FACULTAT DE DRET

UNIVERSITAT DE BARCELONA

LA PROTECCIÓ DE DADES EN EL CONTEXT DE L'*INTERNET OF THINGS* I EL *BIG DATA*

TREBALL FINAL DE GRAU

Autora: Andrea González Fuentes

NIUB: 16458400

Àrea temàtica: Dret Mercantil

Tutora: Prof. Ginebra Comellas i Estibal

Curs: 2016/2017

SUMARI

1. INTRODUCCIÓ 4

2. DEFINICIONS 6

2.1. Internet of Things (IoT) 6
2.2. Intel·ligència artificial 8
2.3. Big Data 9

3. MARC LEGAL 12

3.1. Normativa internacional 12
3.1.1. Open Government Partnership 13
3.1.2. OCDE 14
3.2. Normativa europea 14
3.2.1.Carta dels Drets Fonamentals i Tractat de Funcionament 15
3.2.2. Agenda Digital Europea 16
3.2.3. Mercat Únic Digital 16
3.2.4. Economia de les dades europea 17
3.2.5. Directiva 95/46/CE i Reglament General de Protecció de Dades.....18
3.2.6. Directiva 2002/58/CE 19
3.3. Normativa espanyola 19
3.3.1. Constitució Espanyola de 1978 19
3.3.2. LOPD i Reglament de desenvolupament de la LOPD 20
3.3.3. Llei de Serveis de la Societat de la Informació 21
3.4. Anàlisi del Dictamen 8/2014 del Grup de Treball de l'article 29 21
3.4.1. El Grup de protecció de les persones i el Comitè Europeu de protecció de dades 21
3.4.2. Problemes de protecció de dades i solucions conforme la normativa..... 22
3.4.3. Responsables del tractament 28
3.4.4. Drets de l'interessat 29

4. BIG DATA 31

4.1. Aplicació del Big Data a la pràctica 31
4.1.1. Primera fase 31
4.1.2. Segona fase 32

4.2. Solucions proposades per la normativa del Big Data 32
4.2.1. Desplaçament del requisit del consentiment 32
4.2.2. Introducció de la privacitat per defecte i privacitat des del disseny 33
4.2.3. La propietat de les dades 34
4.2.4. L'apoderament dels individus 34

CONCLUSIONS 37

BIBLIOGRAFIA 39
Referències bibliogràfiques 39
Articles 39
Referències legislatives 40
Sentències 42
Pàgines web 42

1. INTRODUCCIÓ

En els darrers anys s'han produït grans progressos tecnològics que es reflecteixen especialment a la forma de relacionar-se. En efecte, avui és gairebé impossible trobar a algú que no tingui *smartphone*, però l'evolució tecnològica té altres conseqüències: cada vegada és més comú la connexió a internet de dispositius, com electrodomèstics, vehicles i tot tipus d'objectes quotidians. Tant és així que la consultora tecnològica Gartner Group ha previst que a l'any 2020 ja hi haurà uns 21 mil milions de dispositius connectats[1].

L'adopció d'aquests dispositius comporta beneficis tant per a les empreses com per als consumidors, atès que aporta un valor afegit a les organitzacions que n'aprofiten l'ús al reduir costos, augmentar la productivitat o crear noves oportunitats de negoci; mentre que beneficia als usuaris que obtenen una millor experiència ja que, per exemple, els pot facilitar o millorar l'experiència de compra.

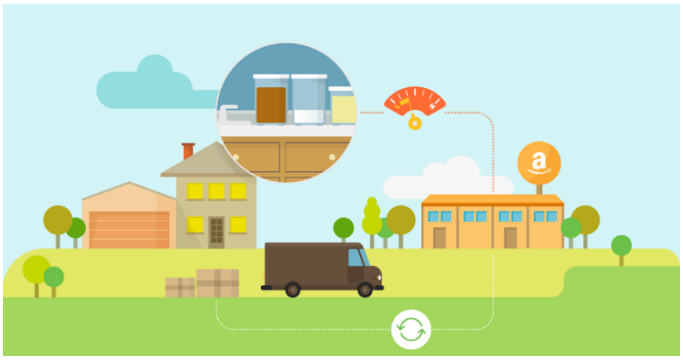
Amazon Dash Button associat a la marca Ariel.

N'és un exemple clar el *Dash Button* d'Amazon[2], un dispositiu en forma de botó que permet demanar un producte només amb un clic. Aquests dispositius es connecten a l'aplicació d'Amazon mitjançant *wifi,* s'associen a una marca i es configuren amb l'aplicació per triar el producte amb el que funcionarà (de moment, els productes disponibles només són bàsics com, per exemple, rentavaixelles). L'idea és que el consumidor col·loqui el botó al costat de la pica per poder demanar el rentavaixelles fàcilment en el moment en que el producte s'esgoti o estigui a punt d'esgotar-se. El que busca l'empresa és evitar el moment en que el consumidor arribi a quedar-se sense el producte.

Una altra tecnologia que ha posat en marxa Amazon és el *Dash Replenishment Service* (DRS)[3], que permet que els propis dispositius demanin el producte quan s'esgoti. Aquest servei està dirigit directament a les empreses que poden incorporar en els seus dispositius el DRS, sempre i quan els dispositius es connectin a internet. Pel seu funcionament, és necessari incorporar-hi uns sensors per tal que puguin detectar quan s'està esgotant el producte que utilitzen, així, el servei beneficia als usuaris que, també en aquest cas, hauran de seleccionar al començar a utilitzar el dispositiu quin és el producte que es demanarà automàticament. El DRS es pot fer servir amb qualsevol aparell i algunes empreses, com Samsung, ja l'utilitzen als seus electrodomèstics. Un bon exemple són les impressores de la marca en les que ja s'inclou aquest sistema, de

[1] Chet GESCHICTER, Kristin R. MOYER. Measuring the Strategic Value of the Internet of Things for Industries < https://www.gartner.com/doc/3299317?refval=&pcp=mpe > [Consulta: 08/04/2017]
[2] Amazon Dash Button. < https://www.amazon.es/b?ie=UTF8&node=10909716031> [Consulta: 07/04/2017]
[3] Amazon Dash Replenishment Service. <https://developer.amazon.com/dash-replenishment-service> [Consulta: 07/04/2017]

manera que quan la impressora detecta que s'està esgotant la tinta que fa servir, la demana automàticament a Amazon.



Esquema del funcionament del Dash Replenishment Service.

El plantejament d'aquest treball sorgeix a partir del coneixement d'aquests i d'altres exemples de dispositius connectats, que formen part del denominat *Internet of Things,* una xarxa mitjançant la qual els diferents objectes connectats capturen informació a través de sensors, possibilitant la seva intercomunicació. Crida l'atenció que, encara que aquestes tecnologies ja són tota una realitat i afecten a nombroses branques del dret, la legislació al respecte és molt parca. Per aquest motiu, el present Treball de Fi de Grau té com a objectiu fer un anàlisi de la legislació aplicable a l'*Internet of Things* (i, en conseqüència al *Big* Data) en matèria de protecció de dades.

En primer lloc, la hipòtesi que es planteja és, **si el règim actual de protecció de dades és l'adequat per les noves tecnologies o si, pel contrari, és necessària una reforma més profunda que la produïda pel Reglament General de Protecció de Dades de la Unió Europea.**

En segon lloc, sorgeix la qüestió de la compatibilitat entre la protecció de les dades personals i la lliure circulació de les mateixes en un context com és el de l'*Internet of Things* i el *Big Data,* en el qual les dades es caracteritzen pel volum, la velocitat, la varietat, la veracitat i el valor.

2. DEFINICIONS

2.1. Internet of Things (IoT)

L'*Internet of Things*[4] es pot definir, d'una manera senzilla, com la xarxa d'objectes o dispositius que capten dades mitjançant sensors i es comuniquen amb d'altres dispositius gràcies a la connexió a internet.

Aquest concepte sorgeix el 1999 de la mà de Kevin Ashton qui el va fer servir per primera vegada a una presentació a Procter & Gamble. L'utilitzà per referir-se a l'idea de que les coses poguessin recopilar informació per elles mateixes sense necessitar que les persones introdueixin la informació en ordinadors o dispositius, d'aquesta manera els ordinadors podrien rastrejar i comptar qualsevol cosa, de manera que es podrien reduir costos i pèrdues.[5]

Trobem una definició més amplia al Dictamen 8/2014 sobre l'evolució recent de l'*Internet of Things* del Grup de Treball sobre la protecció de dades de la Comissió Europea:

> *"El concepto de Internet de los objetos (IO) se refiere a una infraestructura en la que miles de millones de sensores incorporados a dispositivos comunes y cotidianos («objetos» como tales, u objetos vinculados a otros objetos o individuos) registran, someten a tratamiento, almacenan y transfieren datos y, al estar asociados a identificadores únicos, interactúan con otros dispositivos o sistemas haciendo uso de sus capacidades de conexión en red."*

Cal destacar, d'altra banda, la definició de la Unió Internacional de Telecomunicacions (UIT)[6]:

> "*Internet de los objetos (IoT): Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperatividad de tecnologías de la información y la comunicación presentes y futuras.*
>
> *NOTA 1 – Gracias a la identificación, la adquisición y el procesamiento de datos y a las capacidades de comunicación, IoT hace pleno uso de los objetos para ofrecer servicios a todo tipo de aplicaciones, garantizando a su vez el cumplimiento íntegro de los requisitos de seguridad y privacidad*
>
> *NOTA 2 – Desde una perspectiva más amplia, IoT puede considerarse una noción con repercusiones tecnológicas y sociales."*

Les definicions de l'IoT s'enfoquen a diversos aspectes del mateix i emfatitzen, per exemple, en aspectes tècnics (com l'internet, l'interconnectivitat, etc.) o en els components del mateix (com els objectes o els sensors), però crida especialment l'atenció la definició de la UIT per les dues notes que l'acompanyen.

A la primera nota es fa referència al tractament de dades, ja que tracta de la identificació, captació, processament i comunicació de dades mitjançant l'IoT per oferir serveis a aplicacions. La referència al tractament de dades també apareix a la definició de la Comissió Europea i en moltes d'altres definicions. Això fa patent, doncs, que es tracta

---

[4] Conegut en Català com Internet de les Coses o Internet dels Objectes.

[5] Kevin ASHTON, *That "Internet of Things" Thing.*. RFID Journal, 2009 <http://www.rfidjournal.com/articles/view?4986 > [Consulta: 08/04/2017]

[6] Recomanació Y.2060 de la Unió Internacional de Telecomunicacions, de 15 de juny de 2012, Descripció General de Internet dels Objectes.

d'una infraestructura pròpia de la societat de la informació, però que ha aconseguit un intercanvi de dades molt més elevat que els que es produïen fins ara.

És destacable en aquesta última definició la referència als dos grans problemes de l'IoT, la seguretat i la privacitat. L'UIT mostra la seva preocupació a l'incloure aquesta nota en la que afirma que el tractament de dades i les aplicacions que ofereixen l'IoT asseguren que els requisits de seguretat i privacitat es compleixen.

També cal comentar la nota 2 en la que s'admet que, en un sentit més ampli, l'IoT es pot percebre com una visió amb implicacions tecnològiques i socials. S'entén que, en aquest sentit, es fa referència al gran avenç tecnològic que es coneix com la tercera onada tecnològica i a les implicacions socials (i, fins i tot, ètiques) que en són conseqüència.

La connexió d'objectes a internet no és una novetat, però s'ha impulsat l'Internet de les coses degut a diferents tendències tecnològiques com la connectivitat de baix cost i d'alta velocitat, la miniaturització, els avenços en l'anàlisi de dades i el sorgiment del *cloud computing.*[7]

Es pot classificar l'IoT de diferents formes, per exemple, el Dictamen 8/2014 proposa una classificació per raó del tipus de suport o dispositiu:

- ***Wearables* (ordinadors corporals)**: són objectes quotidians, com roba o complements que incorporen altres funcionalitats; en són exemple els *smartwatches* o altres dispositius com ulleres de sol o peces de joies.[8]

- ***Quantified self* (jo quantificat)**: són dispositius que registren dades relatives a l'activitat o l'estil de vida, per tant recullen dades sobre la salut de les persones, que poden servir tant a l'usuari com a les empreses que recullen informació. El Dictamen 08/2014 ressalta que el tipus de dades que recullen aquests dispositius són especialment sensibles donada la seva naturalesa.

