



**Universitat  
Autònoma  
de Barcelona**



**Facultat de Dret**

Departament de Dret Públic i Ciències Històricojurídiques  
Doctorat en Dret Públic Global

**TESI DOCTORAL**

# **LA RESPONSABILITAT DAVANT LA INTEL·LIGÈNCIA ARTIFICIAL EN EL COMERÇ ELECTRÒNIC**

Autora

Elisabet Martín i Palomas

Director

Dr. Antonio Morales Plaza

Tutor

Dr. Manuel Ballbé Mallol

2014



## Presentació

---

Les pàgines que integren aquest treball són el resultat d'un estudi laboriós i prolongat, però per a mi absolutament apassionant. Els antecedents del meu interès pel tema escollit, cal buscar-los en l'evolució de la meua pròpia carrera professional. La vaig iniciar en diferents llocs de l'Administració Pública, i durant el meu pas per l'Agència Catalana del Consum, vaig percebre que els conflictes entre els usuaris i les empreses moltes vegades eren deguts a la diferent interpretació del terme responsabilitat. Això era encara més complex si el conflicte es referia al comerç electrònic realitzat a través d'Internet.

A causa de l'entorn en què es mou internet, aquesta és una qüestió complexa que suposa molts conflictes a superar pel legislador i pel poder judicial. Al mateix temps, la globalització en un espai virtual, fa que la limitació territorial de la responsabilitat o simplement de la llei a aplicar, siguin també temes complexos i en constant evolució.

Vaig passar un any a la Delegació del Govern de la Generalitat de Catalunya a Brussel·les, i després un altre a la University of International Business and Economics de Pequín (对外经济贸易大学-国际学院). Vaig poder comprovar llavors que en cultures i marcs normatius tan diferents aquesta problemàtica era molt semblant. Poc després vaig entrar a treballar en el que avui és un dels grups empresarials relacionat amb el comerç electrònic més prestigiós, el Grup eBay. Allà vaig poder

comprovar com la ingent quantitat de dades a tractar en una multinacional d'aquesta importància, fa del rigor en la gestió, i l'ús de sistemes automatitzats elements fonamentals per mantenir els adequats nivells de qualitat en el servei.

Aquestes experiències em van fer interessar molt aviat en els efectes que podrien tenir sobre el comerç electrònic un tema tan complex com és la progressiva generalització de sistemes cada vegada més autònoms gràcies a la incorporació de metodologies d'intel·ligència artificial, i al desenvolupament de nous paradigmes, com els representats per l'emergència de l'anomenada Web 3.0.

Per tot això, vaig decidir centrar el meu treball de doctorat en un aspecte concret del comerç electrònic, que al meu entendre serà cada vegada més actual, com és el de la responsabilitat per les conseqüències de les accions realitzades per sistemes autònoms, sense la participació directa de cap ésser humà, és a dir, les anomenades "màquines intel·ligents".

Durant els anys que vaig dedicar a aquesta tasca, simultaniejant amb les meves obligacions laborals, han estat moltes les persones que m'han donat suport i que amb els seus coneixements, el seu afecte, i la seva comprensió han fet possible aquest treball. No m'és possible citar totes elles en tan poc espai, però vull simbolitzar el meu agraïment a totes elles nomenant algunes de les que més m'han ajudat.

El meu director, el Doctor Antonio Morales Plaza, una ment brillant, va ser per a mi un gran referent i el qual em va proporcionar la sentència del Tribunal de Justícia de la Unió Europea en el cas de L'Oréal contra eBay (Cas C-324/09) just quan es va publicar. El Doctor Manuel Ballbé Mallol, la paciència, bon fer, i grans coneixements, van fer d'ell un tutor

inestimable, el qual també em va facilitar articles molt interessants i de gran actualitat. Els doctors Jordi Mundó Blanch i Juli Sabaté Delgado i el professor Naixiang Feng les idees i aportacions dels quals em van resultar de gran utilitat. Ramon Galindo Caldés i Inés Martínez Capón que em van ajudar amb la seva amistat i els seus comentaris.

Durant el temps que va durar la realització d'aquest treball van néixer les meves dues meravelloses nebodes, Ona Akiko i Nora Graham, i ja està en camí un/a tercer/a. Elles, junt amb els meus germans, Manel i Xavier, i les seves dones Marlen Arvelo i Sara Yamaka, van ser un referent permanent i una font d'il·lusió. També ho va ser Sergi Garcia Vila, company de fatigues, projectes vitals i llargues converses, que des de la llunyana Xangai va saber transmetre'm el seu afecte i el seu suport.

Especial significat va tenir per a mi l'inestimable suport de Manuel Martín Fernández i Magda Palomas Atcher, "tanto monta monta tanto", que a més de donar-me el meravellós regal de la vida, em van aportar idees, correccions i unes fantàstiques truites de patates que van fer més suportables les interminables nits de treball (gràcies mama).

Aquest treball no hagués estat possible sense el de tants intel·lectuals, acadèmics i professionals, que amb el seu esforç van fer avançar el coneixement i ens van donar les eines intel·lectuals necessàries als que tractem de seguir el camí que ells ens van marcar. De qualsevol mèrit que aquestes pàgines puguin tenir ells són els autèntics responsables. Jo m'he limitat a desenvolupar aquest treball des del privilegi de poder-ho fer pujant-me a les espatlles dels gegants que m'han precedit, dels que m'han format i dels que m'han donat suport. A tots ells moltes gràcies.



# Índex

---

<b>Introducció: L'ahir ja va passar i el demà està passant .....</b>	<b>13</b>
Interacció de persones i màquines intel·ligents .....	13
Nou comerç o nou entorn comercial .....	15
Una hipòtesi de partida .....	16
El contingut del treball .....	18
<b>1ª Part: Del significat al significant: definint un marc teòric .....</b>	<b>29</b>
<u>Capítol primer: La intel·ligència artificial.....</u>	<u>31</u>
El concepte d'intel·ligència artificial.....	31
El Test de Turing.....	35
Intel·ligència Artificial en dispositius automatitzats.....	38
Màquines interaccionant amb màquines.....	40
<u>Capítol segon: Construcció social del concepte de responsabilitat.....</u>	<u>47</u>
Responsabilitat i responsabilitat indirecta.....	47
Responsabilitat d'animals i objectes inanimats .....	50
Influències culturals enfront de la responsabilitat.....	52
La responsabilitat en les noves tecnologies.....	55
<u>Capítol tercer: Internet: una xarxa de xarxes.....</u>	<u>61</u>
El ciberespai, una nova realitat virtual .....	61
Les arquitectures: del web 1.0 a la 2.0 .....	66
Web 3.0: un espai per a màquines intel·ligents .....	70
Internet i les amenaces a la seguretat .....	72

<u>Capítol quart: Comerç electrònic.....</u>	<u>77</u>
El comerç electrònic.....	77
Dret Internacional Privat .....	79
Regulació legal.....	81
Les activitats del comerç electrònic .....	87
<u>Capítol cinquè: Una perspectiva jurídica.....</u>	<u>95</u>
Les noves tecnologies davant les branques del dret .....	95
El dret anglosaxó i el continental .....	98
Desjudicialització de conflictes i mediació en línia .....	100
Dret penal del risc .....	105
<b>2<sup>a</sup> Part: Un nou espai par al comerç electrònic .....</b>	<b>107</b>
<u>Capítol sisè: Big Data: superant els límits .....</u>	<u>109</u>
Gestió de grans volums de dades .....	109
Dades estructurades i no estructurades.....	113
El concepte de macrodades o <i>Big Data</i> .....	115
Responsabilitat en el tractament de <i>Big Data</i> .....	122
<u>Capítol setè: Propietat intel·lectual de les obres .....</u>	<u>127</u>
La protecció jurídica de la propietat intel·lectual.....	127
Propietat de les obres no creades per persones.....	133
Drets d'autor en l'entorn europeu .....	136
Drets de copyright en l'entorn anglosaxó .....	140
<u>Capítol vuitè: La responsabilitat dels intermediaris .....</u>	<u>145</u>
Límits a la responsabilitat del proveïdor de serveis .....	145
Un concepte d'interpretació confusa.....	148
Principi de solidaritat entre responsables del dany .....	152
Teoria del coneixement efectiu.....	153



<u>Capítol novè: Plataformes d'intermediació .....</u>	<u>159</u>
Plataformes d'intermediació: L'exemple d'eBay .....	159
Polítiques de privacitat.....	163
Possibles il·legalitats i responsabilitat de l'intermediari .....	166
L'Oréal vs. eBay .....	172
<u>Capítol desè: Protecció de la marca .....</u>	<u>179</u>
Infraccions contra els drets de marca.....	179
La protecció de les marques.....	181
La territorialitat a Internet .....	185
Altres aspectes relatius al dret d'ús de la marca.....	189
<b>3ª Part: Les amenaces als drets personals .....</b>	<b>193</b>
<u>Capítol onzè: La protecció de dades personals .....</u>	<u>195</u>
Obtenció i tractament de dades personals .....	195
El consentiment per al tractament de dades personals .....	198
El dret de protecció de les pròpies dades.....	202
Dades que permeten identificar l'usuari.....	206
<u>Capítol dotzè: empremta digital i signatura electrònica .....</u>	<u>211</u>
L'empremta digital .....	211
L'empremta digital dels productes electrònics .....	213
L'empremta digital dels usuaris .....	215
La signatura electrònica com a identificador .....	217
<u>Capítol tretzè: Cookies un sistema d'obtenció d'informació .....</u>	<u>223</u>
La regulació legal de les "galetes" ( <i>cookies</i> ) .....	223
Necessitat de prèvia autorització de l'usuari .....	226
La política de galetes de Google .....	232

<u>Capítol catorzè: Enllaços i investigació per internet .....</u>	<u>237</u>
Navegació, enllaços i P2P.....	237
Els enllaços com a comunicació pública .....	240
Allotjament d'arxius: El cas Megaupload .....	244
Recopilació automàtica d'enllaços i continguts.....	246
<u>Capítol quinze: Privacitat i dret a la intimitat .....</u>	<u>249</u>
Protecció jurídica de la intimitat .....	249
La cibercensura .....	253
El repte de l'automatització .....	260
<b>4ª Part: De la culpa del cavall a la culpa del robot.....</b>	<b>265</b>
<u>Capítol setzè: Publicitat i les seves possibles males pràctiques .....</u>	<u>267</u>
La publicitat en Internet.....	267
Personalitzant la publicitat.....	269
L'ús del correu electrònic per a publicitat .....	274
Requisit de consentiment previ.....	278
<u>Capítol dissetè: Creixement de la logística robotitzada .....</u>	<u>281</u>
L'automatització de la logística .....	281
El risc de la fal·làcia androide .....	284
Responsabilitat per danys provocats per robots .....	287
Robots autònoms letals .....	290
<u>Capítol divuitè: La mobilitat en el cicle del comerç electrònic .....</u>	<u>299</u>
Mobilitat automatitzada de productes i persones.....	299
Els vehicles autònoms .....	304
Resposta legal als vehicles autònoms .....	309

<u>Capítol dinovè: Fenomenologia dels sistemes de pagament virtual.....</u>	<u>315</u>
Els sistemes de pagament tradicionals .....	315
PayPal i d'altres passarel·les de pagament.....	317
Bitcoin i d'altres monedes virtuals .....	320
La responsabilitat per l'ús de les monedes virtuals.....	324
<u>Capítol vintè: Del núvol virtual a la web profunda .....</u>	<u>329</u>
Computació en núvol ( <i>Cloud Computing</i> ) .....	329
La responsabilitat en la computació en núvol .....	331
De l'anonimat a la web profunda.....	334
La web profunda i els seus riscos .....	336
<b>Com a conclusió: La responsabilitat no és delegable .....</b>	<b>339</b>
Tecnologia, valors i procediments.....	339
Intel·ligència Artificial i comerç electrònic .....	340
La responsabilitat de les màquines intel·ligents.....	342
A tall de conclusió.....	344
<b>Bibliografia.....</b>	<b>347</b>
<b>Legislació .....</b>	<b>359</b>
<b>Jurisprudència i altres resolucions .....</b>	<b>369</b>



## **Introducció:**

### **L'ahir ja va passar i el demà està passant**

---

#### **Interacció de persones i màquines intel·ligents**

La virtualització que comporta internet modifica profundament, entre altres coses, la nostra concepció de l'espai. La realitat en el món virtual no està vinculada a un espai geogràfic determinat, ni a uns interlocutors concrets. Es tracta d'un nou espai en el que el mateix concepte d'espai és relatiu. La realitat en l'espai virtual és intangible, però no per això és menys real. Si a aquesta intangibilitat li sumem la potència intel·lectual que les tecnologies d'intel·ligència artificial aporten a les màquines, no és estrany que sorgeixin nombroses, i de vegades inquietants, preguntes sobre el futur de les societats que emergiran d'aquesta nova realitat.

De fet, és cada vegada més freqüent l'atribució a les màquines d'una capacitat intel·lectual igual, o fins i tot superior, a la dels propis éssers humans. Algunes de les característiques que tradicionalment definien l'ésser humà, com la memòria, la paraula, la capacitat de calcular, o raonar, i altres de similars, són avui realitzades de manera molt més eficient per màquines dotades d'intel·ligència artificial. Aquesta evolució de la tecnologia ha potenciat la difusió de diferents teories, visions i corrents filosòfics, que pretenen explicar les conseqüències que aquesta evolució tindrà en les nostres societats. Algunes d'aquestes visions

semblen més pròpies de la ciència ficció, però la veritat és que totes elles tenen els seus defensors i detractors.

Alguns autors, des d'un plantejament transhumanista, defensen que en el futur home i màquina arribaran a fondre's en un mateix ésser, constituint una mena de ciborg humanoide. Així, per exemple, un dels autors actuals més característics de la singularitat tecnològica, o singularitarianisme<sup>1</sup>, Ray Kurzweil, sosté que l'acceleració tecnològica farà que en pocs anys el desenvolupament de la intel·ligència artificial, els nano robots, les pròtesis i altres enginys similars, provocaran que home i màquina siguin difícilment diferenciables i que sorgirà amb això un nou home màquina pràcticament immortal (Kurzweil, 2005).

