacitat per defecte (PbDef), constitueixen instruments necessaris qua cal valorar i aplicar a exemples concrets d'Smart Cities, ja que permeten afrontar amb majors garanties la seva implantació.

15) Independentment de la implantació d'aquests instruments específics de la protecció de dades, caldria analitzar i valorar fins a quin punt pot ser necessari un desenvolupament normatiu específic a nivell de la UE o a nivell intern, en relació amb el desenvolupament de determinats serveis d'Smart Cities, per tal d'assegurar adequadament la privacitat i la protecció de dades de les persones físiques en aquest context.