- **Domòtica**: són dispositius integrats a la llar, com els electrodomèstics, alarmes o termòstats. El problema que destaca en aquest cas el Dictamen és que aquests dispositius solen estar constantment rebent i enviant dades al fabricant, la qual cosa planteja greus problemes de privacitat i de seguretat. Recentment, l'assistent domèstic d'Amazon va realitzar en diverses llars dels EUA la compra d'una casa de nines, després de que aparegués una noticia a la televisió en la que es donava una ordre de compra; la qual cosa va provocar una gran alarma respecte aquest problema.[9]

Cal tenir en compte que aquesta classificació, a la pràctica, no comporta l'existència de dispositius completament diferenciats, sinó que poden haver *wearables* que també constitueixen *quantified self.*

---

[7] Karen ROSE, Scott ELDRIDGE, Lyman CHAPIN. La Internet de las Cosas-Una breve reseña. pàg. 14.

[8] Marques com Michael Kors, Tory Burch o Swarovski tenen línies de joiera que registren l'activitat física o les hores de son.

[9] Fox News Tech. TV news report prompts viewers' Amazon Echo devices to order unwanted dollhouses <http://www.foxnews.com/tech/2017/01/06/tv-news-report-prompts-viewers-amazon-echo-devices-to-order-unwanted-dollhouses.html> [Consulta: 08/04/2017]

La classificació que es proposa al Dictamen es centra en aquestes tres categories per analitzar-les en base a la legislació sobre protecció de dades perquè són dispositius i serveis que es troben efectivament en ús i perquè es connecten a l'usuari mitjançant una interfície directa. Tanmateix, l'IoT no només s'utilitza en aplicacions B2C, el seu ús en l'àmbit B2B i M2M[10] és molt estès. Per exemple, en qüestions globals com les ciutats intel·ligents o la conducció autònoma, es produeixen nombrosos intercanvis de dades entre màquines. Tot i això, el Dictamen no se'n ocupa d'aquestes qüestions, sens perjudici que tots els principis i recomanacions continguts en ell són d'aplicació a totes les modalitats d'Internet de les Coses.

2.2. Intel·ligència artificial

La intel·ligència artificial (o AI, per les seves sigles en anglès) va ser definida per John McCarthy, el creador del concepte, com "la ciència i l'enginyeria de crear màquines intel·ligents, especialment, programes informàtics intel·ligents."[11] Es pot considerar que la intel·ligència de les màquines ve donada per la capacitat d'aprendre i adaptar el seu comportament als estímuls als que els sotmeten.

El tema de la intel·ligència artificial es tracta, en nombroses ocasions, juntament amb el de la robòtica; tal com ho fa la Comissió d'Assumptes Jurídics del Parlament Europeu en el seu Informe, de 27 de gener de 2017, amb recomanacions destinades a la Comissió sobre normes de Dret civil sobre robòtica que tracta conjuntament la intel·ligència artificial i la robòtica. Tot i això, cal tenir en compte que, per parlar d'intel·ligència artificial no és necessari que existeixi un suport físic.

A l'informe no s'ofereix una definició d'intel·ligència artificial, però es proposen unes característiques per la definició dels robots intel·ligents:[12]

- Capacitat d'adquirir autonomia mitjançant sensors i/o mitjançant l'intercanvi de dades amb el seu entorn i l'intercanvi i anàlisi d'aquestes dades. Aquesta característica es refereix amb total claredat a l'IoT, doncs són dues qüestions que es troben profundament relacionades, ja que les dades que es recullen mitjançant els sensors dels dispositius connectats permeten que les màquines dotades d'intel·ligència les analitzin i augmentin el seu coneixement.

- Capacitat d'autoaprenentatge a partir de l'experiència i la interacció. La segona característica tracta de l'autoaprenentatge que adquireixen els robots a través de l'experiència, és a dir, de les dades que reben i analitzen. En quant, la interacció es considera que es un criteri no necessari, per parlar de robòtica intel·ligent.

---

[10] Les aplicacions B2C (*business to consumer*) són aquelles que estableixen una relació entre una empresa i un usuari final o consumidor, les aplicacions B2B (*business to business*) permeten les relacions entre empreses, i les aplicacions M2M (*Machine to machine*) es refereixen a l'intercanvi d'informació entre màquines.

[11] MCCARTHY, John. *What is artificial intelligence?* Stanford University, 2007. < http://www-formal.stanford.edu/jmc/whatisai/ > [Consulta 11/04/2017]

[12] Informe, de 27 de gener de 2017, amb recomanacions destinades a la Comissió sobre normes de Dret civil sobre robòtica de la Comissió d'Assumptes Jurídics del Parlament Europeu.

- Un suport físic mínim. Existeix la necessitat, per parlar de robot, d'un suport físic, tanmateix, cal ressaltar que es tracta d'un suport mínim. És cada cop més freqüent l'aparició de nano-bots, que poden mesurar només uns mil·límetres. Si no hi ha aquest suport físic, s'està davant d'una mera intel·ligència artificial.

- Capacitat d'adaptar el seu comportament i accions a l'entorn en el que es situen. En aquesta capacitat radica la característica principal dels robots intel·ligents.

- Inexistència de vida en sentit biològic. Aquest és un límit que es pretén establir per qüestions ètiques, existeixen robots de materials orgànics però no poden crear-se robots que constitueixin vida.

Es plantegen a l'Informe diferents qüestions, tant ètiques com jurídiques: d'entre d'altres temes, es discuteix la responsabilitat jurídica pels danys que puguin ocasionar les actuacions dels robots, proposant un tercer tipus de personalitat, la personalitat electrònica per aquells robots que puguin prendre decisions autònomes o que puguin interactuar independentment i es proposa la creació d'un sistema global de registre de robots dins la Unió Europea. També es fa referència a la necessitat de garantir la llibertat, la intimitat, la integritat i la dignitat, així com la protecció de dades personals, garantida a l'article 16 del TFUE. S'hi fa especial èmfasi a la importància de garantir la seguretat dels sistemes, especialment en aquells que es trobin interconnectats (és a dir, en aquells en que entri en joc l'IoT) i es recalca que la responsabilitat de que aquests dispositius siguin fiables correspon als dissenyadors.

A més, a l'Informe es fa una enumeració de diferents dispositius dotats d'intel·ligència artificial que han de ser regulats i que, coincideixen, en la majoria de casos amb dispositius connectats a la xarxa de l'*Internet of Things:* mitjans de transport autònoms, com vehicles autònoms i drons; robots assistencials i robots mèdics.

2.3. Big Data

El concepte de *Big Data* s'aplica a la informació que, pel gran volum de dades, no pot ser gestionada i analitzada pels procediments o eines tradicionals ja que supera la capacitat d'aquests.[13]

La definició que ofereix el grup Gartner es basa en tres característiques[14]:

> "El Big Data són els actius d'informació de gran volum, gran velocitat i/o gran varietat que demanen formes rendibles e innovadores de processament d'informació que permetin un millor coneixement, presa de decisions i automatització de processos."[15]

És a dir, es refereixen al *Big Data* com els actius d'informació de gran volum, gran velocitat i/o gran varietat. Per tant, no només es tracta d'una gran quantitat de dades sinó que són dades molt heterogènies i que, en moltes ocasions, es capturen i analitzen a temps real. La definició de Gartner continua matisant que aquest tipus de dades

[13] LÓPEZ LÓPEZ, Jose Carlos. El Economista. *La moda del Big Data: ¿En qué consiste en realidad?* <http://www.eleconomista.es/tecnologia/noticias/5578707/02/14/La-moda-del-Big-Data-En-que-consiste-en-realidad.html> [Consulta 10/04/2017]
[14] Gartner IT Glossary. <http://www.gartner.com/it-glossary/big-data> [Consulta: 09/04/2017]
[15] Traducció pròpia.

demanen formes rentables e innovadores de processament de la informació que permetin un millor coneixement, presa de decisions i procés d'automatització.

En realitat, són cinc les característiques a tenir en compte, a les quals sovint se les anomena com les 5Vs del *Big Data:*

- Volum: es tracta de grans quantitats de dades que superen la capacitat dels *softwares* habituals.

- Varietat: són dades molt heterogènies ja que es recullen de diverses fonts, com dispositius connectats, xarxes socials, etc.

- Velocitat: les dades es recullen, processen i es pren decisions a partir d'elles amb una gran rapidesa, de vegades, fins i tot a temps real.

- Veracitat: es refereix a la confiança en les dades, que tenen una qualitat superior atès les fonts de les quals s'extreuen.

- Valor: les dades han adquirit una gran importància pel negoci.

El *Big Data* és, per a moltes empreses, una oportunitat de negoci. Per exemple, el sector bancari és un dels beneficiats directament ja que amb la gestió d'aquestes dades poden fer anàlisis de frau i de risc a temps real. Les oportunitats, però, són molt variades i no es redueixen a l'àmbit bancari, es pot aplicar al màrqueting, a la segmentació de clients, a la presa de decisió, a la planificació, etcètera.[16] De fet, un dels negocis en auge, és el de l'intercanvi d'informació.

La Unió Europea considera la informació digital com una font essencial pel desenvolupament econòmic, la competitivitat, la innovació, la creació de llocs de feina i el progrés de la societat. Així, la Comissió Europea ha aprovat recentment la Comunicació de 10 de gener de 2017 sobre "La Construcció d'una economia de les dades europea" amb l'objectiu principal de crear un marc jurídic per l'economia de les dades, eliminar els obstacles a la lliure circulació de dades i posar fi a la inseguretat jurídica sobre responsabilitat i seguretat en relació amb els dispositius interconnectats, com és el cas dels dispositius de l'IoT.

Les dades que conformen el *Big Data* es poden classificar segons el seu origen[17]:

- Web i xarxes socials

- *Machine-to-machine* (M2M): fa referència a aquelles dades que són obtingudes sense que les introdueixin persones, són les pròpies màquines les que capturen la informació i la traspassen a altres màquines. Així actuen molts dispositius d'IoT.

---

[16] BBVA. Innovation Edge. *Big Data: Es hora de generar valor de negocio con los datos.* <http://www.centrodeinnovacionbbva.com/innovation-edge/big-data/big-data-vision-general > [Consulta: 17/04/2017]

[17] BARRANCO FRAGOSO, Ricardo. *¿Qué es Big Data?* IBM developer Works. <https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/> [Consulta: 10/04/2017]

- *Big transacion data:* es tracta del registre de transaccions tant de facturació com registres de trucades o altres dades.

- Biomètrica: s'hi inclouen les empremtes digitals, el reconeixement facial, etc.

- Generades pels humans: documents, correus electrònics, trucades i qualsevol dada que introduïm a dispositius connectats.

La conclusió que resulta de les definicions que s'han donat en aquest apartat és que l'aparició del *Big Data* està lligada amb l'IoT i amb la intel·ligència artificial, ja que són els seus dispositius els que més dades enregistren. Per tant, es pot afirmar que l'IoT i la intel·ligència artificial persegueixen en últim terme la consecució d'un *Big Data* que avui en dia ja comença a esdevenir una realitat. En altres paraules, l'IoT busca aconseguir dades, donat que ens trobem en un moment en que la informació i les dades són cada cop més importants i generen grans avantatges competitius i grans oportunitats de negoci.

En aquest punt, els beneficis de la tecnologia es troben enfrontats amb la protecció de les dades i la privacitat, ja que el negoci de la informació comporta l'intercanvi d'aquestes dades que sovint poden haver estat capturades sense consentiment o poden vulnerar la intimitat i la privacitat de les persones.

Com es veurà a l'apartat 3.2.3 d'aquet treball, la Unió Europea persegueix l'establiment d'un espai d'intercanvi de dades europeu i ho fa mitjançant:

- La creació del Mercat Únic Digital, un espai de lliure circulació on poder realitzar i accedir a les activitats en línia de tota la Unió Europea sense restriccions. Aquest objectiu té un sentit econòmic i jurídic, doncs es pretenen eliminar els obstacles existents, tant físics com legals, per poder dur a terme aquest mercat únic. A més, també es planteja l'establiment de legislacions unitàries en el marc comunitari per poder aconseguir aquest objectiu.

- La creació de l'Economia de les Dades Europea és un objectiu molt més concret. En tant que l'economia es basa cada cop més en les dades i la tecnologia, es pretén crear un marc en el que els agents del mercat garanteixin dades accessibles i utilitzables. L'Economia de les Dades Europea s'ha de basar en el principi de lliure circulació, tot respectant la privacitat e intimitat de les persones.

3. MARC LEGAL

És evident que la novetat de la matèria impedeix que existeixi una regulació que estudiï *l'Internet of Things* i el *Big Data* a fons i que es detingui a les particularitats que aquestes tecnologies presenten. El Dret segueix al fet, de manera que la regulació neix del costum o de la necessitat de regular una situació no prevista. Així, s'observa que la regulació és escasa en referències a aquestes tecnologies disruptives; tot i així, molta de la normativa aplicable a l'internet i al tractament de dades és, *a priori,* aplicable per analogia a l'IoT.

S'ha de tenir en compte que la regulació de l'IoT compren diferents branques del dret: dret constitucional, dret administratiu, dret penal o dret mercantil en són alguns exemples.