Altres autors sostenen que a mesura que les màquines van adquirint més intel·ligència, adquireixen també més autonomia, el que les fa cada cop més similars a l'ésser humà. Aquests autors plantegen una situació en què les màquines arribaran a superar l'ésser humà, constituint-se en una nova espècie intel·ligent. Moravec arriba a afirmar que cap a l'any 2050 els robots hauran superat en intel·ligència als éssers humans, el que farà que siguin ells els que investiguin i facin avançar la ciència i la cultura (Moravec, 1988).

D'altra banda, són molts més els que defensen que les màquines són només màquines, i que l'anomenada intel·ligència artificial no és més que la capacitat de la que podem dotar les màquines de reproduir processos mentals aparentment intel·ligents.

---

<sup>1</sup> Corrent teòric transhumanista que sosté que al voltant de l'any 2045 la intel·ligència artificial dels ordinadors serà més gran que la intel·ligència de tots els cervells humans del món junts, i això portarà a una simbiosi home màquina impensable en l'actualitat.

Només el futur ens permetrà conèixer quines teories o plantejaments tenen més aspectes de realitat. No obstant això, mentre arriba aquest futur, sobre el qual en realitat ningú té respostes segures, la veritat és que l'evolució tecnològica va avançant, i amb ella la necessitat d'abordar els possibles conflictes que diàriament apareixen en el ciberespai i les diferents interpretacions que tot això comporta.

## **Nou comerç o nou entorn comercial**

Des de la mateixa aparició d'internet, i amb això la generalització del comerç electrònic, s'ha plantejat repetidament el dubte de si es tracta d'un nou comerç, amb els seus propis valors, paradigmes i normes, o si en realitat estem davant el comerç de sempre, encara que desenvolupat en un nou espai virtual, diferent a l'espai físic en què tradicionalment s'havia realitzat.

Sigui quina sigui la resposta, un dels reptes que tot això pot comportar és la gestió d'una creixent tendència a diluir les responsabilitats de l'ésser humà amb motiu de les accions realitzades amb ajuda de sofisticats algoritmes, o fins i tot als danys produïts directament per màquines dotades d'intel·ligència artificial i sense cap participació humana en l'acció de què es tracti.

Tal com plantejava Dieguez en analitzar la possible competència entre éssers humans i robots intel·ligents, un dels perills més immediats i reals en relació a les computadores és que "la dependència de les màquines a l'hora de prendre decisions en àmbits d'especial importància social, [...] l'extensió del seu domini sobre cada vegada més aspectes de les nostres

vides, i la dilució de responsabilitats que el mateix sistema tecnològic imposa, poden aconseguir que el control efectiu de l'ésser humà sobre les seves pròpies accions disminueixi seriosament" (Dieguez, 2001).

Sense entrar a valorar els diferents posicionaments teòrics davant d'aquesta nova realitat, sí que es fa necessari conèixer fins a quin punt les perspectives obertes pels avenços en intel·ligència artificial estan alterant, o poden fer-ho a curt o mig termini, la visió legal i de la jurisprudència, sobre la responsabilitat en matèries tan importants com les relacionades amb el comerç electrònic en les seves diferents facetes.

## **Una hipòtesi de partida**

Les situacions que les noves tecnologies presenten, fan que en la pràctica sigui cada vegada més complex per la legislació i la jurisprudència donar resposta a les diferents problemàtiques que van apareixent. Fins i tot, alguna corrent teòrica sosté la necessitat que es generi una mena de marc normatiu virtual gestionat pels propis usuaris, ja que per a ells resulta evident la impossibilitat que els sistemes tradicionals puguin regular adequadament l'espai virtual representat especialment per Internet.

En el comerç electrònic, igual que succeeix en moltes altres activitats, es produeixen situacions en què entren en conflicte interessos de vegades contradictoris o oposats. Es fa doncs necessari trobar l'equilibri entre aquests interessos quan tots ells són legítims, o establir clarament quins són els nivells de protecció de cada un dels béns jurídics en conflicte.



Així doncs, per exemple, drets com la llibertat d'informació o l'accés i gaudiment de les obres culturals, pot entrar en conflicte amb el dret dels autors a la protecció de la seva propietat intel·lectual. El dret a la intimitat d'uns pot entrar en conflicte amb el dret a la informació d'altres o, fins i tot en alguns casos, amb la interpretació que en cada moment pugui fer l'Estat en relació al que consideri "Seguretat Nacional".

Quan aquests interessos contraposats són gestionats per persones, l'atribució de responsabilitat gira al voltant precisament d'aquestes persones. No obstant això, quan el conflicte es genera per l'acció automatitzada d'un sistema, compost per algorismes i mitjançant la progressiva incorporació de tècniques basades en intel·ligència artificial, és a dir, sense intervenció directa de cap ésser humà, el tema de la responsabilitat com a conseqüència de les accions d'aquest sistema es fa bastant més complex.

En aquest treball es parteix de la hipòtesi que el desenvolupament de sistemes dotats d'intel·ligència artificial, o el que podríem definir com màquines intel·ligents, no modifica el paradigma de la responsabilitat com una cosa aplicable en exclusiva als éssers humans en una activitat tan complexa com és en la pràctica el comerç electrònic.

Per realitzar aquest treball, la metodologia utilitzada ha estat l'anàlisi de la diferent normativa i la jurisprudència existent sobre la responsabilitat en relació als valors i matèries que més fàcilment podrien quedar alterats a l'introduir en el comerç electrònic sistemes automatitzats, capaços d'actuar sense la supervisió de cap ésser humà.

En el treball també s'analitza el marc normatiu i jurisprudencial, tant a nivell nacional com internacional, en relació a les activitats més

característiques del comerç electrònic, com poden ser la publicitat, la logística, la mobilitat o el pagament dels serveis, amb una especial referència a l'aparició d'entorns com el núvol virtual i la web profunda.

## **El contingut del treball**

Aquest treball es planteja per tal de detectar qualsevol possible modificació, atenuació o delegació a l'atribució de responsabilitats als éssers humans, davant les conseqüències de les accions de les màquines i els sistemes dotats d'intel·ligència artificial quan aquests funcionen de manera autònoma i aparentment intel·ligent.

El treball consta de quatre parts diferenciades, cadascuna de les quals es compon de cinc capítols. A la primera part es plantegen els aspectes teòrics dels principals conceptes que formen part consubstancial del tema en estudi.

El primer capítol analitza la intel·ligència artificial. Després de plantejar les diverses accepcions relatives a la intel·ligència, es presenta la intel·ligència artificial com el principal element diferenciador dels diferents sistemes i dispositius automatitzats. Es planteja la intel·ligència artificial seguint aquells autors que tradicionalment han analitzat la intel·ligència com una cosa característica de l'ésser humà.

L'aplicació d'intel·ligència artificial a sistemes i màquines automatitzades planteja uns reptes que obliguen a redefinir el mateix concepte d'intel·ligència. La intel·ligència deixa de ser una cosa mesurable en comparació amb les capacitats humanes per esdevenir alguna cosa

orientada, no tant a aproximar-se a la intel·ligència humana, com a donar resposta amb les característiques pròpies d'aquests sistemes.

En el capítol dos es planteja la interpretació històrica del concepte responsabilitat, definint la interpretació que actualment es dona a aquest terme, tant en relació amb la responsabilitat directa com amb la indirecta. Es planteja en el capítol la importància de les influències culturals i religioses del concepte responsabilitat i es presenten situacions que al llarg de la història han atribuït responsabilitat no només a les persones sinó també a animals i a objectes inanimats. L'aparició de les noves tecnologies unit al desenvolupament de la intel·ligència artificial plantegen la necessitat d'analitzar la resposta que la legislació i la jurisprudència actual adopten davant la responsabilitat pels fets provocats pels sistemes que actuen de manera automatitzada sense la intervenció directa de cap ésser humà.

En el tercer capítol es planteja el ciberespai com una realitat virtual en la que internet configura una xarxa de xarxes que està canviant els sistemes de comunicació i les pautes de comportament vigents a les nostres societats. Després d'analitzar les diferències en les diverses etapes per les que s'ha anat desenvolupant internet, s'expliquen les diferències que aporta l'anomenada Web 2.0 respecte als inicis d'Internet.

A continuació s'analitza l'anomenada Web 3.0 com un espai dissenyat específicament per donar resposta a la generalització de sistemes capaços d'interpretar semànticament les preferències de l'usuari i establir un entorn en el que, gràcies a la intel·ligència artificial, els sistemes desenvolupen cada vegada més recursos per gestionar la

informació de manera totalment automatitzada. El capítol acaba fent una descripció de les principals amenaces a la seguretat que presenten els desenvolupaments exponencials d'internet.

El capítol quart se centra a analitzar el comerç electrònic, no com un tipus de comerç diferent del tradicional, sinó com un espai diferent en el qual es desenvolupa aquest comerç. Després d'analitzar la regulació legal del comerç electrònic s'aprofundeix en la importància del dret internacional privat en aquest tipus de comerç, ateses les particulars característiques de l'entorn virtual. És precisament el fet que el comerç electrònic constitueixi un entorn específic diferent del tradicional el que fa necessari potenciar la protecció jurídica del consumidor enfrontat a noves amenaces. El comerç electrònic introdueix també uns productes electrònics inexistents en l'entorn tradicional com pot ser la compravenda de programes i sistemes informàtics, la gravació i distribució electrònica d'obres protegides per drets d'autor, així com la potenciació de valors específicament amenaçats en aquest entorn com poden ser la protecció de la intimitat, la protecció de marques i els drets de propietat intel·lectual.

El cinquè i últim capítol de la primera part analitza la influència del ciberespai, i en general de les noves tecnologies de la informació, en les branques tradicionals del dret. El risc que introdueixen les noves tecnologies en la societat en general s'analitzen en aquest capítol des de la perspectiva de la legislació i la jurisprudència actual donant resposta a aquests riscos. Concepte com la *International Cyber Law*, o les diferències entre els models anglosaxons i els continentals en temes com la protecció dels drets d'autor o la llibertat personal presenten en tots dos casos diferències que es plantegen.

La resposta que la normativa actual i les interpretacions jurídiques que els tribunals i les organitzacions internacionals donen a la progressiva aparició de sistemes dotats d'intel·ligència artificial, permeten analitzar la tendència en el tema de la responsabilitat pels danys produïts per les accions de sistemes actuant sense la presència de cap ésser humà

La segona part del treball aprofundeix en algunes de les principals característiques en constant evolució en l'espai virtual representat per internet. Així el capítol sisè planteja la problemàtica inherent a la gestió de grans volums de dades. El que se sol denominar *Big Data* és cada vegada més una realitat constant no només en el comerç electrònic, sinó en tots els camps desenvolupats en aquest entorn. En el capítol es plantegen nous termes com macrodades, dades estructurades i dades no estructurades i en general nous conceptes que impliquen un tractament específic d'aquests grans volums de dades.

Davant la impossibilitat que la gestió de *Big Data* pugui ser realitzada de manera eficient per l'ésser humà de manera directa fa que el seu tractament s'hagi de deixar a sistemes automatitzats, el que planteja el tema de la responsabilitat en la gestió de les dades tractades automàticament per sistemes cada vegada més potents i utilitzant tecnologies d'intel·ligència artificial.

En el capítol set es planteja la protecció jurídica de la propietat intel·lectual, diferenciant la protecció atorgada a les obres en el món anglosaxó a través del *copyright* dels atorgats en el món continental. Tot i que els efectes d'aquestes diferències són limitats en la pràctica, el major èmfasi posat a l'entorn europeu sobre els drets morals de l'autor, a diferència de la prioritat donada a la defensa de l'obra en el *copyright*,

planteja alguns efectes que s'analitzen. L'eix d'aquesta anàlisi és específicament la propietat de les obres no creades per persones, entre les quals cal incloure les realitzades per màquines.

El vuitè capítol se centra en la responsabilitat dels intermediaris, encarregats de proveir els serveis que faciliten l'accés i ús d'internet. L'existència de límits a aquesta responsabilitat, i teories com la de coneixement efectiu, o la de solidaritat entre responsables d'un dany són analitzats en aquest capítol.

Per a què es doni responsabilitat en algun dels proveïdors de serveis cal per altra banda que es doni algun tipus de participació, facilitació, o coneixement concret de la possible infracció que es cometi a través dels seus serveis, o que la situació no sigui revertida immediatament, tan aviat com en tingui coneixement. Tot això qüestiona el paper dels sistemes automatitzats, en aquest tema.

Plataformes d'intermediació, aplicades especialment al comerç electrònic constitueixen el tema que s'aborda en el capítol nou. A partir de la sentència del Tribunal de Justícia de la Unió Europea en el cas L'Oréal contra eBay<sup>2</sup>, s'estudia els efectes que determinades situacions poden tenir sobre els límits a la responsabilitat per part dels proveïdors de serveis. Es plantegen els fonaments en què es basa la sentència, així com les polítiques de privacitat provocades per les plataformes d'intermediació així com els proveïdors de serveis d'internet en general.

---

<sup>2</sup> Disclosure: I am an employee of eBay Inc. The opinions expressed here are my own and do not necessarily reflect the opinions of eBay Inc.

Descàrrec de responsabilitat: Sóc una treballadora d'eBay Inc. Les opinions expressades aquí són les meves i no necessàriament reflexen les opinions d'eBay Inc.

En el capítol desè s'estudien els efectes d'internet sobre la protecció de les marques, especialment en tot el relatiu al comerç electrònic. Entre les diferents infraccions contra els drets de marca, i les característiques específiques que les mateixes poden presentar a internet, destaca com a fonamental tot el relacionat amb la territorialitat en el món virtual. A part de l'anàlisi normatiu que afecta els drets de marca, tant a nivell europeu com nacional, s'analitzen algunes de les conseqüències que la sentència en el cas L'Oréal contra eBay presenten en relació a aquest tema.

La tercera part del treball se centra en l'estudi de les amenaces als drets personals més habituals en el comerç electrònic, destacant els efectes que l'aplicació de sistemes dotats d'intel·ligència artificial poden presentar. Així el capítol onze se centra en la protecció de dades personals i tot el relacionat amb la seva obtenció i tractament. El dret de protecció de les dades personals implica la necessitat de consentiment explícit, per al seu tractament, per part del seu titular. S'analitza en el capítol al significat de dades personals i s'assimila a les mateixes totes aquelles que permetin identificar a un usuari en concret.

L'empremta digital i la signatura electrònica, com a elements de garantia de la personalitat de l'usuari, constitueix el tema que s'aborda en el capítol dotze. En aquest capítol es diferencia clarament el concepte d'empremta digital dels usuaris del que es pot trobar en els productes, especialment en els productes electrònics.

Com a continuació dels estudis de l'empremta digital dels usuaris es planteja els efectes de la signatura electrònica com a element identificador de les persones. Els processos de mecanització i

funcionament dels sistemes automatitzats, en relació a l'empremta digital i la signatura electrònica són analitzats en aquest capítol.

El capítol tretze se centra en un dels sistemes més utilitzats actualment per a l'obtenció d'informació personal dels usuaris. Es tracta de les galetes, més conegudes per la seva terminologia anglesa de *cookies*. Aquest tema analitza les galetes emprades com a element fonamental en les campanyes de publicitat, així com la necessitat del consentiment de l'usuari per a la seva instal·lació en el seu sistema. S'estudia la política de galetes a les plataformes d'internet, plantejant l'exemple de les polítiques practicades sobre el tema per Google. La regulació legal de les galetes, tant a nivell nacional com internacional i la interpretació de la jurisprudència sobre elles completa aquest capítol.

El capítol catorze analitza els enllaços, comunament coneguts per la seva denominació en anglès *links*, així com als intercanvis d'arxius directament entre usuaris a través de metodologies *Peer to Peer* (P2P). S'analitzen les conseqüències del recull automàtic d'enllaços i continguts i es fa especial referència a casos com el de la plataforma d'allotjament d'arxius Megaupload. La consideració dels enllaços com a comunicació pública o no, constitueix un element fonamental per analitzar les conseqüències de la seva incorporació a les pàgines web.

L'últim capítol d'aquesta tercera part, el capítol quinze, analitza específicament els riscos que les noves tecnologies presenten per a la privacitat i el dret a la intimitat. S'analitza en profunditat la protecció jurídica de la intimitat tant a nivell nacional com internacional. Des d'aquesta perspectiva es planteja el repte de l'automatització, així com les diferents traves i restriccions a la lliure circulació de la informació, i



molt especialment a la cibercensura. Els mecanismes utilitzats pels usuaris partidaris de l'anonimat, constitueixen un dels aspectes tractats en aquest capítol.

La quarta i última part d'aquest treball se centra en les diferents activitats més usuales en el desenvolupament del comerç electrònic. Així el capítol setze analitza la publicitat i les possibles males pràctiques. La publicitat a internet és l'objectiu principal de gran part dels sensors i sistemes desenvolupats per obtenir informació personal, i amb això generar bases de dades que permetin la major personalització possible d'aquesta publicitat cap al públic diana més susceptible de ser influenciat per aquesta publicitat.

La personalització de la publicitat afecta els diferents camps desenvolupats a internet, entre els quals destaca l'ús massiu de correus electrònics amb tècniques de *spam*. S'analitzen en aquest capítol aquests sistemes, així com el requisit del consentiment previ com a element fonamental per a la recepció de la publicitat.

En el capítol disset s'analitza específicament la cada cop més estesa robotització dels sistemes de logística emprats en el comerç electrònic. Per analogia s'estudia l'efecte de la responsabilitat per danys provocats pels robots en altres camps no específics de la logística del comerç electrònic, però d'importància per conèixer la posició del legislador i la jurisprudència davant aquests sistemes. S'analitza específicament l'anomenat risc de la fal·làcia androide, així com el desenvolupament de robots autònoms letals.

En el capítol divuit es planteja la mobilitat com a part fonamental en el cicle del comerç electrònic, ja que la venda implica fer arribar al

consumidor el producte adquirit. En plantejar la mobilitat automatitzada de productes i persones s'estudia la normativa desenvolupada per a la gestió dels vehicles autònoms, és a dir aquells capaços de circular per les vies públiques sense la presència física en el lloc de cap ésser humà ni que aquest el condueixi de forma remota.

Els vehicles dotats de sistemes d'intel·ligència artificial i sensors capaços d'analitzar l'entorn es refereixen no només als que circulen per terra com ferrocarrils i automòbils sense conductor, sinó que es planteja també el cas específic dels vehicles capaços de desplaçar-se per l'aire sense conductor, també coneguts com a drones, tant en la seva versió de pilotatge remot com els que tenen un funcionament totalment autònom.

El capítol dinou es refereix a la conclusió de l'activitat comercial que constitueix el pagament del producte adquirit. La fenomenologia de pagament virtual inclou els sistemes de pagament tradicionals i les passarel·les de pagament específicament desenvolupades per a internet com poden ser PayPal i altres passarel·les similars. Es fa especial referència a les monedes virtuals generades de manera autònoma per algorismes matemàtics sense suport de cap sistema tradicional com bancs centrals o estats nacionals.

S'estudia en profunditat la responsabilitat possible per l'ús de les monedes virtuals, fent una menció especial a Bitcoin, ja que es tracta de l'exemple més estès d'entre les diferents monedes desenvolupades fins al moment en l'entorn virtual representat per internet.

El capítol vint és l'últim capítol d'aquesta quarta part en què es plantegen les conseqüències de la generalització de les activitats

d'internet incloent el comerç electrònic en l'anomenada computació en núvol (*Cloud computing*). Es planteja la responsabilitat per les activitats i els serveis oferts en núvol a través d'una multiplicitat de proveïdors de serveis, cadascun dels quals aporta una part del contingut global que constitueix el servei finalment configurat pel client, que pot així arribar a oferir serveis de comerç electrònic, o qualsevol altre servei que desitgi, sense la necessitat de desenvolupar notables inversions en infraestructures i en els programes necessaris per gestionar els seus productes.

En el mateix capítol s'analitza la web profunda (*The Deep Web*) i els seus riscos. La recerca per part de molts usuaris de l'anonimat davant diverses cibercensures fa que es generi un entorn virtual basat específicament en l'anonimat que presenta nous reptes per a l'atribució de responsabilitats i que facilita l'aparició d'activitats il·lícites o directament delictives.

El treball conclou amb un capítol en el qual es presenten les conclusions relatives a la responsabilitat en les activitats de comerç electrònic en tot allò relacionat amb les activitats de les màquines dotades amb intel·ligència artificial. Amb la bibliografia i els annexos finalitza aquest treball.



## **1ª Part:**

### **Del significat al significant: definint un marc teòric**



## Capítol primer: La intel·ligència artificial

---

### El concepte d'intel·ligència artificial

Des dels inicis de la informàtica l'ésser humà ha vist feta realitat una cosa que abans només era admès en l'àmbit de la ciència ficció, és a dir, la possibilitat que les màquines puguin exercir tasques intel·lectuals. De fet, el naixement de la informàtica es pot atribuir precisament als intents del Govern britànic durant la Segona Guerra Mundial de disposar d'algun sistema capaç de realitzar a prou velocitat la ingent quantitat d'operacions necessàries per desxifrar els missatges de ràdio interceptats entre els submarins alemanys i els seus comandaments a Berlín. Un grup de científics, entre els quals destaquen Alan Turing, Thomas H. Flowers, i M. Newman, van dissenyar amb aquest objectiu el que es pot considerar el primer ordinador digital de la història basada en tubs de buit, coneguda com "Colossus"<sup>3</sup>.

En realitat "Colossus" va ser concebuda des dels seus inicis com una potent calculadora capaç de realitzar gran nombre de càlculs booleans<sup>4</sup>,

---

<sup>3</sup> Encara que alguns autors difereixen d'aquesta consideració, seguim aquí a Herbert Simon que defineix el "Colossus" com la primera computadora Digital.

<sup>4</sup> Els càlculs booleans són aquells que utilitzen variables binàries, els coneguts 0 i 1 d'informàtica, i els hi aplica operadors de l'àlgebra de Boole com "o", "i" i la negació "no".

però tot i que trigaria alguns anys a desenvolupar-se la idea de la informàtica tal com avui la coneixem (Simon, 1995).

Si conceptuem la intel·ligència com “el conjunt de les habilitats cognitives o intel·lectuals necessàries per obtenir coneixements i utilitzar aquests coneixements de manera correcta per tal de resoldre problemes que tinguin un objectiu i una fita ben descrits”<sup>5</sup>, és a dir, la capacitat de fer eleccions, i fins i tot prediccions, a partir de les informacions i experiències acumulades (Resing i Drenth, 2007). No és estrany que l’aparició de màquines com “Colossus” possessin d’actualitat la por per a uns, i l’esperança per a altres, que algun dia es poguessin desenvolupar màquines intel·ligents. Neix així el concepte que avui coneixem com Intel·ligència Artificial, és a dir, els sistemes creats per l’ésser humà capaços d’aprendre, gestionar idees i conceptes, i en definitiva solucionar problemes.

Així i tot, el 1956 es considera generalment com el veritable any de naixement de la intel·ligència artificial, ja que una de les primeres ocasions en què es va utilitzar aquest terme va ser en la Conferència de Dartmouth de 1956<sup>6</sup>. Aquest acte va ser organitzat per Claude E. Shannon (Bell Telephone Laboratories), Marvin L. Minsky (Harvard University), Nathaniel Rochester (IBM Corporation) i John McCarthy (Dartmouth College) que, tal i com senyalava la introducció de la seva

---

<sup>5</sup> Són moltes les diferents definicions possibles del terme intel·ligència, però se segueix en aquest treball la definició de la intel·ligència donada per Resing, W., i Drenth, P. al ser una de les que millor s’adapten conceptualment a la interpretació que es planteja per la majoria d’autors que tracten actualment la intel·ligència artificial.

<sup>6</sup> Aquest estudi es va materialitzar en el *Dartmouth Summer Research Project on Artificial Intelligence*, celebrat a Hanover, New Hampshire, al 1955.



proposta de conferència, va servir per reunir diversos investigadors en ordinadors, processament del llenguatge natural, xarxes neuronals, teoria de la computació, abstracció i creativitat:

“... Proposem que durant l’estiu de 1956 es dugui a terme en el Dartmouth College a Hannover, New Hampshire, un estudi d’intel·ligència artificial de 2 mesos de durada i per a 10 persones. L’estudi és per a procedir sobre la base de la conjectura que cada aspecte de l’aprenentatge o qualsevol altra característica de la intel·ligència pot, en principi, ser tan precisament descrit que es pot fer una màquina per a simular-ho. Es farà un intent de trobar la manera de fer que les màquines usin el llenguatge, formin abstraccions i conceptes, resolguin tipus de problemes ara reservats per als éssers humans, i millorin per si mateixes. Creiem que un avenç significatiu es pot fer en un o més d’aquests problemes si un grup acuradament seleccionat de científics hi treballen conjuntament durant un estiu...” (McCarthy et al. 1955).

La resta dels assistents van ser Trenchard More, Arthur L. Samuel, Oliver G. Selfridge, Ray Solomonoff, Allen Newell i Herbert A. Simon<sup>7</sup>. Aquests dos últims van aprofitar l’ocasió per presentar el seu programa de raonament automàtic “Logic Theorist” que tractava d’imitar la capacitat de resoldre problemes d’un ésser humà i del qual es diu que va ser “el primer programa d’intel·ligència artificial” (Crevier, 1993). Aquest programa va aconseguir provar 38 dels primers 52 teoremes del capítol

---

<sup>7</sup> Herbert A. Simon, a part de ser un dels pares fundadors de la intel·ligència artificial, va ser un economista guardonat amb el Premi Nobel d’Economia l’any 1978.

2 de l'obra "Principia Mathematica" de Bertrand Russell i Alfred Whitehead.

Però el concepte d'intel·ligència artificial ha tingut diverses interpretacions, realitzades en base a diferents punts de vista. D'una banda, es pot veure la intel·ligència artificial com un camp de la informàtica dedicat a la construcció de programes executables. Així, Herbert Simon en parlar de la Intel·ligència Artificial, va afirmar:

"... El moment de la veritat és un programa en execució..."<sup>8</sup>.

Si ens fixem en els objectius que ha de perseguir aquest programa, veiem que per als defensors d'aquest plantejament la màquina ha de "pensar" racionalment, és a dir, deduir de manera lògica un fet nou a partir del coneixement de què disposa (Simon, 1995).

Un altre enfocament existent és el dels que sostenen que és suficient amb que la màquina actuï racionalment. En aquest cas no és tan important que el procés sigui conseqüència únicament de deduccions lògiques a partir del coneixement previ, sinó que es poden utilitzar altres mecanismes, sempre que siguin adequats per aconseguir el resultat buscat. S'està fent referència al fet que la màquina sigui un agent racional:

"... Un agent és qualsevol cosa que es pugui veure percebent el seu entorn a través de sensors i actuant sobre aquest entorn a través d'efectors..." (Russell & Norvig, 2009).

---

<sup>8</sup> Amb aquesta frase Simon resumeix la seva idea que la Intel·ligència Artificial només s'expressa segons siguin els resultats obtinguts en executar el programa.

D'altra banda tenim el model cognitiu, que es basa en què hi ha intel·ligència artificial quan la màquina raona com les persones. El primer programa d'ordinador que seguia aquest objectiu va ser el Solucionador General de Problemes creat el 1957 per Allen Newell, Joseph Carl Shaw i Herbert A. Simon. Cal destacar que el camp de la ciència cognitiva també es basa en aquest punt de vista.

Si en comptes d'observar el procés de raonament només es té interès en què la màquina actuï com les persones, tenim l'enfocament que Alan Turing apuntava al realitzar el que es coneix com el test de Turing.