En el present treball s'estudien, de forma succinta, diferents fonts a nivell internacional, comunitari i espanyol que s'han de tenir en compte. És objecte d'un anàlisi més profund el Dictamen 08/2014 del Grup de Treball de l'article 29 sobre l'evolució recent del Internet dels objectes, atès que presenta els problemes principals de l'IoT en matèria de protecció de dades i aporta propostes de solució basant-se en la normativa aleshores vigent, la Directiva 95/46/CE. Es pretén realitzar un anàlisi comparatiu entre la Directiva i el Reglament 2016/679 per tal d'esbrinar si les reformes que s'han dut a terme estan en línia amb el que estableix el Dictamen.

El següent quadre mostra un resum dels textos i organismes que s'analitzen, classificats segons el nivell territorial i el tema que tracten:

	Internacional	**Unió Europea**	**Espanya**
Dret a la protecció de dades		CDFUE (art. 8) TFUE (art. 16)	CE (art. 18.4)
Govern Obert	OGP		
Economia de les dades	OCDE	Com. Economia de les dades europea	
Mercat Únic Digital		Com. Agenda Digital Com. Estratègia UE 2020 Com. Mercat Únic Digital	
Protecció de dades		Reglament 2016/679 Directiva 95/46/CE	LOPD Reglament LOPD
Protecció de dades a les TIC		Directiva 2002/58/CE	LSSI
Internet de les Coses		Dictamen 08/2014	

3.1. Normativa internacional

Com s'ha dit, les úniques aproximacions normatives relatives a l'IoT provenen de la Unió Europa. A nivell internacional, no existeix regulació i és per aquest motiu que alguns autors es plantegen quins són els operadors jurídics més adequats per realitzar aquesta tasca.[18] Concretament, es poden plantejar tres opcions:

[18] Rolf H. WEBER.; Romana WEBER. *Internet of Things: legal perspectives*. Pàgs. 27 a 33.

- Xarxes de govern: es tracta d'associacions interestatals entre agències que pretenen resoldre els problemes globals i les llacunes jurídiques mitjançant la coordinació entre elles, l'aspecte positiu és que la creació d'una xarxa específica per l'IoT suposaria la implementació d'un marc jurídic més adequat. Això suposaria la creació d'un nou poder, organisme i legitimació. Les xarxes de govern facilitarien la cooperació entre Estats, ja que es tracta d'una forma d'organització més flexible que la creació d'una institució supranacional.
- Nou legislador internacional: la creació d'una autoritat internacional responsable per la governança de l'IoT suposaria un nivell d'especialització i de coordinació entre Estats més alt. Aquest nou òrgan hauria de tenir en compte les opinions d'òrgans ja existents, empreses, ONGs, usuaris i altres actors de la societat.
- Organisme existent: una altra opció possible és la creació d'un òrgan responsable de l'IoT dins d'algun altre organisme ja existent. Per exemple, es podria encarregar la tasca de crear el cos legislatiu de l'IoT a l'Organització Mundial de Comerç que ja compra amb Comitès específics per diverses qüestions i que constituiria un organisme amb experiència i amb recursos suficients per elaborar un conjunt de normes eficients en la matèria.

3.1.1. Open Government Partnership

Un exemple d'organisme de nova creació, que vindria a classificar-se com una xarxa de govern, és l'Aliança pel Govern Obert, també coneguda com OGP (*Open Government Partnership)*, formada per 75 països que s'hi han unit en el marc de l'ONU a través de la Declaració de Govern Obert que es va redactar el Setembre de 2011.[19] Aquesta organització busca crear una plataforma on els diferents Estats que s'hi han adherit puguin establir un diàleg per arribar a solucions comuns o compatibles.

Aquest és un exemple de l'efecte de l'IoT en el dret administratiu, l'Aliança té dos objectius fonamentals: d'una banda, la transparència o obertura de dades; i d'altra banda, la participació o obertura de processos. Dins d'aquests objectius en trobem d'altres més concrets:

- Augmentar la disponibilitat d'informació sobre les activitats governamentals.
- Donar suport a la participació ciutadana.
- Posar en pràctica els més alts estàndards d'integritat professional a través de les nostres administracions.
- Augmentar l'accés a les noves tecnologies per a l'obertura i la rendició de comptes.

La OGP treballa mitjançant plans d'acció per cadascun dels Estats membres; per exemple, a Espanya arrel d'aquesta iniciativa es va aprovar la Llei 19/2013, de 9 de

[19] Declaració del Govern Obert, de l'Aliança pel Govern Obert, de setembre de 2011. <https://www.opengovpartnership.org/open-government-declaration> [Consulta: 16/05/2017]

desembre, de transparència, accés a la informació pública i bon govern i la Llei 18/2015, de 9 de juliol, per la que es modifica la Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic.

3.1.2. OCDE

L'Organització per la Cooperació i el Desenvolupament Econòmics (OCDE), organisme internacional del qual Espanya en forma part, disposa d'una Direcció de Ciència, Tecnologia i Innovació que s'encarrega de buscar solucions per problemes comuns, compartir experiències i identificar les polítiques més adequades en diversos àmbits, entre els quals destaquen, per exemple, la biotecnologia o el *Big Data.*

El 2015, aquest organisme va publicar un informe anomenat *Data-Driven Innovation: Big Data for Growth and Well-Being* (Innovació basada en les dades: Big Data pel creixement i el benestar), en el qual es fa un anàlisi multidisciplinari amb nombroses recomanacions pels Estats membres de l'Organització.

L'informe posa l'accent en el potencial econòmic de les dades i basa el seu anàlisi en els següents blocs:

- La nova era dels descobriments científics basats en les dades.
- El rol de les dades a la millora dels resultats en salut.
- L'aprofitament de les dades per una millor governança.
- El *cloud computing,* l'analítica i altres eines clau.
- Les habilitats i altres implicacions en l'ocupació.
- Assegurar la confiança en l'economia basada en les dades.
- Mesura de les inversions en dades.

És evident que es tracta d'un anàlisi molt exhaustiu, pels efectes d'aquest treball, el més important és el capítol cinquè de la publicació[20] que tracta de la confiança en la innovació basada en les dades, és en aquest capítol en el qual es parla de la seguretat i la privacitat en quant a l'ús de les dades.

3.2. Normativa europea

A nivell comunitari s'impulsa de manera notable la regulació unitària de l'internet i les TIC, ja que es consideren el mitjà fonamental pel desenvolupament de l'economia i la societat. La Unió Europea ha recalcat en diverses ocasions la importància d'aquesta darrera revolució digital, però és sobretot l'any 2010, durant la crisi econòmica, quan es

[20] OECD. *Data-Driven Innovation. Big Data for growth and well-being*. Pàg. 207 a 236.

pren consciència de la necessitat de regular de manera més exhaustiva la qüestió per aprofitar tot el potencial econòmic i social de la xarxa i impulsar el creixement econòmic.

En la meva opinió, l'objectiu final de la regulació d'internet a la UE és aconseguir la realització del Mercat Únic Digital i, en concret respecte el *Big Data*, la creació de l'Economia de les Dades Europea.

La constitució del Mercat Únic Digital suposa una conseqüència natural del mercat únic o mercat interior, en el qual circulen lliurament persones, béns, serveis i capital. L'obstacle principal per realitzar aquest mercat únic és la fragmentació dels mercats digitals que impedeix la circulació de les dades entre els Estats Membres. Aquest és un problema que cal resoldre per realitzar el mercat digital i per consolidar el mercat únic europeu, doncs és evident que l'economia actual es basa en gran mesura en les tecnologies de la informació i de la comunicació.

3.2.1.Carta dels Drets Fonamentals i Tractat de Funcionament

Article 8 de la Carta dels Drets Fonamentals de la Unió Europea:

> *"Protección de datos de carácter personal*
>
> *1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*
>
> *2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*
>
> *3. El respeto de estas normas quedará sujeto al control de una autoridad independiente*."

Article 16 del Tractat de Funcionament de la Unió Europea:

> *"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*
>
> *2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.*
>
> *Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea."*

A aquests dos articles podem trobar la norma principal de la Unió Europea en matèria de protecció de dades. Tots dos textos tenen una redacció idèntica als seus respectius apartats primers, que enuncien el dret a la protecció de dades de caràcter personal.

El segon apartat dels articles, en canvi, discerneix en el seu contingut. Mentre que la Carta de Drets fonamentals estableix les normes bàsiques pel tractament de les dades, el TFUE es remet a les normes que s'establiran sobre el tractament d'aquestes dades i sobre la lliure circulació de les mateixes.

És important tenir en compte aquest article del TFUE, doncs estableix un dret i una llibertat que, en ocasions, poden trobar-se enfrontats: el dret a la protecció de les dades de caràcter personal i la lliure circulació d'aquestes dades.

Com es veurà més endavant, la Unió Europea opta per donar preferència a la lliure circulació de dades, per tal de poder construir una economia basada en aquestes.

3.2.2. Agenda Digital Europea

La Comissió Europea, amb motiu d'aquesta i d'altres qüestions, va aprovar el 2010 la Comunicació **"Una Agenda Digital per Europa"**[21] com a iniciativa dins la **"Estratègia Europa 2020"**[22] on es fixaven diferents objectius a un termini de deu anys amb prioritats basades en el creixement intel·ligent, el creixement sostenible i el creixement integrador.

La finalitat de l'Agenda Digital és obtenir beneficis econòmics i socials sostenibles que derivin del mercat únic digital, basant-se en un internet ràpid i en aplicacions interoperables. No s'hi fa referència directa a l'IoT, però és una comunicació que estableix les accions clau per aconseguir la digitalització dels mercats europeus, per exemple, s'estableix la necessitat de simplificar la cessió de drets d'autor, revisar el marc regulador de la protecció de dades, establir una política de seguretat de xarxes, etc.

3.2.3. Mercat Únic Digital

A la Comunicació de la Comissió **"Una estratègia pel Mercat únic digital d'Europa"**[23] de 2015 es torna a fer èmfasi a la necessitat de realitzar accions coordinades en els Estats de la Unió Europea per tal d'aconseguir el mercat únic en el qual les persones, físiques i jurídiques, puguin realitzar i accedir a les activitats en línia amb la seguretat de fer-ho en les condicions adients de competència i amb una protecció de dades adequades.

Destaca l'objectiu d'evitar el bloqueig geogràfic, pel qual, en ocasions, no es pot accedir a les webs d'altres Estats o, encara que s'hi pugui accedir, no s'hi pot comprar. Aquest objectiu és rellevant en quant al comerç i l'eficiència competitiva interestatals; a més, el bloqueig dificulta la implementació total de l'IoT i el *Big Data.*

També destaquen els objectius respecte les condicions per les xarxes digitals. En particular, la Comissió subratlla que és imprescindible una normativa de telecomunicacions adequada, ja que els mercats es troben totalment compartimentats i hi ha zones en les que es necessària una major inversió per posar fi als problemes en matèria d'espectre radioelèctric, que és la base de la xarxa d'internet.

---

[21] Comunicació de la Comissió Europea, de 19 d'abril de 2010, Una Agenda Digital per Europa.

[22] Comunicació de la Comissió Europea, de 3 de març de 2010, Europa 2020: Una estratègia per un creixement intel·ligent, sostenible i integrador.

[23] Comunicació de la Comissió Europea, de 6 de maig de 2015, Una Estratègia pel Mercat Únic Digital d'Europa.

D'altra banda, preocupa a la Comissió el problema estructural en els serveis digitals que suposa la ciberdelinqüència. En quant a l'IoT aquest aspecte és rellevant ja que, per l'interconnexió dels objectes que formen la xarxa pot ser fàcil piratejar-ne un d'ells i infectar la resta de dispositius, de manera que es poden interceptar dades, realitzar fraus, etc. També es fa referència, en quant a la ciberseguretat, a la protecció de dades i la privacitat, totes elles són qüestions que estan relaciones.

Finalment, la Comunicació dedica un apartat a l'aprofitament del potencial del creixement de l'economia digital. És en aquest apartat en el qual es refereix explícitament a l'IoT i al *Big Data.*

Amb aquesta comunicació es van assentar les bases per la creació d'una economia de les dades que es constituiria gràcies a les dades massives, els serveis en núvol i l'IoT. Les principals qüestions que es tracten són les següents:

- Les restriccions relacionades a la ubicació de dades: les normatives estatals han fomentat el manteniment de dades dins dels respectius territoris, la qual cosa comporta que els prestadors de serveis hagin de construir centres de dades en cadascun dels territoris en els que operin, això obstaculitza l'ús transfronterer de dades. El mateix ocorre amb les normatives de propietat intel·lectual.

- L'atribució de responsabilitat: és fonamental pel desenvolupament de l'IoT poder determinar la responsabilitat de cadascun dels participants (creador de l'aplicació, prestador de servei, etc.) per a operar en el mercat amb suficient seguretat jurídica.

- La seguretat respecte la protecció de dades i els drets fonamentals: la Comissió planteja la reforma en matèria de protecció de dades que es va dur a terme amb el Reglament General de Protecció de Dades de 2016, que busca garantir un tractament de dades uniforme a tots els territoris de la Unió Europea. A més, tant l'anterior normativa com l'actual pretenen evitar restriccions a la lliure circulació de dades personals, d'aquesta manera es dona preferència a la llibertat de circulació en detriment de la privacitat i la protecció de les dades. La Comunicació anticipa la iniciativa de la lliure circulació de dades que es fa efectiva amb la Comunicació sobre la construcció d'una economia de dades europea.

3.2.4. Economia de les dades europea

La Comunicació de la Comissió "**La Construcció d'una economia de les dades europea"**[24] es conseqüència de l'Estratègia pel Mercat Únic Digital i pretén constituir una iniciativa per eliminar les restriccions injustificades a la lliure circulació de les dades, es busca constituir un marc polític i jurídic que s'adapti a l'economia de les dades i que

[24] Comunicació de la Comissió Europea, de 10 de gener de 2017, La Construcció d'una economia de les dades europea.

elimini la inseguretat jurídica que poden crear les noves tecnologies de dades. Com a objectius complementaris, la Comunicació vol augmentar la disponibilitat i utilització de les dades, fomentar els models empresarials basats en les dades i millorar les condicions d'accés a les dades i el desenvolupament d'anàlisis de dades.

Així doncs, els temes portats a debat a la Comunicació són la lliure circulació de dades, l'accés i transferència en relació a les dades creades mitjançant IoT, la responsabilitat i seguretat de les tecnologies emergents i la portabilitat de les dades.

3.2.5. Directiva 95/46/CE i Reglament General de Protecció de Dades

La Directiva 95/46/CE relativa a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades és l'actual norma d'aplicació general a la Unió Europea en matèria de protecció de dades i de lliure circulació d'aquestes. Tot i que serà derogada pel Reglament que ja ha entrat en vigor, s'estableix un període de transició durant el qual es manté vigent.

El Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016 no començarà a aplicar-se fins el 25 de maig de 2018, de conformitat amb l'article 99 del mateix. D'igual manera s'estableix a l'article 94 del Reglament que la Directiva quedarà derogada amb efecte des del mateix dia.

Cal tenir en compte que el Reglament introdueix, dins les disposicions finals, un aclariment en el qual s'especifica que les referències a la Directiva que puguin estar contingudes en altres textos s'entendran fetes respecte el Reglament. Per exemple, el Dictamen 08/2014 del Grup de Treball de l'article 29 relatiu a l'Internet dels Objectes fa nombroses referències a la Directiva, que hauran de ser enteses fetes al Reglament.

Respecte el Grup de Treball de l'article 29 (o Grup de protecció de les persones en el que respecta al tractament de dades personals) es substitueix pel Comitè Europeu de Protecció de Dades que s'estableix al Reglament a l'article 68, per tant, tota referència feta al Grup de Treball s'entendrà feta al Comitè.

En resum, la normativa marc que s'aplica actualment és la Directiva 95/46/CE i les normatives nacionals de cada Estat membre que l'ha transposen. En el cas d'Espanya, la LOPD.

La diferència principal entre els textos de la Directiva i el Reglament radica a la seva naturalesa jurídica i la seva aplicabilitat. El Reglament és obligatori en tots els seus elements i s'aplica de forma directa a tota la Unió Europea, mentre que la Directiva va necessitar la corresponent transposició, la qual cosa va comportar que la legislació en aquesta matèria no fos unitària. Tanmateix, amb l'aplicació del Reglament es produirà el desplaçament de les corresponents normatives estatals, doncs, hi ha preeminència de la regulació comunitària i s'aconseguirà finalment una regulació unitària.

El preàmbul del Reglament també conté diferències substancials, doncs posa en context la rellevància que ha pres el tractament de dades personals, destacant a l'apartat sis la gran magnitud de recollida e intercanvi de dades personals que es dóna a l'actualitat i que es produeix degut a les tecnologies que permeten que empreses i autoritats

públiques utilitzin dades a una escala fins ara inimaginable. Així doncs, fa palesa la diferència en els objectius d'ambdós textos.

Cal destacar, per altra banda, la introducció de dos nous drets, molt relacionats amb internet. En primer lloc, l'anomenat dret a l'oblit, un dret que sorgeix de la sentencia del Tribunal de Justícia de la Unió Europea en el Cas C-131/12 i que es formalitza al introduir-se al Reglament. En segon lloc, el dret a la portabilitat de dades, que destaca per la seva utilitat en l'àmbit de l'IoT, ja que la portabilitat de dades implica que es puguin transferir les dades d'un sistema de tractament electrònic a un altre i també permet obtenir una copia de les dades personals en format electrònic.

3.2.6. Directiva 2002/58/CE

La Directiva 2002/58/CE relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les comunicacions electròniques completa la Directiva 95/46/CE, és a dir, la Directiva general de protecció de dades s'aplica en tot allò que no estigui regulat específicament a la Directiva sobre privacitat i comunicacions electròniques i així ho estableix el considerant desè d'aquesta.

El text ve a substituir l'anterior Directiva sobre la privacitat i les telecomunicacions[25], que tenia un àmbit d'aplicació molt més reduït, centrant-se específicament a la telefonia, mentre que l'actual actua en tots els àmbits de la comunicació electrònica. La Directiva es basa en un concepte ampli de les comunicacions electròniques, doncs, tal i com apunten diversos autors[26], no s'haurien d'incloure dins d'aquesta categoria els serveis de contingut en línia ja que s'exclouen expressament a la definició de servei de comunicacions electròniques que apareix a la Directiva 2002/21/CE. Tot i això, l'àmbit de protecció de la directiva inclou tant els serveis de transmissió com els de contingut (o serveis de la societat de la informació).

3.3. Normativa espanyola

3.3.1. Constitució Espanyola de 1978

El fonament constitucional del dret a la llibertat informàtica (i conseqüentment del dret a la protecció de dades a la informàtica) es troba situat a l'apartat 4 de l'article 18 de la Constitució Espanyola, del tenor literal de l'article sorgeixen alguns dubtes degut a la poca claredat del redactat.

[25] Directiva 97/66/CE del Parlament Europeu i del Consell de 15 de desembre de 1997 relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les telecomunicacions.

[26] En aquesta línea:

- Luis Ángel BALLESTEROS MOFFA. La privacidad electrónica. Internet en el centro de protección. Pàg. 236.
- Martien SCHAUB. European Legal Aspects of E-commerce. Pàg. 114.

Així, l'article enuncia que "La llei limitarà l'ús de la informàtica per tal de garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets". De fet, no es menciona l'existència d'un dret a la privacitat de dades, sinó que s'insta al legislador a acotar la utilització de la informàtica; per tant, tal com recull Ballesteros Moffa, es tracta d'una remissió al legislador que no estableix un dret *per se.*[27] La constitució del dret es deu al desenvolupament legislatiu i a la interpretació que en fa el Tribunal Constitucional en sentències com la STC 290/2000 i 292/2000.

S'ha d'entendre el dret a la protecció de dades personals com el dret a controlar l'ús que es pugui realitzar de les dades personals d'un mateix.

En quant al precepte i la configuració del dret a la protecció de dades es plantegen dues qüestions: en primer lloc, si es tracta d'un dret fonamental o si parlem d'un dret de configuració legal; i en segon lloc, si estem davant d'un dret fonamental, si ho és per si mateix o ho és per la seva inclusió a d'altres drets fonamentals com el dret a la intimitat. La doctrina i la jurisprudència han considerat que, efectivament, es tracta d'un dret fonamental amb un contingut essencial que necessita una interpretació legislativa.

3.3.2. LOPD i Reglament de desenvolupament de la LOPD

La Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal és la norma que s'encarrega del tractament, automatitzat o no, de dades. Es tracta d'una llei amb una vocació de protecció ampla, que suposa la transposició de la Directiva 95/46/CE.

La LOPD garanteix el poder de control sobre les seves dades personals mitjançant els anomenats drets ARCO que són els següents:

- Accés: es troba regulat a l'article 15 de la llei, aquest dret permet als ciutadans sol·licitar la informació sobre les seves pròpies dades personals.

- Rectificació: regulat a l'article 16, es confereix la possibilitat de modificar les dades quan les recollides són inexactes, incompletes, inadequades o excessives.

- Cancel·lació: es regula juntament amb el dret a rectificació, quan es donen les circumstàncies descrites anteriorment també es pot exercir el dret de cancel·lació, que permet la sol·licitud d'eliminació de les dades personals.

- Oposició: es troba a l'article 30.4 de la llei, és la facultat del titular de les dades per requerir que es deixin de tractar les seves dades personals quan s'estiguin tractant sense consentiment, quan es realitzi amb finalitats de publicitat o prospecció comercial i quan el tractament tingui per finalitat l'adopció d'una decisió basada únicament en un tractament automatitzat.

[27] BALLESTEROS MOFFA. Pàg. 80.

El Reial Decret 1720/2007, de 21 de desembre, pel que s'aprova el Reglament de desenvolupament aprofundeix en totes aquelles matèries de la protecció de dades que ho requereixin. Per exemple, en el Reial Decret es desenvolupen els drets ARCO d'una manera més concreta.

3.3.3. Llei de Serveis de la Societat de la Informació

La Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic és la llei espanyola que transposa la Directiva de Comerç Electrònic[28]. En ella es regulen els serveis de la societat de la informació en un sentit ampli, tal i com es recull al segon apartat de l'exposició de motius, que determina que aquests serveis incorporen tant la contractació de béns i serveis per via electrònica, com el subministrament d'informació per aquesta via, la transmissió de dades o qualsevol altre servei que es presti quan es tracti d'una activitat econòmica pel prestador. Aquesta llei és d'aplicació a l'IoT, doncs podem entendre l'Internet de les Coses com un servei de transmissió de dades.

3.4. Anàlisi del Dictamen 8/2014 del Grup de Treball de l'article 29

El Dictamen 8/2014 sobre l'evolució recent de l'Internet dels objectes, del Grup de Treball de l'article 29, de 16 de setembre de 2014 és un document de treball en el qual s'aborden els principals problemes relatius a l'IoT, s'estableixen els objectius que es pretenen aconseguir a nivell comunitari i, finalment, conclou amb una sèrie de recomanacions pràctiques per respectar la intimitat i la protecció de dades mentre s'aconsegueix una lliure circulació de les dades.

Els problemes que es plantegen en relació a l'IoT, amb caràcter general, són relatius a la pèrdua de dades, a la infecció per *spywares*, l'accés no autoritzat a les dades i la utilització de dispositius de vigilància il·legal.

En quant als objectius, el Dictamen busca aconseguir una aplicació uniforme del dret de protecció de dades europeu i desenvolupar un nivell de protecció per l'IoT adequat al marc jurídic de la Unió Europea.

3.4.1. El Grup de protecció de les persones i el Comitè Europeu de protecció de dades

El Grup de Treball (o Grup de protecció de les persones en el que respecta el tractament de dades personals) es crea en base a l'article 29 de la Directiva 95/46/CE, es tracta d'un Grup independent i de caràcter consultiu. Per tant, els seus dictàmens no vinculen

28 Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior

als òrgans de la Unió Europea ni als Estats membres; tanmateix, són rellevants per la Comissió Europea perquè estableixen orientacions útils sobre el nivell de protecció dels Estats membres.

El Grup està format per experts representants de cadascuna de les autoritats de control de cada Estat membre, de les autoritats de les institucions comunitàries i per un representant de la Comissió. Les tasques del Grup es descriuen a l'article 30 de la Directiva, tenen encomanat l'estudi de l'aplicació de les legislacions estatals per aplicar la Directiva, emetre els dictàmens respecte els nivells de protecció, assessorar sobre projectes de modificació de la Directiva i emetre dictàmens sobre els codis de conducta comunitaris.

Tal com s'ha comentat a l'apartat 3.2.5, amb el nou Reglament no existeix la figura del Grup de Treball. De fet, a l'apartat segon de l'article 94 s'estableix que qualsevol referència feta al Grup de Treball s'entendrà feta al Comitè Europeu de Protecció de Dades establert al Reglament.

El Comitè es crea mitjançant l'article 68 del present Reglament, la seva composició és molt similar a la del Grup de Treball, tot i que a la composició del Grup hi havia un representant de la Comissió, que podrà estar present a les reunions del Comitè però sense dret a vot. Així es reforça la independència del òrgan, que ja es recollia a la Directiva i que es reitera al Reglament. Com a novetat, s'introdueix a l'article 76 la confidencialitat dels debats del Comitè quan es consideri necessari, tot i que l'accés als documents presentats serà públic.