## El Test de Turing

Alan Turing el 1950<sup>9</sup> va tractar de respondre a la inquietant qüestió de fins a quin punt les màquines són, o seran en un pròxim futur, capaces de pensar. Aquesta no era una qüestió nova sinó que des de feia molt temps ja havia diferents corrents filosòfics que plantejaven la qüestió de si és possible que una màquina pensi. Ja Descartes va plantejar el tema en 1637 en el seu Discurs del Mètode:

“... Quants autòmats o màquines semovents pot construir la indústria humana [...] ja que si bé es pot concebre que una màquina estigui feta de tal manera, que profereixi paraules, i fins que les profereixi a propòsit d'accions corporals que causin

---

<sup>9</sup> Alan Turing va publicar el 1950 a la revista Mind l'article "Computing Machinery and Intelligence" que va establir les bases del que al llarg dels anys s'ha convertit en un tema recurrent d'estudi, és a dir, si les màquines poden arribar algun dia a ser intel·ligents en el sentit humà del terme.

alguna alteració en els seus òrgans, com, *verbi gratia*, si se la toca en una banda, que preguntí el que se li vol dir, i si en una altra, que cridí que se li fa mal, i altres coses pel mateix estil, tanmateix, no es concep que ordeni de diverses maneres les paraules per contestar al sentit de tot el que en la seva presència es digui, com poden fer-ho fins i tot els més estúpids d'entre els homes...”<sup>10</sup>.

Quan Turing va publicar els seus arguments a favor de la possibilitat que les màquines poguessin arribar a pensar, es va haver d'enfrontar a plantejaments teològics (Déu només va posar una ànima pensant en l'ésser humà); etnocentristes (l'ésser humà és superior a tot el conegut precisament gràcies a que és l'únic capaç de pensar); matemàtics (les màquines només poden raonar sobre continguts expressables matemàticament); filosòfic-deontològiques (només l'ésser humà té la facultat d'elaborar pensaments i raonaments relatius a aspectes com els sentiments, l'art, la moral,...); criticistes (les màquines només poden desenvolupar les seves respostes en base a un nombre limitat d'alternatives prèviament programades); educatius (una màquina no pot fer res realment nou ni aprendre dels seus errors).

Després de qüestionar cadascun dels posicionaments anteriors, Turing va arribar a la conclusió que no només podien pensar o arribar a fer-ho, sinó que era possible desenvolupar un instrument que permetés mesurar el grau d'“intel·ligència” desenvolupat per una màquina en un moment donat. Va sorgir així el test de Turing, utilitzat encara avui amb aquest

---

<sup>10</sup> Descartes va negar que qualsevol màquina pogués pensar, ser racional i intel·ligent, ja que un mecanisme no pot pensar per molt sofisticat que sigui, tal com es veu en: DESCARTES, R.: *Discurs del mètode*; traducció d'Arnau Gras, H.; ed. Alhambra, Madrid, 1987.

mateix objectiu. El test de Turing consisteix bàsicament en una sèrie de preguntes realitzades a una persona i a una màquina situades fora del camp de visió de l'examinador. Si aquest no pot diferenciar quan respon la màquina, o quan ho fa la persona, s'interpreta que la màquina ha raonat com la persona.

A Internet s'utilitzen programes basats en el test de Turing per detectar correus brossa (SPAM) els quals solen ser enviats directament per una màquina. Així igualment, per exemple, la prova Captcha, que consisteix en una sèrie de lletres i números presentats de manera distorsionada que l'usuari ha de repetir, també es basa en el test de Turing. La prova es basa en el supòsit que una màquina no podrà interpretar aquests caràcters, cosa que si poden fer els humans.

No obstant això, el test de Turing va ser superat per primera vegada el 2010 pel robot "Suzette", de Bruce Wilcox, el qual va ser el primer a guanyar el premi Loebner, organitzat anualment per a aquells que aconseguissin superar aquest test. Més recentment el test de Turing també va ser superat per "Eugene Goostman" un ordinador que va poder enganyar al 33% dels jutges al simular la intel·ligència d'un nen de 13 anys<sup>11</sup>.

Alguns autors qüestionen que aquests resultats demostrin que les màquines poden arribar a alguna cosa que puguem considerar intel·ligència. En aquest sentit els crítics asseguren que aquests resultats només demostren que les màquines poden imitar la intel·ligència humana, però no que puguin tenir intel·ligència per si

---

<sup>11</sup> Es considera superat el test de Turing quan la màquina aconsegueix enganyar almenys a un 30% dels jutges.

mateixes. De fet, els estudis actuals sobre Intel·ligència Artificial no es basen en tractar d'imitar la intel·ligència humana sinó en el desenvolupament d'aplicacions basades en les característiques dels sistemes artificials.

## Intel·ligència Artificial en dispositius automatitzats

A la pràctica, i seguint a Rusell i a Norving, podem classificar les diferents aplicacions de la Intel·ligència Artificial d'acord al seu objectiu. Així, podem referir-nos a sistemes l'objectiu dels quals és pensar com a humans, és a dir, raonar, prendre decisions, aprendre, resoldre problemes; sistemes que es pretén que actuïn com humans, o sigui, imitant el seu comportament; sistemes que es pretén que pensin racionalment, d'acord a plantejaments de lògica ideal; i sistemes que tenen com a objectiu actuar racionalment segons aquesta mateixa lògica ideal (Rusell & Norving, 2009). En tots aquests casos les aplicacions són diferents, però totes basades en el que podem anomenar Intel·ligència Artificial<sup>12</sup>.

Un exemple de l'aplicació de la Intel·ligència Artificial el constitueix el desenvolupament de sistemes basats en el Raonament Qualitatiu (QR) una branca de la Intel·ligència Artificial que automatitza el raonament

---

<sup>12</sup> Al definir que és la Intel·ligència Artificial, Russell i Norving recorren a quatre grans components: *Acting humanly*, *Thinking humanly*, *Thinking rationally*, *Acting rationally*. Així, inclouen sistemes com el Test de Turing en la categoria dels sistemes que tracten d'actuar com els humans; el model cognitiu que tracta de pensar com els humans; els sistemes que tracten de pensar racionalment, és a dir d'acord a les normes ideals de la lògica; i els sistemes que tracten d'actuar racionalment, d'acord amb aquestes mateixes normes ideals. Tots ells es basen en el que defineixen com Intel·ligència Artificial.

sobre el comportament dels sistemes físics mitjançant l'ús d'informació qualitativa més que quantitativa (Burrieza, 2013); la mineria de dades, estructurades o no estructurades, amb la qual s'intenta descobrir patrons en grans masses de dades (Hernandez 2004); la lògica computacional, des de la qual es busca la relació entre la lògica i el desenvolupament dels sistemes intel·ligents (Paniagua 2003); el processament del llenguatge natural, branca de la Intel·ligència Artificial que busca crear models computacionals per a la comprensió i comunicació home-ordinador per mitjà del llenguatge humà, utilitzada especialment per exemple per a la traducció automàtica entre llengües (Collobert 2011).

Podem incloure els principals estudis actuals que porten al desenvolupament de la computació quàntica, des de la qual es superen espectacularment les prestacions de la computació digital. Una de les característiques que més interès desperta entre els Governos és precisament la capacitat de la criptografia quàntica per xifrar i desxifrar missatges de forma segura, ja que les dades es codifiquen usualment en fotons, o partícules de llum, que no poden ser llegits sense ser destruïts. Aquests procediments són realitzats cada vegada més per les pròpies màquines (Teran, 2012).

Sistemes multiagent, visió artificial, robòtica,... són múltiples els camps que actualment s'estan desenvolupant a partir de la intel·ligència artificial. No obstant això, sense aprofundir en la discussió sobre què podem considerar intel·ligència o no, el cert és que a nivell pràctic cada vegada són més les situacions en què una màquina interacciona amb altres màquines prenent decisions i executant accions en què no intervé directament cap ésser humà.

## Màquines interaccionant amb màquines

Són múltiples els exemples que podem trobar actualment de màquines que interaccionen amb altres màquines sense intervenció directa de cap ésser humà. Dispositius intel·ligents que són capaços d'adaptar el seu comportament a les circumstàncies noves o canviants i que poden ser reprogramats per adaptar-se ràpidament a l'evolució de la societat i de la tecnologia.

Així es poden trobar electrodomèstics intel·ligents equipats amb connectivitat màquina a màquina<sup>13</sup>. Per exemple, hi ha neveres amb un sistema de gestió dels aliments que permet a l'usuari verificar els aliments emmagatzemats en el seu interior mitjançant un telèfon intel·ligent. D'aquesta manera es té accés a informació com el contingut, la data de caducitat dels aliments o veure recomanacions de plats que es poden cuinar amb els ingredients que es tenen en la nevera. Fins i tot existeixen ja neveres que, a més de complir amb tot l'anterior, ofereixen la possibilitat d'encarregar directament la compra d'aquells productes que es necessiten.

Un altre exemple es pot trobar en una indústria mil·lenària com és la de la producció de llet. Actualment aquest procés està totalment automatitzat, les vaques són munyides per robots mentre un programa subjacent llegeix les dades i els hi envia a l'agricultor mitjançant missatges de text al seu telèfon. D'aquesta manera l'agricultor obté la

---

<sup>13</sup> Alguns exemples d'aquest tipus de neveres són els models: Electrolux ScreenFridge; LG Digital Déu Refrigerator; LG GR-D267DTU; LG Smart ThinQ LFX31995ST; Samsung RH2777AT HomePAD Internet Refrigerator; Samsung Zipel e-Ciary; o, Whirlpool GD5VVAXT Refrigerator.



informació sobre quines vaques han estat munyides, la quantitat de llet que cada vaca està produint o quant es mou cadascuna, ja que una gran quantitat de moviment podria significar que aquesta vaca està en període de zel.

Hi ha altres serveis que es beneficien de les comunicacions màquina a màquina, tant en l'extracció de productes energètics, com el petroli i el gas, com en la facturació als clients. Els sensors remots poden detectar paràmetres importants en un lloc de perforació de petroli. Els sensors poden enviar informació sense fils a un ordinador amb els detalls específics sobre la pressió, cabal i les temperatures o fins i tot el nivell de combustible de l'equip. Així, l'ordinador pot ajustar automàticament l'equip per maximitzar l'eficiència.

Aquests avenços també s'utilitzen per a millorar el medi ambient, com per exemple a través de la utilització de mesuradors d'aigua intel·ligents. No es tracta només de poder facturar al client pel seu consum exacte sense que se l'hagi de molestar per visites a domicili per veure els comptadors, sinó que a part els clients reben alertes automàtiques en cas d'un consum anormal.

Aquesta tecnologia també aporta seguretat en el transport, ja que permet el seguiment de la flota que, juntament amb l'ús de serveis basats en localització com ara GPS, pot assenyalar les ubicacions dels vehicles en temps real i realitzar un seguiment dels llocs de recollida i lliurament dels béns. Això dona coneixement a l'instant sobre cada vehicle i el què aquest ha de fer. Així mateix permet l'assistència als conductors en cas de col·lisions o altres dificultats en el viatge. També pot servir per combatre el robatori. Per exemple, als Estats Units a finals

de 2007, aquesta tecnologia va ajudar a desarticular una banda que robava maquinària de construcció quan una empresa de lloguer va notar que els sensors dels seus equips mostraven que les excavadores estaven a gairebé 100 quilòmetres del lloc que tenien assignat. Com que es va observar que era una situació generalitzada, la companyia de lloguer va decidir desactivar a distància les excavadores mentre s'avisava a la policia, que varen aconseguir interceptar l'equip robat que es dirigia a la frontera amb Mèxic.

El control de trànsit és un altre entorn dinàmic que es beneficia de les comunicacions màquina a màquina. En un sistema típic, hi ha sensors que controlen variables com el volum de trànsit i velocitat. Els sensors envien aquesta informació als ordinadors que utilitzen programari especialitzat que controla els dispositius de control de trànsit, com els semàfors i els cartells informatius variables. Amb la utilització d'aquestes dades d'entrada, el programari manipula els dispositius de control de trànsit per maximitzar el flux circulatori.

Igualment l'àmbit de la salut s'ha vist revolucionat per la interacció màquina a màquina. Alguns pacients amb problemes cardíacs utilitzen monitors especials que recullen informació sobre la manera en què el seu cor està funcionant. Les dades s'envien automàticament als dispositius implantats, els quals produeixen una descàrrega elèctrica per corregir un ritme erràtic.

Un altre exemple el podem trobar en hospitals que, a part d'utilitzar sistemes de monitorització de pacients, creen unitats de cures intensives (UCI) a casa dels propis pacients. Un sistema de programari s'instal·la als sensors màquina a màquina de diversos dispositius mèdics,

com ara els que controlen la freqüència cardíaca o els monitors de signes vitals, que es troben a la capçalera del pacient. El sistema actua com un centre de control de trànsit aeri, de manera que els metges especialistes i les infermeres de cures intensives a l'hospital estan connectats en xarxa a diversos pacients de l'UCI, que estan tots allotjats a casa seva, a través de veu, vídeo bidireccional i dades. A través del sistema, aquests treballadors de la salut poden executar plans predefinits o intervenir en situacions d'emergència. La comunicació es torna més eficaç entre l'equip de l'hospital i l'equip a domicili i el temps entre la identificació del problema i la intervenció es redueix. D'aquesta manera es permet als pacients de l'UCI recuperar-se i ser controlats però en la comoditat i la familiaritat de la seva pròpia llar; i d'altra banda, els hospitals són capaços de processar més casos a través del sistema sense haver de posar més llits ni personal, el què comporta una millora en els costos dels hospitals.

En l'àmbit de l'entreteniment també s'ha pogut veure exemples on un simple concepte màquina a màquina s'ha convertit en art. Un exemple són els vestits i el vestuari que utilitza llums que s'encenen de manera automàtica sense fil per a que coincideixi amb la música i la coreografia<sup>14</sup>. Els artistes usen vestits lluminosos que es poden controlar sense necessitat de mantenir la pressió de botons i que es mouen en patrons a través del seu cos en sintonia amb l'entorn.

---

<sup>14</sup> Es pot trobar diversos exemples, com Black Eyed Peas, que va utilitzar aquest tipus de vestuari en la gira de 2011; o Illuminate, un grup de la sisena temporada de America 's Got Talent que actuava en la foscor i així es podien veure els llums intermitents que tots els ballarins portaven i amb diversos efectes sincronitzats.

En els exemples anteriors es pot veure la importància que està agafant la comunicació màquina a màquina, però si ens fixem en el camp de la robòtica es poden observar molts altres avenços. Hi ha robots que són usats en entorns perillosos per a l'home (com en accidents nuclears, en la desactivació de bombes o per netejar camps minats, en la recerca i neteja en casos de desastres naturals). En moltes ocasions la utilització de robots respon a criteris exclusivament econòmics, doncs en general el seu ús resulta molt més rendible que fer les mateixes tasques per éssers humans (com en l'agricultura en què s'usen robots per substituir les grans màquines usades per excavar, fer la collita i d'altres activitats similars). Tanmateix, els motius més freqüents per a la utilització de robots, o màquines dotades d'intel·ligència artificial, estan més vinculats a una més gran eficiència per part d'aquests.

També s'usen en el transport, des d'helicòpters autònoms fins cadires de rodes automàtiques i fins i tot portadors de càrrega, fins els drones (vehicles autònoms usats freqüentment per a finalitats militars). Igualment són útils per a l'exploració de llocs inaccessibles com poden ser els volcans o en les expedicions a Mart.

En l'àmbit de la salut també s'utilitzen robots per ajudar en operacions d'alt risc, per ajudar a persones grans com caminadors robòtics o aparells que recorden quan prendre la medicació. Finalment, a la llar també han aparegut robots que fan tasques com la de tallar la gespa o netejar la casa.

Aquesta evolució de la intel·ligència artificial, aplicada als més variats dispositius, comporta una reflexió sobre les implicacions que la seva generalització pot tenir sobre el concepte de responsabilitat. Molt

especialment s'ha de considerar la interpretació que el legislador i la jurisprudència estiguin fent d'aquesta responsabilitat, especialment davant les conseqüències de les accions realitzades per màquines dissenyades per actuar de manera autònoma, i sense la intervenció directa de cap ésser humà.



## **Capítol segon: Construcció social del concepte de responsabilitat**

---

### **Responsabilitat i responsabilitat indirecta**

Etimològicament la paraula responsabilitat deriva del llatí 'responsum', és a dir, respondre per algú. Actualment quan utilitzem el terme "responsable" pretenem indicar que algú està subjecte a respondre dels seus actes o, fins i tot, els d'un altre<sup>15</sup>. Es tracta d'una obligació legal o moral. Implica per tant una atribució d'obligacions derivades dels propis actes o dels que s'espera de la persona que compleix un determinat paper.

La responsabilitat comporta un valor moral que condiona els nostres actes i les seves conseqüències. En el moment en que entre les diferents accions o omissions possibles optem per un comportament determinat passem automàticament a ser responsables de les conseqüències que d'aquest comportament es deriven.

Podem analitzar la responsabilitat com a valor des d'una perspectiva sociològica, filosòfica, o fins i tot religiosa, però no obstant això, és la

---

<sup>15</sup> D'acord amb el diccionari de la Reial Acadèmia Espanyola de la Llengua el terme responsable deriva del llatí responsum, supí de respondere, (respondre) Es refereix a qui està obligat a respondre d'alguna cosa o per algú. El Gran Diccionari de la Llengua Catalana, el defineix al seu torn com aquell "Obligat a respondre dels seus actes, a respondre d'una cosa".

perspectiva legal la que defineix el marc concret en què podem exigir l'assumpció de responsabilitat, fins i tot penal, pels nostres actes o omissions. Des d'aquesta perspectiva legal, la responsabilitat es vincula a aquells actes o omissions que conscientment provoquen directament o indirectament un fet amb rellevància jurídica. Tal com indica Aramayo:

"... Les conseqüències d'un acte, tot i que puguin tenir un caràcter fortuït i absolutament mancat d'intenció, sempre generen una o altra classe de responsabilitat, ja ho sigui d'índole moral, política o juridicopenal, tenint en compte que algú ha de respondre del dany causat i això ha de ser així, encara que les conseqüències de les nostres accions estiguin subjectes al concurs de l'atzar i no depenguin únicament de nosaltres..." (Aramayo, 2012).

A diferència de la responsabilitat objectiva derivada dels propis actes, quan es tracta de fets realitzats per altres persones sobre les que hi ha obligació de custòdia, o control, també existeix responsabilitat, encara que de caràcter subjectiu. Es tracta d'una responsabilitat indirecta, també anomenada responsabilitat per fet d'un altre. Un exemple clàssic seria la responsabilitat de pares i tutors pels fets realitzats pels seus fills o pels menors o incapacitats situats sota la seva tutoria. L'article 1903 del Codi Civil recull aquesta responsabilitat<sup>16</sup>.

---

<sup>16</sup> "L'obligació que imposa l'article anterior és exigible, no només pels actes o omissions propis, sinó pels d'aquelles persones de qui s'ha de respondre. Els pares són responsables dels danys causats pels fills que estiguin sota la seva guarda. Els tutors ho són dels perjudicis causats pels menors o incapacitats que estan sota la seva autoritat i habiten en la seva companyia. Ho són igualment els amos o directors d'un establiment o empresa respecte dels perjudicis causats pels seus dependents en el servei dels rams en què els tinguessin empleats, o en ocasió de les seves funcions. Les persones o entitats que siguin titulars d'un Centre docent



La responsabilitat de la qual parla el Codi Civil, es fonamenta doncs, en l'obligació d'emprar tota la diligència possible per prevenir el dany que puguin provocar aquells dels que s'ha de respondre, com seria el cas dels empresaris pels danys causats pels seus dependents en exercir les seves funcions. Es tracta de responsabilitat per *culpa in vigilando*.

Encara podem anar a l'analogia per aplicar a altres àmbits de responsabilitat, en realitat s'ha d'aplicar amb molt de compte aquesta analogia en parlar d'aquest tema. En el Dret Penal l'analogia "*in malam partem*" està expressament prohibida, admetent només en algun cas excepcional, com pot ser el cas dels atenuants per analogia de l'article 21.7 del Codi Penal, i encara en aquest cas només en casos ben fonamentats. No es pot oblidar que "... Les lleis penals no s'aplicaran a casos diferents dels compresos expressament en elles..."<sup>17</sup>.

La jurisprudència en l'àmbit penal és doncs molt acurada en tractar el tema de l'analogia en definir la responsabilitat, de manera que la doctrina s'aplica en aquests casos de manera que es persegueixi successivament als autors materials del fet, d'acord amb la responsabilitat concreta que es derivi en cada cas de les accions o omissions realitzades per cadascun.

---

d'ensenyament no superior respondran pels danys i perjudicis que causin els seus alumnes menors d'edat durant els períodes de temps en què els mateixos es trobin sota el control o vigilància del professorat del Centre, desenvolupant activitats escolars o extraescolars i complementàries. La responsabilitat de què tracta aquest article cessa quan les persones que s'hi esmenten proven que van emprar tota la diligència d'un bon pare de família per prevenir el dany" (Article 1903 del Codi Civil, aprovat per Reial Decret de 24 de juliol de 1889).

<sup>17</sup> Article 4.1 del Codi Penal, aprovat per la Llei Orgànica 10/1995, de 23 de novembre.

En tractar, per exemple, de la responsabilitat penal per danys produïts per objectes inanimats no es pot acudir sistemàticament a l'analogia. Les pròpies característiques del medi, faciliten l'anonimat, la suplantació de personalitat, la indefinició territorial, la multiplicitat d'actors, ... pel que el legislador primer, i la jurisprudència després, ha de definir de manera concreta i objectiva els nivells de responsabilitat en cada cas. No obstant això, en l'àmbit no estrictament penal, sí que és possible acudir a l'analogia per discernir la responsabilitat indirecta per aquests danys produïts per objectes inanimats.

## **Responsabilitat d'animals i objectes inanimats**

L'article 1905 del Codi Civil especifica que: "El posseïdor d'un animal, o el que se serveix d'ell, és responsable dels perjudicis que causi, encara que se li escapi o extravii". Es tracta d'una responsabilitat vinculada a l'obligació de supervisar i prendre les mesures oportunes per evitar que les accions provocades per animals o objectes inanimats, que en principi no són susceptibles de ser responsables, provoquin danys a uns altres. Això és així, atès que no existeix en l'actualitat un fonament filosòfic consolidat que sostingui l'atribució de responsabilitat als animals i als objectes inanimats.

No obstant això, al llarg de la història podem trobar diversos exemples de responsabilització d'animals, o fins i tot d'objectes inanimats, pels danys que han provocat. Un exemple de responsabilització als objectes o animals que causin un dany, el podem trobar a les lleis de Dracon<sup>18</sup>. Ja

---

<sup>18</sup> Legislador d'Atenes en el s. VII A.C.

en 1836 Filangieri en el seu "Ciència de la legislació" se sorprèn que una de les lleis de Dracon, ratificada després per Soló i per Suidas, condemnava a mort al cavall o un altre animal que hagi causat algun mal, i cita Pausanias que feia extensible aquesta responsabilitat a les coses inanimades:

"... Pausanias refereix que s'estenia aquesta llei a les coses inanimades; de manera que si en caure una estàtua, un atuell, columna, etc. mataven o ferien un home que les estava observant o passava per sota d'elles, es formava immediatament un procés, i l'estàtua, la columna o l'atuell que havien causat el dany, eren condemnades a ser fetes trossos..." (Filangeri, 1836, pp. 277).

Aquesta sorpresa de Filangieri és raonable ja que el dret romà consagrava una divisió tripartida entre coses, animals i persones, i només s'atribuïa finalitats i racionalitat a la condició de persona i, per tant, només ella podia ser subjecte de responsabilitat.

En la mateixa obra Filangieri crida l'atenció sobre el fet que el mateix Plató no veiés l'absurditat de processar i condemnar un cavall homicida, o una cosa inanimada, i que instruís als jutges sobre la condemna a mort que s'ha d'imposar a una bèstia de càrrega o un altre animal que hagi mort un home, o si s'escau la destrucció d'objectes<sup>19</sup>.

---

<sup>19</sup> *Si jumentum, aut aliud animal, hominem interficiat, nisi publico in certamine id fecerit, interfecti hominis propinqui id iudicibus deferant; et agrorum curatores illi, quibus, quotque propinquus ipse mandavit, iudicent, et damnatum jumentum extra regionis fines interficiant. Quod si quid inanime, praeter fulmen aut aliud telum divinitus missum, anima hominem cadentem ipsum. Aut ipsum cadens, privaverit genere propinquis interfecto, proximum in vicinia ad hoc; constituat iudicem; atque hoc et coetera, prout erga mortuum ipsum*

La sorpresa que expressa Filangeri es deu sobretot al fet que, en la tradició greco-llatina, els instruments no es consideren subjectes de responsabilitat. Aristoteles, per exemple, només atribuïa responsabilitat a l'ésser humà racional i lliure. L'esclau era des de la seva perspectiva un "instrument vocale" i per tant no responsable, els animals eren "instrument semivocale" i els objectes només simples instruments. Cap d'aquests casos era doncs susceptible de responsabilitat, ja que, seguint Jordi Mundó, la responsabilitat depèn de dues variables: l'autonomia i la intencionalitat<sup>20</sup>.

## Influències culturals enfront de la responsabilitat

Des d'una perspectiva religiosa, les tres religions anomenades "del llibre": catòlica, jueva i musulmana, atribueixen en exclusiva a l'ésser humà el lliure albir, i amb això la responsabilitat per les seves accions. Per al catolicisme només la persona està dotada d'ànima i amb lliure albir per superar el pecat original i per escollir el camí del bé o del mal. Déu pot estar en les coses inanimades, però només Ell té autonomia i, per tant, és l'únic responsable de les possibles fets succeïts.

En l'islam, no s'accepta la idea de pecat original, ja que només l'home és responsable individualment dels seus actes. L'atribució de responsabilitat a les coses inanimades no és des d'aquesta perspectiva

---

*convenit, pro sui ipsius, et cognationis totius expiatione perficiat. Quod vero damnatum fuerit, ut de animalibus dictum est, exterminetur* (Platon de Legib. Dial. IX) citat per Filangeri en el seu "Ciencia de la Legislación".

<sup>20</sup> Es recullen aquí els plantejaments sobre la responsabilitat en Aristoteles, així com en la Escolàstica, del Doctor Jordi Mundó Blanch, citat pel Doctor Juli Sabaté Delgado.

majoritàriament assumible. Tampoc el judaisme l'admet, ja que Jahvè va crear l'home lliure per fer el bé o el mal.

A vegades també s'han donat interpretacions religioses que atribueixen una certa responsabilitat també als objectes inanimats. Així, Sheikh al-Uzaymín, en explicar la Surah al-Ahzab 33:72 als què es pregunten com pot atribuir responsabilitat als cels, la terra i les muntanyes quan aquests són inanimats, i no tenen intel·lecte o sentiments, els respon: "D'acord amb Al·là tot objecte inanimat té un intel·lecte que entén i segueix un mandat"<sup>21</sup>.

No obstant això, malgrat tot podem trobar casos d'atribució de responsabilitat a animals o objectes inanimats. Filangieri, cita alguns d'aquests casos, com ara el d'un porc penjat solemnement durant el regnat de Lluís IX, per haver matat un noi, o el d'uns gossos jutjats i condemnats a Itàlia per seguir els seus instints naturals (Filangieri, 1836). Són nombrosos els casos que podem trobar al llarg de la història de condemnes, en ocasions oficials i en altres de fet, a animals o coses inanimades per danys causats a les persones. Hi ha en tot això un cert animisme latent, doncs per a un genet caigut sempre resulta més gratificant responsabilitzar al cavall que l'ha tirat que a la seva pròpia falta de perícia.

De fet, des de corrents mecanicistes, s'ha mantingut tradicionalment un cert escepticisme sobre l'existència o no del lliure albir defensat per les principals religions. Si es concep l'ésser humà com una simple

---

<sup>21</sup> "Vam proposar el dipòsit (la responsabilitat) als cels, a la terra i a les muntanyes, però es van negar a fer-se càrrec d'ell, van tenir por. L'home, en canvi, es va fer càrrec. És, certament, molt impiu, molt ignorant" (Surah al-Ahzab 33: 72).

màquina biològica composta de molècules agrupades en cèl·lules, neurones, gens o sistemes, és discutible la possibilitat real de prendre decisions que realment canviïn les respostes programades en l'organisme.