Les funcions del Comitè s'augmenten de manera significativa amb el reglament, s'estableixen a l'article 70 les funcions que durà a terme; amb caràcter general, el Comitè vetllarà per garantir la aplicació harmonitzada o coherent del Reglament.

3.4.2. Problemes de protecció de dades i solucions conforme la normativa

Falta de control i asimetria de la informació

En ocasions, la falta de transparència en la recollida de dades pot portar als usuaris a la pèrdua del control de la difusió d'aquestes. Aquest problema té una gran relació amb el *big data,* ja que al Dictamen es considera que el gran volum de dades que es generarà mitjançant la interrelació dels objectes no podrà ser controlada per les eines clàssiques de protecció.

És per això que el Reglament de Protecció de Dades introdueix a l'article 12 el requisit de la transparència de la informació, requisit que no apareixia a la Directiva. La transparència en l'obtenció de les dades implica la utilització d'un llenguatge senzill fàcil de comprendre per recavar el consentiment.

Alguns autors entenen que la transparència a la recollida de dades pot portar a una paradoxa[29], ja que, si bé la senzillesa i la claredat en la redacció de les polítiques de privacitat comporten que es faciliti la seva comprensió, també comporta una pèrdua de

[29] Elena GIL GONZÁLEZ. *Big Data, privacidad y protección de datos*. Págs. 71 a 72.

precisió a l'explicació, podria ser que, tot i ser enteses fàcilment, no es tingués informació suficient per donar un consentiment vàlid.

Els articles 13 i 14 imposen obligacions als responsables del tractament en relació a la informació que s'ha de facilitar, tant si les dades s'han obtingut de l'interessat o s'han obtingut per un altre via.

D'entre els deures d'informació que s'imposen s'ha d'informar de la identitat del responsable, les finalitats del tractament de dades, les categories de dades que es tracten i els seus destinataris, etc. A l'apartat d'aquest treball relatiu a les conclusions extretes de les dades i la readaptació del tractament original es tractaran els problemes que ocasiona el deure d'informar sobre la finalitat del tractament de les dades.

Qualitat del consentiment de l'usuari

L'existència del consentiment de l'usuari és fonamental, haurà d'estar degudament informat sobre les dades recollides i el tractament que es durà a terme.

La Directiva establia al seu article 7 els requisits per tal que el tractament de dades sigui lícit, al Reglament s'hi troben pràcticament els mateixos requisits amb alguna modificació substancial, com és el cas de la primera lletra: mentre la Directiva parla de consentiment inequívoc (un terme indeterminat, que pot portar a dubtes respecte l'existència o no del consentiment); el Reglament estableix que el consentiment del interessat haurà de ser donat per una o diverses finalitats específiques. Insisteixo en la importància i la problemàtica que suposa el fet d'haver d'informar de les finalitats del tractament de les dades i de donar el consentiment sobre aquestes, doncs el Big Data pot comportar que les dades combinades amb d'altres acabin sent d'utilitat per finalitats que no havien estat previstes.

Així doncs, un dels requisits per que el tractament sigui vàlid és que hi concorri el consentiment de l'interessat; però també pot ser lícit si es tracta d'una qüestió de necessitat com les que es plantegen a les lletres b a f, tant de l'art. 7 de la Directiva com de l'art. 6 del Reglament. En aquests casos, no serà necessari el consentiment, però es tracta de situacions taxades en les que es prioritza l'interès públic, les obligacions legals o els interessos vitals de l'interessat davant de la privacitat o la intimitat del subjecte.

En tot cas, el Reglament defineix el consentiment del interessat, a l'apartat 11 de l'article 4, com "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

Per tant, la normativa actual no prescindeix del caràcter inequívoc del consentiment, sinó que estableix a l'article 4 les característiques de forma que hauran de donar-se mentre que a l'article 6 s'hi estableix l'objecte del consentiment.

A més, el consentiment ha de ser explícit pel tractament de categories especials de dades, com aquelles que revelin el origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques, o la afiliació sindical i el tractament de dades genètiques, biomètriques, relatives a la salut o relatives a la vida sexual o les orientacions sexuals d'una persona. A la meva opinió, aquest article perd rellevància en el context del Reglament ja que a la definició del consentiment ja s'estableix que el

consentiment haurà de consistir en una declaració o acció afirmativa (per tant, serà un consentiment explícit). En tot cas, es tracta d'un recordatori i una advertència en relació a aquestes categories especials de dades.

Cal tenir en compte, a més, l'aplicació de l'art. 5.3 de la Directiva 2002/58/CE en relació al consentiment pel cas en que s'emmagatzemi informació o s'obtingui informació emmagatzemada en un equip terminal, com pot ser un telèfon mòbil. L'obligació de recavar el consentiment en aquest cas afecta tant als fabricants dels dispositius com a les parts que desitgin obtenir accés a les dades emmagatzemades en ells.

El Dictamen planteja a més, la qüestió de la divergència entre la propietat del dispositiu i l'emmagatzematge de les dades, ja que pot ser que concorrin diferents persones en l'ús del mateix dispositiu. Això planteja un problema que pot ser transcendent en ocasions, ja que cada persona hauria de donar el seu consentiment per emmagatzemar les dades. A la pràctica, però, no es dona un consentiment personal de cada usuari ja que és impossible controlar qui és l'usuari que està aportant les dades.

En matèria de l'IoT es plantegen diverses qüestions respecte el consentiment, doncs en moltes ocasions els dispositius com els *wearables* no podran ser identificats. En aquest sentit, el Grup de Treball es planteja la possibilitat de senyalitzar aquells dispositius que siguin susceptibles de captar informació.

El problema en aquest punt és que els dispositius capten informació, no només de la persona que els du, sinó també de tercers. Això a la pràctica porta a un consentiment inexistent o a un consentiment que al Dictamen es qualifica de baixa qualitat.

D'altra banda, és freqüent que els usuaris de terminals mòbils o d'altres aparells no puguin renunciar a alguns serveis o característiques d'aquest. Per tant, ens trobem novament amb un problema de baixa qualitat, ja que no serà un consentiment lliure i conforme al dret europeu.

El Grup de Treball considera que haurien d'introduir-se nous mecanismes als sensors que capten informació per tal de poder notificar-ne la captació i el tractament que es realitzarà. D'igual manera, s'haurien d'introduir mecanismes de consentiment en els propis dispositius per tal que el consentiment compleixi amb els requisits continguts a la normativa.

Conclusions extretes de les dades i readapatació del tractament original

El Grup de Treball de l'article 29 es preocupa per l'anàlisi de la combinació de dades de diferents dispositius que es pot du a terme per finalitats diferents a les que s'havien establert en primer lloc.

Existeixen riscos que es donen en relació a la fusió de dades de sensors que consisteix en "combinar datos de diferentes sensores o procedentes de diferentes fuentes para obtener información mejor y más precisa que la que se podría conseguir de esas fuentes por separado"[30]. La fusió de dades de sensors és molt habitual a l'IoT, d'aquesta manera, la informació primària pot ser combinada i, així, s'obtindrà un segon tipus

[30] Dictamen 08/2014, apartado 2.4 Revelación invasiva de pautas de comportamiento y perfiles, pág. 9.

d'informació que seran les dades extretes; per últim, hi ha un tercer tipus, les anomenades dades visualitzades, que són les que l'usuari obté.

El Dictamen determina que els operadors de l'IoT han d'assegurar la protecció de tots els nivells de dades i l'adequació de totes les finalitats per les que s'utilitzen per tal que siguin compatibles amb la finalitat original.

El problema que es planteja, com ja s'ha observat amb anterioritat a aquest treball, és doble: d'una banda, l'obligació del responsable d'informar de la finalitat del tractament de les dades; d'altra banda, el consentiment de l'usuari respecte aquestes finalitats.

Donat que el valor de les dades que s'obtindran pot ser desconegut, alguns autors[31] plantegen la possibilitat que l'obligació d'informar s'ampliï per tal d'abastar tota la informació que potencialment es podria obtenir després del tractament de les dades primàries. Aquest raonament s'infereix de la naturalesa del *Big Data*, doncs, les possibilitats d'aquest es veurien reduïdes. D'altres autors, son contraris a aquesta possibilitat i consideren que el consentiment ha de referir-se només a les dades primàries i el seu tractament, ja que del contrari es tractaria d'un consentiment invàlid i excessivament ample, que resultaria d'una informació parcial i no específica a l'interessat.

Revelació invasiva de pautes de comportament i perfils

La captació de dades pot comportar la revelació de determinats aspectes privats de la vida d'una persona; es poden detectar pautes de comportament, hàbits o estil de vida i preferències. D'aquesta manera es poden arribar a realitzar perfils molt detallats de les persones.

L'elaboració de perfils es defineix a l'apartat 4 de l'article 4 del RGPD com "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física".

És a dir, es tracta de crear perfils que permeten classificar els individus en categories que es determinen segons les dades obtingudes i de les quals se'n extreuen d'altres que no són apreciables *prima facie.*

Això es tradueix, amb l'aparició de l'IoT, en una vigilància que afecta a la privacitat de les persones de forma molt íntima i que, potencialment, podria comportar una vigilància inclús a l'àmbit de la llar. A més, la creació de perfils subsumeix els usuaris en categories a les quals se les assigna determinades característiques o comportaments que poden ser erronis i, especialment, es poden crear estereotips que no tinguin la precisió adequada.

La solució que aporta el Reglament es conté a l'article 22, aquest conté diverses modificacions respecte l'article 15 de la Directiva, que tenia una redacció força més

[31] GIL GONZÁLEZ. Pág. 73.

succinta i poc precisa. L'article 22 estableix que l'interessat té dret a no ser objecte d'una decisió basada en el tractament automatitzat (fent menció expressa a l'elaboració de perfils) que produeixi efectes jurídics o que li afecti de forma similar. No es prohibeix de forma absoluta la creació de perfils ja que s'estableixen certes excepcions: en primer lloc, que la decisió sigui necessària per la celebració o l'execució d'un contracte entre les parts; en segon lloc, que la decisió estigui autoritzada pel Dret de la Unió o dels Estats membres; y, en tercer lloc, que la decisió es basi en el consentiment explícit de l'interessat.

Tanmateix, al meu parer, aquest article només resol de forma parcial la problemàtica, ja que la creació de perfils es produeix a la majoria d'ocasions sense que l'interessat en sigui conscient. Hi ha, per tant, un problema de transparència a la recollida i tractament de les dades.

Limitació de la possibilitat de restar a l'anonimat quan es fa ús d'aquests serveis

S'ha de tenir en compte que la protecció de dades s'aplica només a les dades personals, és a dir, a aquella informació relativa a persones físiques identificades o identificables. El RGPD estableix que es considera identificable tota persona que es pugui identificar mitjançant, per exemple, un nom, un número d'identificació, dades de localitzador o elements propis de la identitat física, econòmica o social d'aquesta.

El procediment que es segueix per evitar la identificació dels interessats és la pseudonimització, que consisteix en el tractament de dades de forma que no es puguin identificar amb l'interessat sense utilitzar informació addicional. Però no s'ha d'entendre que aquestes dades pseudonimitzades són dades anònimes, sinó que es consideren dades relatives a persones identificables i, per tant, són dades subjectes a la protecció que atorga el dret i així ho especifica el Reglament en el considerant número 26.

L'ús dels sensors a l'àmbit de l'IoT pot portar a la creació d'identificadors i petjades digitals que, com ja s'ha vist, deriven, per exemple, en l'anàlisi de localització o de pautes de moviment. La conseqüència de tot plegat consisteix en facilitar enormement la possibilitat de reidentificar els usuaris, amb la qual cosa és difícil mantenir l'anonimat de les dades.

El Reglament esmenta, en el considerant 26, que la possible identificació depèn de la probabilitat raonable de que s'utilitzin mitjans per identificar a una persona física, tenint en compte factors com els costos i el temps necessari, així com la tecnologia disponible. Així, en el context actual es pot considerar que les dades són fàcilment reidentificables i així ho proven diferents casos.

Per exemple, Netflix va posar a disposició del públic una base de dades anonimitzada amb l'objectiu de realitzar un concurs el premi del qual s'obtenia si s'aconseguia escriure un algoritme per la recomanació de pel·lícules que millorés el que s'utilitzava en aquell moment; un grup de participants, durant les seves investigacions, va combinar les dades amb les de la pàgina IMDB, reidentificant els usuaris. El Dictamen 5/2014 del Grup de Treball de l'article 29, de 10 d'abril de 2014, sobre tècniques d'anonimització menciona aquest cas per la seva rellevància, ja que posa de manifest les carències d'aquestes tècniques.

Riscos per la seguretat: seguretat en front a eficiència

En últim terme, el Dictamen s'ocupa de la qüestió de la seguretat dels dispositius de l'IoT. Tot i que la tecnologia ha avançat notablement fins el punt de poder desenvolupar l'Internet de les coses, hi ha certes limitacions tècniques, per la qual cosa es dona preferència a l'eficiència (per exemple, a la duració de la bateria) en detriment de la seguretat.