No obstant això, Shaun Nichols, a l'analitzar un estudi de Kathleen Vohs i Jonathan Schooler, va trobar que en totes les cultures hi ha persones deterministes que neguen el lliure albir, però curiosament aquestes persones escèptiques també atribueixen responsabilitat moral a les accions humanes:

"... En totes les cultures, es van trobar que la majoria de la gent va dir que el nostre univers no és determinista i també que la gent en l'univers determinista no són responsables de les seves accions. Encara que això no és particularment sorprenent -la gent vol creure que té lliure albir- sorgeix alguna cosa interessant quan ens fixem en el grup més petit de persones que diuen que el nostre univers és determinista. A través de totes les cultures, aquesta minoria substancial dels escèptics del lliure albir també eren molt més propensos a dir que les persones són responsables, encara que el determinisme és veritable. Una manera d'interpretar aquesta troballa és que si s'arriba a creure en el determinisme, no per això s'abandonen les actituds morals. Més aviat, simplement es demostra errònia l'opinió que el determinisme exclou la responsabilitat moral..." (Nichols, 2008).

És cridanera l'aparent contradicció entre el determinisme, és a dir, el negacionisme respecte al lliure albir, i la generalitzada acceptació de la

responsabilitat moral per les accions humanes. Es reconeix doncs l'existència de responsabilitat moral amb independència que es consideri l'ésser humà com una simple màquina biològica, o com un ésser més complex. La clau estaria doncs en l'existència d'un sistema de valors, la capacitat de diferenciar entre accions bones i dolentes, la decisió d'actuar d'una manera o d'una altra, i la de preveure les conseqüències d'aquestes accions.

En realitat des d'una perspectiva jurídica, la responsabilitat subjectiva està vinculada a l'existència d'una obligació de vigilància, supervisió, control o similar respecte a la persona, animal o objecte causant del dany. El fonament és la presumpció que aquests no estan en condicions de garantir que posseeixen un sistema de valors socialment acceptats; que saben diferenciar entre accions bones i dolentes; i que són capaços d'adoptar decisions adequades i de preveure les conseqüències que tindran aquestes accions.

## **La responsabilitat en les noves tecnologies**

En els inicis d'Internet el Dret es centrava específicament en aquelles conductes que puguin perjudicar els sistemes informàtics i les dades tractades des d'aquests sistemes<sup>22</sup>. Aquest criteri és avui més ampli, de manera que no es vincula exclusivament a aquelles accions que perjudiquin els sistemes o les dades, sinó que es vincula amb les accions realitzades en el passat i en com van ser realitzades. Així, el

---

<sup>22</sup> Pifarré, Maria Jose, "Internet y redes sociales: Un nuevo contexto para el delito". Revista d'Internet, Dret i Política N° 16 (Universitat Oberta de Catalunya) Barcelona 2013.

Grup de Protecció de Dades de l'article 29<sup>23</sup>, defineix la responsabilitat en informàtica com:

"... En informàtica, la responsabilitat es pot definir com la capacitat de determinar el que va fer una entitat en un moment determinat en el passat i de quina manera ho va fer. En l'àmbit de la protecció de dades, aquest concepte té sovint un sentit més ampli i descriu la capacitat de les parts per demostrar que van prendre les mesures adequades per garantir l'aplicació dels principis de protecció de dades.

La responsabilitat en informàtica és especialment important per investigar violacions de dades personals, en les quals els clients, proveïdors i el sotsencarregat del tractament poden tenir cadascun algun grau de responsabilitat operativa. La capacitat de la plataforma en el núvol per proporcionar mecanismes de registre amplis i un control fiable és de vital importància per aconseguir-ho..."<sup>24</sup>.

L'esmentat Grup de Protecció de Dades de l'Article 29, introdueix entre les seves propostes "l'obligació legal per al responsable del tractament de les dades, d'aplicar les mesures tècniques i d'organització adequades". En el cas que un encarregat del tractament d'aquestes mateixes dades, no s'atengui a les instruccions de l'esmentat

---

<sup>23</sup> Aquest Grup de treball va ser creat per l'article 29 de la Directiva 95/46/CE del Parlament Europeu i del Consell. Es tracta d'un òrgan europeu consultiu en matèria de protecció de dades i privacitat. Les seves funcions es descriuen en l'article 30 d'aquesta mateixa Directiva 95/46/CE i en l'article 15 de la Directiva 2002/58/CE.

<sup>24</sup> Dictamen 05/2012 del Grup de Protecció de Dades de l'Article 29, sobre la computació en núvol, adoptat l'1 de juliol de 2012.



responsable del tractament serà considerat ell mateix com a responsable del tractament.

En referir-nos a la responsabilitat en les noves tecnologies de la comunicació, sorgeix immediatament el fet, cada vegada més freqüent, de les accions automatitzades, i molt especialment les produïdes a partir de sistemes dotats d'Intel·ligència Artificial. L'absència de qualsevol ésser humà en el moment de produir-se l'acció automatitzada, podria aparentment posar en qüestió l'existència de responsabilitat en no existir culpa. No obstant això, tal com indica Roca Trias, no n'hi ha prou amb l'absència de culpa perquè algú pugui quedar exonerat de responsabilitat:

"... Al que s'ha exposat cal afegir, seguint la sentència de 23 de gener de 1998, parcialment transcrita en les SSTS de 9 d'octubre de 2009, Rec 5285/2005, i de 23 d'octubre de 2013, Rec 1067/2006, que *«encara que la culpabilitat de la conducta també ha de ser objecte de prova, s'ha de considerar en ordre a l'assumpció de la corresponent càrrega, que ordinàriament els elements volitius i cognoscitius necessaris per apreciar aquella formen part de la conducta típica provada, i que la seva exclusió requereix que s'acrediti l'absència d'aquests elements, o en la seva vessant normativa, que s'ha emprat la diligència que era exigible per qui addueix la seva inexistència; no n'hi ha prou, en definitiva, per l'exculpació davant d'un comportament típicament antijurídic la invocació de l'absència de culpa»...*" (Roca, 2009).

La possibilitat que no estigui llunyà el dia en què sistemes automatitzats dotats d'Intel·ligència Artificial puguin valorar la situació, prendre decisions i executar accions de manera molt més àgil i eficient del que puguin fer-ho els éssers humans, fa que s'hagi de replantejar el tema de la responsabilitat.

La forta progressió produïda en els últims temps en aquest tipus de sistemes fa que sorgeixin algunes veus que auguren pròxim el moment en què amb prou feines hi hagi diferència, a efectes de la responsabilitat, entre els éssers humans i els mecanismes dotats d'Intel·ligència Artificial.

Així, alguns autors, partint dels principis de les ciències cognitives, sostenen que si s'arriba a una profunda intel·ligència artificial, és a dir, que les màquines arribin a assolir la capacitat de ser "intencionals" se'ls podria atribuir responsabilitat (Rodríguez, 1996). Aquest plantejament parteix del supòsit de que aquesta intencionalitat de les màquines es basa en un principi fonamental en les ciències cognitives, és a dir, que els mecanismes de cognició i els processos de pensament associats desenvolupats per la màquina siguin similars o superiors als dels éssers humans. En aquests processos cognitius s'inclouen aspectes com memòria, atenció, intel·ligència, percepció, emoció i capacitat d'aprenentatge.

No obstant això, en el cas dels danys produïts per aquests sistemes podríem aplicar, per analogia, els mateixos criteris que en el cas de la responsabilitat per danys produïts per animals, o els que poguessin provocar persones dependents de pares, o tutors i altres casos similars. Tanmateix, es fa necessari analitzar com va evolucionant el marc

legislatiu i jurisprudencial en relació a la responsabilitat en els casos en què només actuen sistemes dotats d'Intel·ligència Artificial, sense intervenció directa de cap ésser humà en aquesta actuació de la màquina.



## **Capítol tercer: Internet: una xarxa de xarxes**

---

### **El ciberespai, una nova realitat virtual**

La constant evolució de les tecnologies de la informació i la comunicació (TIC) obliga a una permanent adaptació dels sistemes legals i jurisprudencials a les peculiaritats d'aquest nou espai de l'activitat humana. Els estats legislen sobre aquesta nova realitat social amb la finalitat, teòricament, d'establir normes de conducta a la xarxa i amb l'objectiu de garantir la convivència i el benestar social. Així, la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic, planteja normativament aquests serveis en l'Estat Espanyol, desenvolupant la Directiva 2000/31/CE, de 8 de juny, del Parlament Europeu i del Consell.

Internet apareix com una conseqüència de la xarxa Arpanet, creada el 1969 pel Departament de Defensa dels Estats Units. Es tractava d'una nova eina per connectar els seus ordinadors, ubicats en diferents espais físics, amb els de les universitats i centres d'investigació que estaven desenvolupant programes vinculats o d'interès per al Pentàgon. No obstant això, molt ràpidament es va començar a generalitzar el seu ús i a mitjans dels anys vuitanta ja es pot parlar pròpiament d'Internet com una xarxa de xarxes universal, que permet l'intercanvi d'informació entre usuaris de tot el món.

Internet és, en definitiva, una xarxa d'ordinadors, els quals estan interconnectats formant una xarxa de xarxes, composta per multitud d'usuaris independents. Aquests usuaris utilitzen els serveis de proveïdors que permeten la transmissió de dades a través de nodes al llarg de la xarxa. És a dir, a través d'una xarxa d'ordinadors, els usuaris poden interconnectar entre ells, independentment d'on estiguin ubicats els seus ordinadors, o quins programes o sistemes utilitzin, gràcies a aquesta configuració en forma de xarxa de xarxes, característica d'Internet.

Cada dispositiu final està físicament connectat a internet utilitzant un primer encaminador, generalment conegut per la seva denominació en anglès, *router*, i per mitjà d'una xarxa d'accés. Aquesta xarxa està connectada a la malla de commutadors, de paquets i d'enllaços que interconnecta els dispositius finals d'internet mitjançant una xarxa que s'anomena *Network Core*. El lloc on arriba cada xarxa d'accés (el primer encaminador) és on comença el *Network Core*, per tant, la unió del *Network Core* i les diferents xarxes d'accés és el que configura pròpiament Internet.

La informació està agrupada per cada dispositiu en paquets i enviada a internet. Els commutadors de paquets poden utilitzar diferents tècniques per enviar-los a través de la xarxa. Els més freqüents són el de tallar-continuar (*cut-through*) i el d'emmagatzemar-transmetre (*store-and-forward*).

En tallar-continuar, el commutador rep la primera part del paquet on hi ha l'adreça de destinació, i després de decidir si ha de ser reenviat o filtrat, inicia la seva transmissió, encara que no hagi estat rebut en la

seva totalitat. Mitjançant emmagatzemar-transmetre, la font envia un paquet al commutador de paquets, el qual els va emmagatzemant fins que ha acabat d'arribar totalment. Un cop tot el paquet està en el commutador aquest el reenvia i, en cas que hi hagi més paquets, la font comença a enviar el següent.

Per Moncada Flórez la xarxa representa "una societat virtual de comunicació, permet a qualsevol persona accedir i integrar-s'hi i participar del més ràpid i complex intercanvi d'informació en forma digital, col·locant als Estats en l'obligació d'establir normes de conducta que orientin l'actuació a la xarxa, afavorint la recerca del benestar social" (Moncada, 2009 Pag.1).

Encara que l'aspecte més conegut d'internet és la possibilitat de navegar a través de la *World Wide Web*, són molts els diferents serveis als quals avui es pot accedir a través del ciberespai. Alguns dels quals són els següents:

Correu electrònic	correu electrònic	Missatges i documents enviats a altres usuaris
Llistes de distribució	<i>LD</i>	Missatges enviats mitjançant correu electrònic a una llista preestablerta d'usuaris
Grup de notícies	<i>Newsgroup</i>	Missatges enviats a una base de dades, que és al seu torn consultable per altres usuaris
FTP	<i>File Transfer Protocol</i>	Enviament i recepció d'arxius entre ordinadors
Xat	<i>Internet Relay Chat</i>	Comunicació entre usuaris. Permet les videoconferències, les trucades telefòniques o també la missatgeria instantània.

WWW	<i>World Wide Web</i>	Accés a documents multimèdia publicats majoritàriament en forma de pàgines web
P2P	Punt a Punt	Intercanvi directe d'informació entre usuaris
Bitacores	<i>weblogs</i>	Difusió de notes, opinions i articles sobre els diferents temes de debat presentats
Xarxes socials	<i>Social Networking</i>	Comunicació entre grups de persones per afinitat d'interessos, amistat o qualsevol altre motiu

Una de les característiques del ciberespai és que no té un únic centre de control que permeti dirigir i controlar tota la informació que circula per aquest espai. Els milions d'usuaris poden comunicar-se entre si de manera dinàmica i altament descentralitzada. L'única limitació és el diferent accés que pugui tenir cada usuari a un node de comunicacions, el que usualment es realitza a través d'un servidor.

Per tal que sigui possible la comunicació entre ordinadors, cal que utilitzin un llenguatge que tothom pugui interpretar, aquesta funció la realitzen els protocols. Un protocol no és més que un conjunt de regles establertes perquè els diferents paquets d'informació que un ordinador concret envia a la xarxa puguin ser acoblats i interpretats correctament per l'ordinador que rep aquesta informació.

Un altre element fonamental per poder establir la comunicació és la identificació de cada ordinador que accedeix a la xarxa, ja que si no estigués identificat els protocols sols no podrien redirigir els paquets d'informació a l'ordinador concret que els va sol·licitar. Actualment s'identifica cada ordinador mitjançant una adreça IP que no és més que un grup de nombres únic per a cada ordinador situat en una mateixa



xarxa. Per tal de facilitar la gestió de les adreces IP es van desenvolupar els noms de domini (DNS, *Domain Name System*) que no és més que un servei que tradueix els noms a adreces IP.

Un altre servei que agilitza les comunicacions i facilita la navegació per la Web, són els anomenats Punts Neutres. Un punt neutre d'accés a internet és un punt de trobada on múltiples proveïdors d'internet poden enllaçar. D'aquesta manera els proveïdors d'internet regional o d'accés poden evitar un excés de trànsit amb els proveïdors d'internet globals.

Així, per exemple, a Catalunya, el punt neutre d'Internet és el CATNIX<sup>25</sup> que va néixer com una iniciativa conjunta del Govern de la Generalitat i Localret, i es troba dins de les instal·lacions del Centre de Serveis Universitaris de Catalunya (CSUC). El CATNIX ofereix un ampli ventall de serveis als usuaris<sup>26</sup>.

---

<sup>25</sup> El CATNIX té una infraestructura que consisteix en dos commutadors Cisco Catalyst 4507R-E, connectats amb un enllaç de 2 Gbps cadascun d'ells, instal·lat en un dels dos emplaçaments del CATNIX (Campus Nord - CSUC-CN i Telvent - CSUC-T ), a on es connecten els equips de les institucions que hi pertanyen, tal i com s'indica a: <http://www.catnix.net/ca/infraestructura/>

<sup>26</sup> Els serveis oferts per CATNIX als seus usuaris són, entre altres, els següents: a) Possibilitat de fer intercanvis privats a més a més de l'intercanvi amb el comú del punt neutre, el multicast; b) Intercanvi de trànsit Ipv6; c) Rèpliques del .com i .net; un servei per atendre les incidències 24 hores al dia els 7 dies de la setmana; d) Test de velocitat; e) Gestió fora de banda, el que permet fer un primer diagnòstic ràpid en cas de problemes a la xarxa o al encaminador de l'entitat; f) Seguiment de problemes d'encaminament mitjançant una eina anomenada looking glass que és una eina que ajuda al seguiment de problemes d'encaminament; g) Servidor de temps NTP amb el qual poder sincronitzar els equips; h) Servidor IXP-Watch que permet detectar el tràfic potencialment perillós; i) Servidor de prefixos bogon que serveix per evitar l'adreçament a nivell global i evitar així atacs de denegació de servei; j) Servidor arrel de noms F que permet augmentar el temps de resposta en les consultes al servidor de noms i incrementar la seguretat; k) Servidor arrel de noms J que, igual que el servidor arrel de noms F, permet augmentar el temps de resposta en les consultes al servidor de noms i incrementar la

Els punts neutres d'accés a internet constitueixen una eina que facilita la navegació, però alhora poden facilitar atacs i problemes de seguretat. És per això que gran part dels seus recursos estan centrats en mantenir la seguretat davant d'atacs externs.

## **Les arquitectures: del web 1.0 a la 2.0**

L'arquitectura Client/Servidor es basa en la relació entre un ordinador actuant com a servidor, és a dir, qui ofereix un recurs i una altra que actua com a client, és a dir, la que sol·licita aquest recurs. En aquest cas, qualsevol client que vulgui accedir a un recurs ubicat en un servidor concret, cal que connecti amb aquest servidor i aquest ha d'estar configurat i disponible per poder respondre a les demandes que se li facin per part del client. Es tracta d'una relació unidireccional, en què una part disposa del recurs, és a dir, la pàgina web, les dades, o qualsevol recurs similar, mentre que l'altra part només pot accedir a aquest recurs.

En els inicis d'internet, el que avui coneixem com a Web 1.0, només permetia a l'usuari accedir a les informacions que cada proveïdor de continguts havia editat en una pàgina web, generalment utilitzant tecnologies html. No hi havia interacció, de manera que es tractava d'una relació passiva que, en el cas del comerç electrònic, es diferenciava poc de la tradicional venda a distància mitjançant catàleg, ja que en realitat funcionava més aviat com un aparador on mostrar els productes als potencials compradors.

---

seguretat; l) Servidor arrel de noms L que, igual que el servidor arrel de noms F i el servidor arrel de noms J, permet augmentar el temps de resposta en les consultes al servidor de noms i incrementar la seguretat.

El desenvolupament de la web 1.5 va representar la introducció d'un cert dinamisme en els documents incorporats a les pàgines web i permetre que les pàgines de comerç electrònic oferissin als usuaris la possibilitat de l'autoservei en línia. No obstant això, no va ser fins al desenvolupament de noves tecnologies que a la pràctica es va possibilitar la plena interacció entre els usuaris.

Avui la web permet aquesta interacció entre usuaris, en el que es denomina Web 2.0. Des d'aquesta perspectiva, els usuaris tenen la possibilitat d'interactuar i compartir informació entre ells, tot i que cal que es classifiquin mitjançant etiquetes els continguts en un llenguatge accessible.

A la Web 2.0 els usuaris han d'explicitar les seves demandes, és a dir, a quines informacions volen accedir o compartir, mentre que per la seva banda els proveïdors de continguts han d'etiquetar cadascun dels continguts de manera que es defineixi adequadament el tema que tracten.

De fet, en el que es coneix com la Web 2.0, els usuaris es converteixen freqüentment ells mateixos en indexadors de la informació. I ho fan en relacionar aquestes informacions amb paraules clau o marques (*tags*) que ells mateixos trien lliurement d'entre les diferents possibilitats existents<sup>27</sup>.

Aquesta indexació és possible perquè la Web 2.0 es sustenta en bases de dades que poden ser modificades per l'usuari. En aquest sentit, són

---

<sup>27</sup> Ribes, Xavier. "La Web 2.0. "El valor de los metadatos y de la inteligencia colectiva" Telos. Cuadernos de Comunicación, Tecnología y Sociedad. Nº 73, (Fundación Telefónica, diciembre 2007).

diverses les definicions que diferents autors utilitzen per definir la Web 2.0, però en general s'accepta la utilització de bases de dades modificables com una de les principals característiques de la Web 2.0. Així, Xavier Ribes utilitza per referir-se a la Web 2.0, la definició donada per l'Institut Nacional de Tecnologies Educatives i de Formació del Professorat, (INTEF) del Ministeri d'Educació Cultura i Esport, en el qual es defineix com a Web 2.0:

"... Totes aquelles utilitats i serveis d'Internet que se sustenten en una base de dades, la qual pot ser modificada pels usuaris del servei, ja sigui en el seu contingut (afegint, canviant o esborrant informació o associant dades a la informació existent), doncs bé en la forma de presentar-los, o en contingut i forma simultàniament..."<sup>28</sup>.

L'esmentat Institut Nacional de Tecnologies Educatives i de Formació del Professorat, recull alguns dels exemples més característics de la Web 2.0 en els quals es pot apreciar com la interacció entre els usuaris i els proveïdors de continguts, o entre els mateixos usuaris entre si, constitueixen l'element diferenciador de la Web 2.0 respecte a altres versions de la web<sup>29</sup>:

- **Blocs:** Proporcionen un sistema fàcil i assequible de publicar a Internet a títol individual o col·lectiu.

---

<sup>28</sup> Pot consultar-se a [http://www.ite.educacion.es/formacion/materiales/155/cd/modulo\\_1\\_Iniciacionblog/qu\\_es\\_la\\_web\\_20.html](http://www.ite.educacion.es/formacion/materiales/155/cd/modulo_1_Iniciacionblog/qu_es_la_web_20.html).

<sup>29</sup> Fernando Posada Prieto et al. "Multimèdia i web 2.0" Instituto Nacional de Tecnología Educativas y de Formación del Profesorado Febrer 2012.

- **Wikis:** Permet crear la documentació d'un projecte de forma col·laborativa: glossaris, enciclopèdies, manuals, etc.
- **Gestors CMS:** (Sistema de Gestió de Continguts) Permeten la publicació col·laborativa (rols) en línia de les notícies que afecten a una comunitat.
- **Plataformes d'e-learning:** (Sistemes de Gestió de l'Aprenentatge) S'utilitzen per crear diferents entorns d'e-learning.
- **Imatges:** Permeten l'allotjament en línia d'imatges i després la seva posterior utilització en altres serveis o recursos.
- **Podcasts:** Permeten l'emmagatzematge i difusió d'àudios.
- **Google Maps:** Permet la localització geogràfica d'imatges, textos, enllaços, vídeos o documents.
- **Repositoris de vídeos:** Proporcionen suport d'emmagatzematge de vídeos, així com la seva difusió en *streaming* facilitant la seva correcta visualització.
- **Ofimàtica en línia:** Permet d'una banda la creació i publicació compartida de documents de text, presentacions i fulls de càlcul i per una altra la comunicació en temps real (missatgeria instantània) o diferit (correus electrònics).
- **Presentacions:** Permet el disseny i publicació a la web de presentacions de diapositives, fotografies, de documents etc. que després s'insereixen en blogs, wikis i altres recursos similars.

- **Marcadors socials:** Permet disposar en línia dels marcadors o llocs web favorits i compartir aquestes adreces amb els altres.

## Web 3.0: un espai per a màquines intel·ligents

La pròpia evolució de la web va fent aparèixer tecnologies cada vegada més complexes que permeten l'ús pels sistemes informàtics de programes en els ordinadors que busquen informació sense operadors humans, el que sol denominar-se "Agents intel·ligents". Aquesta nova etapa en el que sembla el previsible futur del web, es defineix amb el terme Web 3.0.

El terme Web 3.0 apareix per primera vegada el 2001, en un article de la revista Nature, escrit per Tim Berners-Lee i James Hendler, en què plantejaven la necessitat dels usuaris de poder accedir ràpidament en internet a la informació desitjada. Perquè aquesta agilitat fos possible, els dos autors sostenien que, donada la ingent quantitat d'informació disponible, les màquines haurien de ser capaces de gestionar la informació comprenent d'alguna manera el seu significat per facilitar a l'usuari allò que desitja.

La Web 3.0 per tant es basa en què la informació pugui ser processada directament pels ordinadors basant-se en el significat i no en la terminologia utilitzada per publicar-la. Les recerques de continguts passen a ser semàntiques, és a dir, centrades en el significat que busca l'usuari, en lloc de sintàctiques basades en les paraules utilitzades.

Encara que no hi ha acord sobre el significat real de Web 3.0 i hi ha grans discrepàncies entre diferents autors en tractar de definir-ho, podríem caracteritzar la Web 3.0 com la incorporació de les tecnologies d'intel·ligència artificial a la web. Encara que freqüentment s'assimila el concepte de Web 3.0 al de "Web Semàntica" en realitat el concepte és bastant més ampli, inclou ara la "*squared web*", que incorpora a la web dades del món real recollits directament pel sistema a partir de sensors.

La Web Semàntica incorpora metadades semàntiques a la informació que circula per internet, és a dir, mitjançant les metadades afegim a les dades informació que les expliqui o les contextualitzi. Ara per ara aquests metadades s'han d'establir per humans, però l'objectiu últim de la Web 3.0 seria la indexació semàntica automàtica dels continguts. Així doncs, el més característic del Web 3.0 futura seria, la incorporació de tecnologies que permetessin als servidors interpretar els continguts i associar-los als interessos de l'usuari sense precisar cap tipus de supervisió humana. Es tracta d'una actuació proactiva que tracta de personalitzar al màxim la informació facilitada a l'usuari.

Les tecnologies Web 3.0 són encara molt incipients, però totes elles tendeixen a facilitar que els continguts siguin interpretats directament pels servidors, sense necessitat que l'usuari els classifiqui mitjançant l'ús d'etiquetes assignades per ell mateix. La idea bàsica és que de manera automàtica, i sense supervisió humana directa, el servidor sigui capaç de conèixer els interessos i les preferències d'un usuari concret sense que aquest hagi de expressar-ho, o si s'escau, interpretar i reconduir les peticions de cerca d'aquests usuaris.

Un exemple de Web 3.0 són els cercadors que suggereixen termes (*tags*) en forma de núvol relacionats amb la recerca que poden ajudar a centrar més aquesta cerca. El cercador presenta un conjunt d'enllaços que ofereix a l'usuari una sèrie de pàgines a les que pot accedir, i que tenen continguts relacionats amb allò que presumiblement està buscant l'usuari. En alguns casos es presenten també informacions sobre pàgines a les quals han accedit altres usuaris que aparentment realitzaven una recerca similar.

## **Internet i les amenaces a la seguretat**

No és només internet l'únic sistema que treballa en xarxa. Hi ha altres xarxes com ara les de telefonia mòbil; les corporatives d'organitzacions i empreses; les dels campus universitaris; les que poden configurar-se en domicilis particulars o en un vehicle,... Això dóna una idea de la diversitat i el gran nombre d'àmbits d'aplicació dels sistemes en xarxa.

Així, per exemple, les xarxes de telefonia mòbil permeten donar cobertura als telèfons mòbils evitant que s'interrompi una trucada quan el mòbil es desplaça d'una zona a una altra; des d'un vehicle es poden utilitzar serveis com el GPS per orientar la direcció, o per localitzar el vehicle en cas de robatori; les xarxes en domicilis particulars permeten la unió de diversos dispositius, com pot ser l'ordinador, la impressora, o l'escàner; les xarxes dels campus universitaris, o les xarxes corporatives permeten treballar coordinadament a diferents usuaris de la mateixa universitat, empresa, o organització. Quan alguna d'aquestes xarxes s'administren separatament, i de manera accessible únicament per als membres de l'organització de què es tracti, es denomina Intranet.



No obstant això, internet és un sistema enorme, que permet una varietat també molt elevada d'aplicacions. Amb Internet podem accedir a serveis com el *World Wide Web*, el correu electrònic, la transferència de fitxers i molts altres serveis similars. Actualment, una gran part de la població utilitza diàriament un motor de cerca per buscar informació; llegir continguts diversos, incloent llibres que estan digitalitzats a la web; mantenir contactes personals i/o professionals mitjançant les xarxes socials; utilitzar opcions d'entreteniment com els jocs en línia o escoltar música o veure vídeos també en línia; fer compres a través del comerç electrònic, tant de productes alimentaris bàsics, com roba, viatges, entrades a espectacles o qualsevol altre servei o producte; consultar o fer moviments financers en el seu compte bancari a través de la banca en línia; o també utilitzar serveis a nivell educatiu o professional. Aquesta multitud de serveis possibles va acompanyat també d'un variat ventall d'amenaques per a la seguretat del sistema.

Un dels problemes de seguretat que es poden donar en un ordinador és la introducció d'un programa maliciós en el dispositiu a través d'Internet. D'aquesta manera, la persona que ha introduït el programa maliciós en el dispositiu pot eliminar arxius o recopilar informació personal.

Un altre dels atacs de seguretat més freqüents és el denegació de servei. Aquest atac va dirigit als dispositius que donen serveis, com pot ser els servidors de correu electrònic o de pàgines web. La forma en què es produeix aquest atac pot ser divers: d'una banda, es pot enviar una seqüència de paquets a una aplicació o sistema operatiu vulnerable que fa que el servei pari o, fins i tot, que el dispositiu es bloquegi; per una altra banda, es pot enviar molts paquets al dispositiu objectiu que embussen l'accés a peticions legítimes; i, finalment, es pot establir un

gran nombre de connexions falses que facin que el dispositiu deixi d'acceptar noves connexions legítimes.