D'aquesta manera, els dispositius poden ser pocs segurs i el fet que estiguin connectats té com a conseqüència que l'atac a un d'ells pugui infectar a tots els altres dispositius que s'hi relacionen. La seguretat de tota una xarxa depèn del dispositiu menys segur. Així es pot produir una vigilància, una violació de les dades personals o d'altres atacs amb diferents finalitats que fan que es percebi l'IoT com una tecnologia poc segura.

El Dictamen insta a les diferents parts involucrades a coordinar-se per poder establir una xarxa completament segura. Com es veurà al següent epígraf, hi ha diverses parts que intervenen d'una manera o d'una altra i que han de complir amb els seus deures i obligacions des de la fabricació del dispositiu fins el tractament de les dades. És precís, per tant, que s'implementin sistemes de seguretat ens tots els moments del procés.

Davant la multitud de parts involucrades, es pot plantejar la qüestió de qui és el responsable de cara a possibles errors de seguretat.

Tant la Directiva, a l'article segon, com el nou Reglament, a l'article quart, defineixen el responsable del tractament com una persona física o jurídica, una autoritat pública, un servei o un altre organisme que decideix sobre la finalitat i els mitjans empleats pel tractament. D'altra banda, també es defineix als articles esmentats la figura de l'encarregat del tractament, que és la persona que tracta les dades per compte d'una altra persona, és a dir, del responsable.

Cal tenir en compte el Dictamen 1/2010 del Grup de Treball de l'article 29 sobre els conceptes de "responsable del tractament" i "encarregat del tractament" que estableix unes directrius per aclarir aquests conceptes amb objecte de garantir el compliment a la pràctica en un context en el que el desenvolupament de les TIC i la globalització del tractament de dades porta a una complexitat creixent del tractament i de la determinació de la responsabilitat.

El Grup de Treball de l'article 29 conclou l'existència de dues característiques fonamentals per definir el responsable del tractament: d'una banda, es tracta d'un concepte autònom, és a dir, és un concepte que s'ha d'interpretar conforme la legislació comunitària; d'altra banda, és funcional, això vol dir que s'utilitza per assignar responsabilitats segons la capacitat d'influència, no es tracta d'un anàlisi formal, és un anàlisi de fet.

Segons aquest Dictamen, la capacitat de determinar les finalitats i els mitjans del tractament (per tant, la consideració de responsable) pot provenir de diferents fets:

- Competència legal explicita: si la pròpia legislació estableix el nomenament del responsable.

- Normes jurídiques generals o funcions tradicionals existents: si la llei implica una responsabilitat dins d'organitzacions. L'exemple més obvi és el de l'ocupador respecte les dades dels seus empleats.

- Circumstàncies de fet i altres elements: poden ser circumstàncies tals com l'exercici del control real, una relació contractual, etc.

Les obligacions del responsable i de l'encarregat es troben principalment als articles 24 a 31 del RGPD, tanmateix el considerant 146 ja determina que el responsable o encarregat del tractament haurà d'indemnitzar pels danys i perjudicis soferts a conseqüència d'una infracció a la normativa respecte el tractament.

Una novetat destacable del Reglament és l'establiment a l'article 25 d'un sistema de protecció de dades des del disseny i per defecte, això significa que el responsable està obligat a aplicar mesures tècniques i organitzatives apropiades per aplicar els principis de protecció de dades, sempre tenint en compte l'estat de la tècnica, el cost i les finalitats del tractament. Aquestes mesures s'han d'aplicar des que es determinen els mitjans del tractament com en el moment del propi tractament. L'article 32 del Reglament exemplifica les mesures tècniques i organitzatives que es poden prendre.

En quant, a la responsabilitat, s'atribueix de forma conjunta entre tots els responsables que hagin determinat els objectius i els mitjans del tractament.

3.4.3. Responsables del tractament

Com s'ha indicat a l'epígraf anterior, l'aplicació de les noves tecnologies (i en particular de l'IoT) implica que hi intervinguin un gran número de parts i complica l'assignació de responsabilitats respecte el tractament de les dades personals. És per això que el Dictamen 8/2014 diferencia les responsabilitats que es poden atribuir a cadascun dels interessats:

- Fabricants de dispositius: molts dels fabricants modifiquen el sistema operatiu de l'objecte o hi instal·len programes informàtics que determinen la seva funcionalitat i tot el relatiu a les dades. Per tant, els fabricants dels dispositius han de ser considerats com responsables del tractament.

- Plataformes socials: també són responsables quan s'hi comparteixen dades, ja que les plataformes tractaren les dades que l'usuari hagi introduït. Per exemple, si es comparteixen les dades obtingudes per un podòmetre, la plataforma social analitzarà les dades i deduirà que aquesta persona practica esport i li mostrarà anuncis de calçat o roba esportiva.

- Tercers creadors d'aplicacions: l'accés dels creadors de les aplicacions a les dades contingudes en els dispositius on s'instal·len (com telèfons mòbils o *wearables*) constitueix un tractament de les dades, per tant es considera al creador de l'aplicació com un responsable.

- Altres tercers: certs tercers poden utilitzar els dispositius d'IoT per recollir informació i tractar-la, un exemple podria ser el d'una asseguradora que regala

podòmetres als clients per controlar quant exercici realitzen i, així, reduir les primes de l'assegurança. En aquest context, l'asseguradora seria considerada responsable del tractament de les dades.

- Plataformes de dades de IO: existeixen plataformes que tenen com a objectiu allotjar les dades recollides per diferents dispositius, de forma que es centralitzi la seva gestió, aquestes plataformes són considerades responsables.

3.4.4. Drets de l'interessat

El Grup de Treball de l'article 29 considera als abonats i als usuaris de l'IoT com interessats. A diferència del que ocorre respecte els responsables, no es conté a la normativa una definició de la part interessada. Tanmateix, es pot considerar que són interessats totes aquelles persones sobre les quals es recullen dades. Com s'aclareix a la directiva, el concepte d'interessat i l'aplicació de la normativa de protecció de dades no es supedita a la propietat del dispositiu, sinó al tractament de les dades personals ja que es donen nombroses casuístiques en les que el propietari del dispositiu i l'interessat no coincideixen: tant si es tracta d'un bé arrendat, com si es recullen dades de terceres persones alienes.

El Dictamen analitza els drets de l'interessat des de la perspectiva de la Directiva, però ja tenint en compte algunes modificacions que introdueix el Reglament i que encara no s'havien aprovat en el moment de redacció.

D'una banda es parla del **dret d'accés**, que es reconeix a l'article 15 del RGPD (i a l'article 12 de la Directiva). Aquest dret possibilita als interessats a obtenir dels responsables, la comunicació de les dades que són objecte del tractament, així com de tota la informació de l'origen de les dades i de les finalitats per les que s'utilitzaran, els destinataris de la informació, etcètera.

El Grup de Treball de l'article 29 considera que a l'actualitat no és produeix un exercici efectiu del dret d'accés ja que els responsables del tractament no posen a disposició les dades primàries recollides, sinó que en nombroses ocasions es proporcionen dades incompletes.

El Dictamen ja avançava la consagració d'un **dret a la portabilitat** que finalment s'ha incorporat al Reglament a l'article 20 i que comporta que l'interessat pugui transferir les seves dades a un altre responsable del tractament i optar per altres serveis. Aquest dret es pot considerar una modalitat del dret d'accés a les dades que elimina algunes barreres de competència entre els agents del mercat.

Un altre dels drets en relació a la protecció de dades és el **dret de rectificació,** establert a l'article 16 del Reglament de manera expressa, tot i que no es contenia a la Directiva. La possibilitat de l'usuari de rectificar les dades incorrectes no planteja, a la pràctica, grans problemes.

La segona novetat en matèria de drets de l'interessat al Reglament és la incorporació d'un **dret de supressió,** més conegut com a dret a l'oblit. Aquest dret prové de la

jurisprudència del TJUE i es va reconèixer per primera vegada en la sentència del Cas Google Spain S.L. contra Agència Espanyola de Protecció de Dades.[32]

El dret a l'oblit es pot exercir per demanar la supressió de les dades quan es donin alguns dels requisits de l'article 17 del Reglament: que ja no siguin necessaris per la finalitat, que es retiri el consentiment en que es basa el tractament, que l'interessat exerceixi el dret d'oposició, que les dades s'hagin obtingut il·lícitament, que les dades s'hagin de suprimir per donar compliment a una obligació legal o que les dades s'hagin obtingut en relació amb ofertes de serveis de la societat de la informació per menors de 16 anys.

S'estableix al Reglament un **dret a la limitació** del tractament a l'article 18, que preveu una solució a mig camí de la supressió i la oposició. Pot ser útil una limitació al tractament de les dades quan l'interessar vol exercir una reclamació i necessita les dades però el responsable ja no les necessita; d'aquesta manera, les dades es conserven però s'hi estableix una limitació.

Per últim, els interessats disposen d'un **dret d'oposició** que es recull a l'article 21 del Reglament (i a l'article 14 de la Directiva) i que suposa la possibilitat de que l'interessat retiri el consentiment del tractament de les dades i s'oposi a que es segueixin tractant les seves dades.

En aquest cas, el Dictamen considera que els responsables haurien d'articular aquest dret de manera que l'interessat pugui oposar-se a:

- El tractament de dades recollides per un objecte determinat. Per exemple, la petició de que un rellotge intel·ligent deixi de recollir dades; i, per tant, passi a funcionar com un rellotge convencional.

- El tractament d'un tipus de dades recollides per qualsevol objecte. Per exemple, que no es recullin dades mitjançant qualsevol dispositiu que registri la ubicació, sigui un cotxe, un ordinador o un rellotge.

- Un tractament de dades determinat. Per exemple, que el rellotge no reculli dades relatives a la ubicació, però segueixi recollint totes les demés dades.

[32] STJCE 2014/85, de 13 de maig de 2014, cas Google Spain S.L. contra Agència Espanyola de Protecció de Dades (AEPD)

4. BIG DATA

4.1. Aplicació del Big Data a la pràctica

Per poder entendre adequadament el *Big Data* i les seves implicacions legals s'ha de tenir en compte que aquesta tecnologia s'aplica en dues fases que suposen reptes i efectes diferents en quant a la protecció de dades. En conseqüència, seran necessàries solucions o propostes diferents per cadascuna d'aquestes fases.

4.1.1. Primera fase

La primera fase del *Big Data* consisteix en la recol·lecció de les dades i el seu tractament o processament automatitzat per descobrir l'existència de correlacions. Es tracta d'extreure conclusions sobre com afecta una circumstància concreta al comportament de l'individu. Per tant, s'ha de poder associar les dades com a pertanyents a aquesta persona en concret i, així, es podran identificar les variables coincidents o diferents entre grups de persones.

Gràcies a aquesta primera fase, per exemple, es poden fer estudis mèdics en que es conclogui que una malaltia es dóna amb més freqüència en persones amb unes determinades característiques, com estil de vida, sexe o genètica.

El fet que les dades de cada persona s'hagin d'associar com relatives a la mateixa no implica, però, que les dades hagin d'identificar a la persona. És important per aquesta la fase les tècniques de pseudonimització de les que s'ha parlat a l'epígraf 3.4.2 d'aquest treball.

És interessant la discussió doctrinal respecte l'existència d'un *ius usus inocui* digital. Els qui defensen aquesta postura consideren que hi ha un dret d'aprofitament de la cosa aliena, utilitzant-la per raó de la seva utilitat, sense que el propietari pateixi cap perjudici. En aquest àmbit de la tecnologia, la cosa aliena serien les dades i es podria aplicar aquest principi sempre que les actuacions fossin innòcues per l'individu, com en investigacions o estudis.[33]

Tanmateix, si es pren com a vàlida l'aplicació del principi del *ius usus inocui,* no seria necessari un consentiment de l'individu ja que s'entendria que, tàcitament, accepta la utilització de les seves dades. Així, prendria més rellevància el dret d'oposició al tractament de les dades en detriment del consentiment que passaria a quedar en un segon pla.

[33] GIL GONZÁLEZ. Pàg. 57.

4.1.2. Segona fase

A la segona fase de l'aplicació del *Big Data* es té en compte el model que s'ha obtingut mitjançant la comparació i s'aplica a una persona determinada. Així, es tractaran les dades d'aquesta persona i s'extrauran conclusions en base a models obtinguts a la primera fase. Seguint l'exemple de l'apartat anterior, segons les dades obtingudes d'una persona (edat, pes, sexe, etc.) es podrà inferir si és propens a patir una malaltia.

A diferència del que ocorria a la primera fase, en aquesta segona fase és necessari un consentiment informat de la persona, ja que es prenen decisions que hi afecten directament, fet que comporta un risc ètic molt major. Per exemple, quan s'infereixen els resultats d'un grup, poden no correspondre amb un l'individu que s'analitza encara que presenti les mateixes característiques, hi ha el risc de generalitzar uns resultats per tots els individus que compleixin uns determinats requisits o característiques.

4.2. Solucions proposades per la normativa del Big Data

La irrupció del *Big Data* ha suposat un repte per la legislació en diversos àmbits com poden ser, la protecció de dades, la responsabilitat, el dret de la competència o els drets de propietat industrial.

Per l'anàlisi realitzat en aquest treball interessa sobretot estudiar els efectes del *Big Data* a la protecció de dades. La qüestió que es planteja és si la normativa relativa al tractament de les dades és l'adequada en un moment en el que les tecnologies disruptives com l'IoT, el *cloud computing,* l'automatització i el *Big Data,* fomenta que les dades es recullin, es processin i es reutilitzin en pocs segons.

Com s'ha vist a l'estudiar el nou Reglament i la Directiva, hi ha dues grans limitacions a la normativa actual de protecció de dades: en primer lloc, les tècniques d'anonimització han esdevingut cada vegada menys segures ja que existeix un risc de reidentificació elevat; en segon lloc, el consentiment s'ha convertit en una eina poc útil perquè sovint no es pot informar de les finalitats per les que s'utilitzarà la informació.

Tant autors com diferents organismes han proposat solucions per crear una nova normativa de protecció de dades o per reformar-ne l'existent, en aquest punt del treball s'analitzaran diferents opcions a tenir en compte.

4.2.1. Desplaçament del requisit del consentiment

En l'aplicació del *Big Data,* sovint, la informació adquireix valor en base als usos secundaris pels quals es pot fer servir, és a dir, que el què és rellevant no són les dades primàries que s'obtenen en la recollida, sinó les dades secundàries obtingudes mitjançant el tractament donat que revelen informació desconeguda.

A la pràctica, doncs, es pot concloure que la informació que s'extreu del tractament és impredictible i, per tant, no es sabrà amb certesa la finalitat per la qual s'utilitzaran les

dades recollides. Els responsables del tractament es troben amb un primer obstacle a l'hora d'informar als interessats, que no poden conferir un consentiment plenament vàlid si no disposen d'aquesta informació. Per tal de complir amb la normativa, els responsables haurien de tornar a demanar el consentiment cada vegada que les dades s'utilitzessin per una finalitat que no fos la prevista inicialment.

Un altre problema és el de la pèrdua de control de les dades per part de l'individu interessat, que ja s'ha definit a l'apartat. 3.4.2.a d'aquest treball, la transferència de dades entre diferents responsables es produeix a una gran velocitat, la qual cosa provoca una falta de transferència de l'usuari.

En síntesi, la falta d'informació i la pèrdua de control de les dades per part dels usuaris provoca que el consentiment hagi deixat de ser una eina útil per controlar el tractament. Tanmateix la reforma europea segueix atorgant un paper fonamental al consentiment, el qual ha de referir-se a fins específics.

4.2.2. Introducció de la privacitat per defecte i privacitat des del disseny

Una manera útil de garantir la seguretat de les dades és la introducció de sistemes de privacitat per defecte i des del disseny a la construcció i configuració de les tecnologies, això permet que s'apliquin els principis de privacitat al funcionament dels dispositius.

Els sistemes de privacitat per defecte garanteixen que la configuració del dispositiu establerta de fàbrica sigui la més protectora possible i només si l'usuari vol permetre d'altres utilitats la configuració de privacitat serà inferior; mentre que els sistemes de privacitat des del disseny són aquells en que les tecnologies o els dispositius es construeixen tenint en compte la necessitat de la protecció de la privacitat.

Per consegüent, la millor solució, com exposa Elena Gil[34], és <<incluir la configuración más segura por defecto en un sistema diseñado bajo los principios de privacidad desde el diseño>>.

És per aquest motiu que el Reglament General de Protecció de Dades de la UE estableix al considerant 78 que la protecció del tractament de dades personals imposa l'adopció de mesures tècniques i organitzatives per garantir el compliment de la llei. Més encara, també insta als productors de serveis, productes i aplicacions a que tinguin en compte el dret a la protecció de dades quan es desenvolupin i es dissenyin aquests productes.

A l'article 25 es configura el principi de protecció de dades des del disseny i per defecte. Tanmateix, l'apartat primer es refereix a la protecció des del disseny amb un redactat poc clar en que es determinen les mesures que es podran prendre des del moment de determinar els mitjans de tractament i estableix , des del meu punt de vista, una sèrie de límits al principi, com són l'estat de la tècnica, el cost d'aplicació, les finalitats del tractament, el risc de la probabilitat i de la gravetat del tractament de les dades. En altres paraules, s'entén que el responsable del tractament usarà els sistemes de protecció modulant-ne l'aplicació segons les circumstàncies que es donin. A més, aquest primer

[34] Ibídem, pàg. 136.

apartat exemplifica les mesures de protecció del disseny i per defecte fent referència a la pseudonimització de les dades; exemple que no sembla del tot encertat tenint en compte la limitació que suposa la reidentificació en aquesta tècnica.

L'apartat segon es refereix a la protecció per defecte, imposa una obligació al responsable del tractament d'aplicar mesures tècniques i organitzatives per que només siguin objecte de tractament les dades personals que siguin necessàries per cadascuna de les finalitats del tractament. S'esmenta, en particular, que les dades personals no seran accessibles sense la intervenció de la persona (per tant, al consentiment) a un número indeterminat de persones físiques.

4.2.3. La propietat de les dades

En quant a la propietat de les dades hi ha dues posicions contraposades: d'una banda, molts dels individus interessats consideren que les dades els pertanyen en la mesura que la informació es refereix a ells mateixos; d'altra banda, les empreses consideren que les dades són de la seva propietat pel fet que inverteixen grans quantitats de recursos a la seva recollida i tractament.

El Fòrum Econòmic Mundial[35], en vista de les posicions radicalment diferents de les parts interessades, proposa que totes les parts comparteixin drets i responsabilitats sobre la informació doncs ambdues parts interactuen en la creació de les dades. Ara bé, es precisa que cadascun dels individus requerirà permisos diferents per poder exercir aquests drets. Es configuren els drets de manera que no són exclusius, sinó que es consideren comuns o compartits entre les parts interessades; això és així perquè els drets sorgeixen en un context social.

La propietat no atorga drets necessàriament exclusius, i encara menys al context digital en el que operen l'IoT i el *Big Data,* on les dades són béns immaterials.

4.2.4. L'apoderament dels individus

Una altra solució pels reptes que suposa el *Big Data* és l'apoderament dels individus. Autors com Ira S. Rubinstein[36] proposen un model de negoci en el que l'administració de les dades correspongui als individus. En altres paraules, es tracta de passar d'un model en el que les organitzacions recullen i utilitzen la informació pels seus fins propis, a un on els individus administren la seva informació i la destinen pels seus fins o per fins conjunts, compartint informació amb proveïdors de serveis, per exemple. Això permet que els consumidors deixin de ser els subjectes passius als quals se'ls ofereixen productes per convertir-se en subjectes actius del mercat que poden demanar als venedors què volen, com, on i quan ho volen.

---

[35] FÒRUM ECONÒMIC MUNDIAL; THE BOSTON CONSULTING GROUP. *Rethinking personal data: Strengthening trust.* Pàg. 10.
[36] Ira S. RUBINSTEIN. Big data: The End of Privacy or a New Beginning? Pàgs. 9 a 11.

L'utilització d'aquest model d'apoderament es basa en els anomenats "serveis de dades personals" (o PDS, *personal data services*) que desplaça a les empreses en el rastreig i monitorització de les dades en benefici de l'usuari que pot fer ús d'aquest servei per escollir quines dades estan disposats a publicar i sota quines condicions.

Es considera que, per que el sistema funcioni, hi ha vuit característiques fonamentals en els serveis de dades personals:

1. Els individus són el centre de recol·lecció, gestió i ús de les dades personals.

2. Divulgació selectiva de la informació, sense revelar més informació personal de la que l'individu desitja.

3. Control de les finalitats primàries i secundaries de les dades i de la seva duració, per mitjans tècnics o contractes.

4. Mitjans dels individus per expressar les seves demandes de béns o serveis de forma oberta, evitant els lligams a cap organització en concret.

5. Gestió d'identitat que permet l'autentificació de la identitat de l'usuari que accedeix al sistema.

6. Seguretat al més alt nivell.

7. Portabilitat de les dades, és a dir, l'habilitat de traslladar totes les dades personals de l'individu d'un proveïdor a un altra utilitzant formats de dades estàndard.

8. Mesures per que les empreses proveïdores d'aquests serveis es facin responsables de la seguretat de les dades i protegir-les d'acord amb els permisos que l'individu hagi atorgat.

La professora Rubinstein analitza com encaixen aquests elements amb els principis de protecció de dades de la Unió Europea. En primer lloc, s'assegura que el sistema basat en l'apoderament de l'individu permet un nivell de transparència molt més elevat del que es pot aconseguir amb un sistema basat en l'administració de les dades per part de les empreses. A continuació, es fa èmfasi en les característiques enumerades de l'1 al 3, es considera que aquestes tracten de les finalitats del tractament de les dades i a les limitacions a la recollida, així com al control de les dades. L'element 1 es refereix a la qualitat de les dades, que seran més acotades i verdaderes si és el propi usuari qui les gestiona. L'element 6 tracta de la seguretat de les dades que s'ha comentat en altres epígrafs i que, pren rellevància en quant a la protecció per defecte i des del disseny. L'element 8 es refereix a la responsabilitat dels responsables del tractament de les dades.

És rellevant també la característica o element número 7 que tracta de la portabilitat de les dades, el nou dret introduït al Reglament. Això fa patent que el sistema està alineat amb els principis de protecció de dades de la Unió Europea, mentre que ofereix una solució innovadora en matèria de *Big Data* i no prevista a la normativa.

Evidentment, aquests sistemes de gestió de dades beneficien a l'individu, atès que li concedeix un major control i permet que s'emmagatzemin dades que provenen de diferents fonts. Aleshores facilita la portabilitat de les dades en tant que un mateix pot recopilar totes les seves dades i concedir permisos a altres organitzacions per poder accedir a aquestes dades.

En canvi, la utilitat o el benefici per les empreses és menys evident. Tot i així, les organitzacions tenen diversos incentius: en el pla econòmic, hi ha una important reducció dels costos dedicats a l'emmagatzematge de dades; en un sentit competitiu, permet la creació d'oportunitats de negoci a nous operadors que no es beneficiaven del *Big Data;* per últim, en un sentit d'utilitat, s'entén que les qualitat de les dades és major i, pe tant, els resultats obtinguts mitjançant l'aproximació predictiva serà més acurada.

CONCLUSIONS

I. L'IoT és una tecnologia que ja es troba en funcionament i que recull dades de forma constant, la qual cosa ha provocat que la legislació al voltant de la protecció de dades adquireixi una gran transcendència. La implementació de l'IoT i d'altres tecnologies ha permès el desenvolupament del *Big Data*, que té com a objectiu final l'anàlisi predictiu, és a dir, el descobriment de noves tendències i hàbits que es desconeixien i que permeten millorar la presa de decisions.

II. El Big Data ha provocat que les dades siguin considerades un actiu de gran importància a l'economia, això vol dir que les empreses precisen d'aquestes dades ja que els suposa un avantatge competitiu. Tanmateix, en ocasions, els usuaris no són conscients de les dades que estan aportant ni de les finalitats per les quals s'utilitzen.

III. En conseqüència, sorgeix un conflicte entre la protecció de les dades personals i la lliure circulació de les dades. La protecció de les dades és un dret fonamental consagrat a les normes de més alt nivell de l'ordenament jurídic, com són la Carta de Drets Fonamentals de la Unió Europea, el Tractat de Funcionament de la Unió Europea i la Constitució Espanyola; mentre que la lliure circulació és un dels objectius primordials de la Unió Europea i es recull al Tractat de Funcionament.

IV. Cal afegir que la normativa europea de dades s'emmarca o persegueix dos objectius: aconseguir un Mercat Únic Digital i crear una Economia de les dades europea. Aquests objectius es desprenen de les corresponents Comunicacions de la Comissió, ambdues molt recents, especialment la Comunicació, de 10 de gener de 2017, sobre la Construcció d'una economia de les dades europea. S'entén que la posició de la Unió Europea és la de donar prevalença a la lliure circulació de les dades per tal de poder aconseguir aquests dos objectius.

V. En quant al dret a la protecció de les dades personals, la Unió Europea va aprovar el darrer any el Reglament General de Protecció de Dades, el qual forma part de la reforma per modernitzar la legislació en aquesta matèria. Com a novetat destacable, s'ha introduït el dret a la portabilitat de les dades, el qual es considerava en diversos textos com un dret necessari a l'era del *Big Data*. La seva introducció es proposava al Dictamen del Grup de Treball de l'article 29 sobre l'evolució recent de l'Internet dels objectes, a diverses comunicacions de la Comissió i a la doctrina en publicacions de diferents autors.

VI. Tanmateix, el Dret europeu continua considerant el consentiment com la peça fonamental del sistema legislatiu: el consentiment ha de ser explícit, vinculat a fins específics, lliure, informat i inequívoc, i ha de prestar-se mitjançant un acte afirmatiu. Com s'ha vist al llarg de tot el treball, amb el *Big Data* és possible que els fins pels quals s'utilitzaran les dades no estiguin completament determinades i el fet de posar el consentiment en el primer pla del règim de protecció de dades pot posar traves, alentir o entorpir el desenvolupament de l'Economia de les dades i el *Big Data.*

VII. Una altra novetat del Reglament és la introducció de la privacitat o protecció de dades des del disseny i per defecte, que implica que s'apliquin mesures tècniques des del moment de creació del producte i que la configuració inicial del dispositiu sigui la més protectora, aquesta mesura és útil per garantir la protecció de les dades.

VIII. Així doncs, des del meu punt de vista, la normativa europea mostra, en ocasions, certa falta de consistència entre els objectius que es pretenen aconseguir i els mitjans que s'utilitzen per aconseguir-los. Si bé el Reglament ha introduït mesures importants, com la privacitat des del disseny i per defecte, seria necessària una reforma més profunda: el consentiment no pot ser el mitjà principal de protecció de dades si l'objectiu és aconseguir una economia basada en les dades.

IX. La Unió Europea hauria de plantejar-se la introducció de les solucions que es mostren als apartats 4.2.3. i 4.2.4. del treball per aconseguir un equilibri entre la protecció de les dades i la lliure circulació de les mateixes. És especialment interessant la proposta de l'apoderament dels individus ja que els permet que comparteixin la informació que desitgin i els converteix en subjectes actius que poden comunicar els seus gustos i preferències.

X. En síntesi, les solucions adoptades pel Reglament semblen vàlides a curt termini; tanmateix, per la consecució dels objectius plantejats a llarg termini és adequada la introducció d'un règim basat en la propietat compartida de les dades i en l'apoderament dels individus. Aquestes dues solucions estan en línia amb les tendències d'obertura que estan desenvolupant els governs arreu del món, els quals es basen en la transparència i les dades obertes, i a l'hora apoderen a l'individu que té un poder de participació molt més gran. Per tant, la tendència és que amb l'obertura de dades i els processos de *Big Data* els individus adquireixin poder, tant en els àmbits públics com en els àmbits privats, i és per aquesta raó que la normativa ha d'anar encaminada a un apoderament que permetrà als individus controlar les seves dades i decidir per ells mateixos.

BIBLIOGRAFIA

Referències bibliogràfiques

BALLESTEROS MOFFA, Luis Ángel. *La privacidad electrónica: Internet en el centro de protección*. Valencia: Tirant lo Blanch, 2006. 348 p. (Tirant monografías; 413). ISBN: 978-84-845-6490-4.

GIL GONZÁLEZ, Elena. *Big Data, privacidad y protección de datos.* Madrid: Imprenta nacional de la Agencia Estatal Boletín Oficial del Estado, 2016, 149 p. ISBN: 978-84-340-2309-3.

OECD. *Data-Driven Innovation: Big Data for Growth and Well-Being*. Paris: OECD Publishing, 2015, 452 p. ISBN 978-92-64-22935-8.

SCHAUB, Martien. *European Legal Aspects of E-commerce*. Groningen: Europa Law, 2004, 216 p. ISBN: 907687137X

WEBER, Rolf H.; WEBER, Romana. *Internet of Things: legal perspectives.* Zurich: Springer, 2010, 126 p. ISBN 978-3-642-11709-1.

Articles

ASHTON, Kevin. That "Internet of Things" Thing. RFID Journal, 2009 <http://www.rfidjournal.com/articles/view?4986> [Consulta: 08/04/2017]

BARRANCO FRAGOSO, Ricardo. *¿Qué es Big Data?* IBM developer Works, 2012. <https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/> [Consulta: 10/04/2017]

BBVA. Innovation Edge. *Big Data: Es hora de generar valor de negocio con los datos.* <http://www.centrodeinnovacionbbva.com/innovation-edge/big-data/big-data-vision-general > [Consulta: 17/04/2017]

FÒRUM ECONÒMIC MUNDIAL; THE BOSTON CONSULTING GROUP. *Rethinking personal data: Strengthening trust.* Proyecto Rethinking Personal Data, 2012.

GESCHICTER, Chet; R. MOYER, Kristin. *Measuring the Strategic Value of the Internet of Things for Industries* <https://www.gartner.com/doc/3299317?refval=&pcp=mpe> [Consulta: 08/04/2017]

LÓPEZ LÓPEZ, Jose Carlos. El Economista. *La moda del Big Data: ¿En qué consiste en realidad?* < http://www.eleconomista.es/tecnologia/noticias/5578707/02/14/La-moda-del-Big-Data-En-que-consiste-en-realidad.html > [Consulta: 10/04/2017]

MCCARTHY, John. *What is artificial intelligence?* Stanford University, 2007. <http://www-formal.stanford.edu/jmc/whatisai/> [Consulta: 11/04/2017]

ROSE, Karen; ELDRIDGE, Scott; CHAPIN, Lyman. *La Internet de las Cosas-Una breve reseña.* Internet Society, 2015.

RUBINSTEIN, Ira S. *Big data: The End of Privacy or a New Beginning?* International Data Privacy, volum 2, edició 3, 2013.

Referències legislatives

Espanya. Constitució Espanyola, de 27 de desembre de 1978. (BOE [en línia], núm. 311, 29-12-1978, pàgs. 29313 a 29424).< https://www.boe.es/buscar/doc.php?id=BOE-A-1978-31229 >. [Consulta: 01/05/17].

Espanya. Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal. (BOE [en línia], núm. 298, 14-12-1999, pàgs. 43088 a 43099). <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750 >. [Consulta: 15/04/17].

Espanya. Llei 18/2015, de 9 de juliol, per la que es modifica la Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic. (BOE [en línia], núm. 164, 10-07-2015, pàgs. 57436 a 57450). < https://www.boe.es/buscar/doc.php?id=BOE-A-2015-7731 >. [Consulta: 05/05/17].

Espanya. Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern. (BOE [en línia], núm. 295, 10-12-2013, pàgs. 97922 a 97952). <https://www.boe.es/buscar/doc.php?id=BOE-A-2013-12887 >. [Consulta: 05/05/17].

Espanya. Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic. (BOE [en línia], núm. 166, 12-7-2002, pàg. 25388 a 25403). <https://www.boe.es/buscar/doc.php?id=BOE-A-2002-13758 >. [Consulta: 15/04/17].

Espanya. Reial Decret 1720/2007, de 21 de desembre, pel que s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal. (BOE [en línia], núm. 17, 19-01-2008, pàgs. 4103 a 4136). < https://www.boe.es/buscar/doc.php?id=BOE-A-2008-979 >. [Consulta: 01/05/17].

Unió Europea. Tractat de Funcionament de la Unió Europea, Roma, 25 de març de 1957. (DOUE [en línia], núm. 83, 30-05-2010, pàgs. 47 a 199. <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70006 >. [Consulta: 01/05/17]

Unió Europea. Carta dels Drets Fonamentals de la Unió Europea, Niça, 7 de desembre de 2000. (DOUE [en línia], núm. 83, 30-05-2010, pàgs. 389 a 403. <http://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003 >. [Consulta: 01/05/17]

Unió Europea. Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE. (DOUE L [en línia], núm. 119, 04-05-2016, pàgs. 1 a 88). <https://www.boe.es/diario_boe/txt.php?id=DOUE-L-2016-80807>. [Consulta: 03/05/17]

Unió Europea. Directiva 2002/58/CE del Parlament Europeu i del Consell, de 12 de juliol de 2002, relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les comunicacions electròniques. (DOUE L [en línia], núm. 201, 31-07-2002, pàgs. 37 a 47). <https://www.boe.es/buscar/doc.php?id=DOUE-L-2002-81371>. [Consulta: 04/05/2017]

Unió Europea. Directiva 2000/31/CE, del Parlament Europeu i del Consell, de 8 de juny del 2000, relativa a determinats aspectes jurídics dels serveis de la societat de la informació, en particular el comerç electrònic en el mercat interior. (DOUE L [en línia], núm. 178, 17-07-2000, pàgs. 1 a 16). <https://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295>. [Consulta: 05/05/2017]

Unió Europea. Directiva 97/66/CE del Parlament Europeu i del Consell de 15 de desembre de 1997 relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les telecomunicacions. (DOUE L [en línia], núm. 24, 30-01-98, pàgs. 1 a 8). <https://www.boe.es/buscar/doc.php?id=DOUE-L-1998-80151>. [Consulta: 04/05/2017]

Unió Europea. Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques en el que respecte el tractament de dades personals i la lliure circulació d'aquestes dades. (DOUE L [en línia], núm. 281, 23-11-1995, pàgs. 31 a 50). <https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678>. [Consulta: 03/05/2017]

Unió Europea. Comunicació de la Comissió Europea, de 10 de gener de 2017, La Construcció d'una economia de les dades europea. (COM (2017) 9 final). < http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0009&from=EN>. [Consulta: 10/05/2017]

Unió Europea. Comunicació de la Comissió Europea, de 6 de maig de 2015, Una Estratègia pel Mercat Únic Digital d'Europa. (COM(2015) 192 final). <http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52015DC0192>. [Consulta: 10/05/2017]

Unió Europea. Comunicació de la Comissió Europea, de 19 d'abril de 2010, Una Agenda Digital per Europa. (COM (2010) 245 final/2). <http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:52010DC0245>. [Consulta: 20/05/2017]

Unió Europea. Comunicació de la Comissió Europea, de 3 de març de 2010, Europa 2020 Una estratègia per un creixement intel·ligent, sostenible i integrador. (COM (2010) 2020 final). <http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52010DC2020>. [Consulta: 10/05/2017]

Unió Europea. Dictamen 8/2014 del Grup de Treball de l'article 29, de 16 de setembre de 2014, sobre l'evolució recent de l'Internet dels Objectes (WP 223). <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf>. [Consulta: 10/04/2017]

Unió Europea. Dictamen 5/2014 del Grup de Treball de l'article 29, de 10 d'abril de 2014, sobre tècniques d'anonimització (WP 216). <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf> [Consulta: 04/06/2017].

Unió Europea. Dictamen 1/2010 del Grup de Treball de l'article 29, de 16 de febrer de 2010, sobre els conceptes de <<responsable del tractament>> i <<encarregat del tractament>> (WP 169).

<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf>. [Consulta: 20/04/2017]

Unió Europea. Informe de la Comissió d'Assumptes Jurídics del Parlament Europeu, de 27 de gener de 2017, amb recomanacions destinades a la Comissió sobre normes de Dret civil sobre robòtica. (2015/2013 (INL)) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//ES>. [Consulta: 14/04/2017]

Aliança pel Govern Obert. Declaració del Govern Obert, de l'Aliança pel Govern Obert, de setembre de 2011. <https://www.opengovpartnership.org/open-government-declaration>. [Consulta: 16/05/2017]

Unió Internacional de Telecomunicacions. Recomanació de la Unió Internacional de Telecomunicacions, de 15 de juny de 2012, Descripció General de Internet dels Objectes. (Y.2060). <https://www.itu.int/rec/T-REC-Y.2060-201206-I/es>. [Consulta: 10/04/2017]

Sentències

Sentència del Tribunal Constitucional 290/2000, de 30 de novembre de 2000.

Sentència del Tribunal Constitucional 292/2000, de 30 de novembre de 2000.

Sentència del Tribunal de Justícia de la Unió Europea 2014/85, de 13 de maig de 2014. Cas Google Spain S.L. contra Agència Espanyola de Protecció de Dades (AEPD). C-131/12.

Pàgines web

Amazon Dash Button. <https://www.amazon.es/b?ie=UTF8&node=10909716031>. [Consulta: 07/04/2017]

Amazon Dash Replenishment Service. <https://developer.amazon.com/dash-replenishment-service>. [Consulta: 07/04/2017]

Fox News Tech. TV news report prompts viewers' Amazon Echo devices to order unwanted dollhouses. <http://www.foxnews.com/tech/2017/01/06/tv-news-report-prompts-viewers-amazon-echo-devices-to-order-unwanted-dollhouses.html>. [Consulta: 08/04/2017]

Gartner IT Glossary. <http://www.gartner.com/it-glossary/big-data>. [Consulta: 09/04/2017]