També hi ha el perill de l'atac que consisteix en fer una còpia dels paquets que s'envien i, per tant, amb aquesta còpia es pot analitzar i obtenir informació confidencial. Altres sistemes d'atac es basen en el falsejament d'identitat que consisteix en enviar un paquet amb una adreça d'origen falsa que l'encaminador pren com a certa. Amb aquest atac s'aconsegueix accedir a llocs on normalment no es té accés.

Internet s'ha convertit en un registre de la nostra vida i és que amb una simple cerca a la xarxa podem trobar nombroses dades sobre nosaltres, moltes d'aquestes que afecten la nostra intimitat i privacitat com aficions, tendències polítiques i sexuals, estat civil, domicili o professió.

Aquesta informació de vegades pot plantejar als ciutadans problemes personals i professionals en ser utilitzada per tercers amb finalitats diferents per a les que en un principi es van subministrar. Per aquest motiu moltes persones han reclamat el seu dret a desaparèixer d'Internet en resultar comprometedor.

Amb l'expansió d'Internet, els drets a l'honor i a la pròpia imatge són uns dels drets més atacats avui dia. Freqüentment es publiquen comentaris o informacions sobre persones a les que insulten o acusen de fets que en moltes ocasions són incerts i que menyscaben la seva imatge pública. Això a més a més es facilita amb la possibilitat d'un aparent anonimat a la xarxa de qui moltes vegades difon aquests comentaris. Això augmenta, a més a més, amb l'enorme capacitat dels cercadors (especialment Google) per referenciar i indexar tota aquesta informació i mostrar-la per ordre de rellevància.

D'aquesta manera i en molts casos, en buscar el nom d'una persona a internet lluny d'aparèixer les dades del seu currículum vitae i dels seus èxits, ens apareixen crítiques, insults i informacions dubtoses sobre ella. Això danya enormement la seva reputació tant a nivell privat com professional. Especialment preocupant per la privacitat i la intimitat és el recent fenomen de les xarxes socials que, lluny de constituir una moda passatgera, han arribat per quedar-se i formen ja una nova realitat social.

Aquests riscos s'agreugen en pertànyer la major part de les xarxes socials a empreses ubicades als Estats Units, pel que en la pràctica moltes vegades s'aplica la seva legislació i normativa pel que fa a les mesures de protecció en matèria de privacitat.

Una altra problemàtica que es planteja en l'ús de les noves tecnologies afecta de ple als drets de l'interessat ja que cada vegada és més freqüent que l'usuari es trobi amb dades publicades a la xarxa sense el seu consentiment o coneixement, un expedient acadèmic, una publicació ja oblidada, la fitxa d'antics alumnes, el perfil publicat a les xarxes socials, aquelles fotografies que pretenien il·lustrar moments i situacions concretes. Són innombrables les informacions que es poden trobar a internet.

Gran part d'aquesta informació la subministren els propis usuaris, simplement en utilitzar les xarxes socials i en accedir a les múltiples possibilitats que ofereix internet. A tot això s'ha d'afegir que no sempre el titular de les dades disposa de la informació suficient sobre la destinació que es pot donar a les seves dades, especialment quan es tracta de dades personals. En molts casos tampoc s'ha obtingut una

autorització vàlida d'aquest usuari perquè les seves dades a la xarxa puguin ser publicades o utilitzades.

## **Capítol quart: Comerç electrònic**

---

### **El comerç electrònic**

El comerç electrònic va rebre en els seus inicis un tractament legal similar al de la venda per correspondència. Aquest sistema de venda per correspondència es va iniciar a finals del segle XIX als Estats Units, quan empreses com Sears i Montgomery Ward van començar a utilitzar la venda per catàleg.

No obstant això, no va ser fins als inicis de la dècada dels anys 70 del segle XX quan es va generalitzar l'automatització en les transaccions a distància mitjançant l'edició de factures, ordres de compra, bases de dades, i en general les tasques de suport administratiu.

A mitjans de la dècada següent va començar a generalitzar l'ús de la televisió com a complement a la venda per catàleg mitjançant el que es va denominar "venda directa" en què el venedor presentava els seus productes per televisió i el comprador feia la seva comanda per telèfon, abonant mitjançant targeta de crèdit. Finalment, a mitjans dels anys 90, es produeix l'eclosió de la venda a través d'Internet, que des de llavors no ha parat de créixer.

El que coneixem com a comerç electrònic no es refereix únicament a la compra i la venda de diferents productes i serveis, sinó que és un

concepte més ampli que es refereix a qualsevol transacció comercial realitzada electrònicament.

La compravenda realitzada mitjançant comerç electrònic presenta molts avantatges, ja que permet realitzar les transaccions sense limitacions horàries ni territorials; elimina intermediaris; el contacte és relativament senzill; redueix costos, [...] No obstant això, com a contrapartida té també alguns inconvenients, entre els quals destaquen la necessitat de garantir la seguretat en els productes o en els mitjans de pagament; una més complexa identificació de venedors i compradors; la possible no adequació dels productes rebuts respecte als oferts; i altres problemàtiques similars que, tot i que també es donen en la resta de modalitats de la venda a distància, en el cas de les transaccions electròniques presenten una peculiar idiosincràsia.

El comerç electrònic o *e-commerce* es basa en la compra i venda de productes o serveis utilitzant les noves tecnologies de la comunicació, especialment Internet. L'activitat pot donar-se entre empreses i particulars *Business to Consumer* (B2C), entre empreses, *Business-to-business* (B2B) entre consumidors directament *Consumer to consumer* (C2C). Hi ha altres modalitats de comerç electrònic menys conegudes, com les que es donen entre consumidors i empreses *Consumer to Business* (C2B); les empreses i els seus empleats *Business to employee* (B2E); les empreses i l'Administració (B2A) i altres similars<sup>30</sup>.

---

<sup>30</sup> Són diverses les modalitats de comerç electrònic conegudes per les inicials dels seus denominacions en anglès. Podem trobar, entre d'altres: Business-to-Government (B2G); Business-to-Machines (B2M); Business-to-Manager (B2M); Consumer-to-Business (C2B); Consumer-to-Consumer (C2C); Citizen (Consumer)-to-Government (C2G); Government-to-Business (G2B); Government-to-Citizen (G2C); Government-to-Employee (G2E); Government-

Centrant-nos en el comerç electrònic B2C, és a dir, l'activitat que es dóna entre empreses i particulars, el venedor actua com a "proveïdor de continguts" atès que el seu paper és el de subministrar els productes i serveis a vendre a través d'Internet.

No obstant això, perquè aquests continguts arribin a l'usuari es fa també necessària la participació d'altres proveïdors de serveis que faciliten el contacte entre els usuaris o clients i els proveïdors d'aquests continguts. Aquests proveïdors, en la mesura que també participen en el procés, poden incórrer en responsabilitat, de manera que en analitzar la responsabilitat en matèria de comerç electrònic cal referir-nos no només als proveïdors de continguts, sinó també als que realitzen tasques de intermediació per tal que pugui produir-se aquest comerç, de manera que en la pràctica hi participen. Es tracta del que en terminologia de Montcada López podem anomenar "Prestadors de serveis d'intermediació"<sup>31</sup>.

## **Dret Internacional Privat**

El comerç electrònic s'ha desenvolupat en els últims anys de manera exponencial i tots els indicadors apunten que aquesta progressió serà encara més important en un futur immediat. Això fa que es vagi

---

to-Government (G2G); Manager-to-Consumer (M2C);... És més discutible que altres denominacions freqüentment tractades com a comerç electrònic, com és el cas de Peer-to-Peer (P2P), ho siguin en realitat.

<sup>31</sup> Montcada Flórez, Juan Pablo La responsabilidad de los prestadores de servicios de intermediación en la sociedad de la información. Tesis doctoral presentada el 2009 a la Facultat de Dret de la Universitat de Granada.

configurant un extens Dret del Comerç Electrònic amb què el legislador, i naturalment la corresponent jurisprudència, pretén donar resposta als diferents i complexos conflictes que aquesta modalitat de comerç comporta internacionalment en l'actualitat.

No obstant això, la realitat és que els avenços tecnològics en aquest camp fan que ens trobem davant d'un entorn que canvia permanentment a gran velocitat, i per tant deixa obsolets els paradigmes amb els quals en un moment donat es pretén analitzar la situació en què es produeix l'intercanvi comercial per aquest mitjà.

Per això el marc legal i jurisprudencial relacionat amb el comerç electrònic és dels més dinàmics que actualment podem trobar. No només cal donar resposta als problemes jurídics inherents a aquest tipus de contractació a mesura que els avenços tecnològics van evolucionant, sinó que si no es fa així hi ha un greu risc d'indefensió per part de consumidors, propietaris de marques, dominis intel·lectuals, i altres similars. En general corre risc el propi concepte de comerç tal com el coneixem actualment, ja que al llarg dels anys s'ha anat configurant un marc de relacions que permet un desenvolupament amb uns nivells acceptables de seguretat i de l'atribució de la responsabilitat.

Avui, la problemàtica representada pel comerç electrònic, especialment el realitzat a través d'Internet, va més enllà que la mera computació client/servidor. La computació client/servidor es basa en la relació entre un servidor, que és qui ofereix un recurs, amb el client, que és qui ho sol·licita. En aquest cas, qualsevol client que vulgui aquest recurs ha de connectar amb el servidor i aquest ha d'estar sempre disponible, és a dir, que el client tindrà el rol actiu i el servidor el rol passiu.



La invocació remota en aquest context s'inicia per un client que envia una petició a un servidor remot per a executar un mètode. Per la seva banda, el servidor pren els paràmetres que també li envia el client i computa la resposta que posteriorment retornarà al client que li ha fet la petició.

Aquesta problemàtica es pot abordar des de diferents perspectives en la seva regulació. No obstant això, el fet que les pròpies característiques d'Internet facin que la seva activitat es desenvolupi freqüentment de manera internacional, fa que s'hagi d'acudir a un marc regulador basat fonamentalment en el dret internacional privat, o bé des de l'*International Cyber Law*, tal i com veurem posteriorment.

## Regulació legal

La regulació del comerç electrònic a Espanya, es basa fonamentalment en els principis enumerats en la Llei 7/1996, de 15 de gener, d'ordenació del comerç minorista, especialment en tot el relatiu a les vendes a distància. Aquesta llei regula el règim jurídic general del comerç minorista. S'hi estableix que l'activitat, per ser considerada comerç minorista, s'ha de desenvolupar professionalment, amb ànim de lucre, i consistir en oferir qualsevol classe d'articles a un destinatari final:

"... Als efectes d'aquesta Llei, s'entén per comerç minorista aquella activitat desenvolupada professionalment amb ànim de

lucre consistent a oferir la venda de qualsevol classe d'articles als seus destinataris finals, utilitzant o no un establiment..."<sup>32</sup>.

És interessant destacar el fet que no sigui necessari utilitzar un establiment perquè es produeixi el comerç. De fet, la principal característica de les vendes a distància és precisament que es realitzen sense la presència física simultània del comprador i del venedor:

"... Es regiran pel que disposa aquest títol els contractes celebrats a distància amb els consumidors i usuaris en el marc d'un sistema organitzat de venda o prestació de serveis a distància, sense la presència física simultània de l'empresari i del consumidor i usuari, i en el que s'hagin utilitzat exclusivament una o més tècniques de comunicació a distància fins al moment de la celebració del contracte i en la pròpia celebració d'aquest.

Entre altres, tenen la consideració de tècniques de comunicació a distància: el correu postal, Internet, el telèfon o el fax..."<sup>33</sup>.

Per tal de garantir un cert control de les empreses dedicades en el territori espanyol a la venda a distància, es va crear un òrgan de caràcter públic i naturalesa administrativa, dependent de la Direcció General de

---

<sup>32</sup> Article 1.2 de la Llei 7/1996, de 15 de gener, d'ordenació del comerç minorista.

<sup>33</sup> Article 92 del text refós de la Llei General per a la Defensa dels Consumidors i Usuaris i altres lleis complementàries aprovat pel Reial Decret Legislatiu 1/2007, de 16 de novembre, i al qual fa referència l'article 38.1 de la Llei 7/1996, de 15 de gener, d'ordenació del comerç minorista.

Política Comercial del Ministeri d'Indústria, Turisme i Comerç, denominat "Registre d'empreses de vendes a distància"<sup>34</sup>.

No obstant això, és la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic, la que específicament regula el comerç electrònic. En aquesta llei es dona especial importància a la identificació de l'empresa que utilitzi els serveis de la societat de la informació com a canal de vendes.

El legislador és conscient de la dificultat d'establir les responsabilitats de l'oferent en una relació de comerç minorista, quan aquesta es produeix utilitzant les noves tecnologies electròniques. Per això s'inclou en la regulació d'aquest comerç, no només al venedor, sinó també als que actuen com a intermediaris en la transmissió de continguts per les xarxes de telecomunicacions:

"... És objecte d'aquesta Llei la regulació del règim jurídic dels serveis de la societat de la informació i de la contractació per via electrònica, pel que fa a les obligacions dels prestadors de serveis inclosos els que actuen com a intermediaris en la transmissió de continguts per les xarxes de telecomunicacions, les comunicacions comercials per via electrònica, la informació prèvia i posterior a la celebració de contractes electrònics, les condicions relatives a la seva validesa i eficàcia i el règim

---

<sup>34</sup> Reial Decret 225/2006, de 24 de febrer, pel qual es regulen determinats aspectes de les vendes a distància i la inscripció en el registre d'empreses de vendes a distància.

sancionador aplicable als prestadors de serveis de la societat de la informació..."<sup>35</sup>.

En tot cas, per garantir la responsabilitat del venedor i de l'intermediari, el legislador deixa clar que s'han de donar els requisits que estableixen els codis Civil i de Comerç, així com les restants normes civils o mercantils sobre contractes. Però no només estableix que s'han de complir aquests requisits, així com les normes de protecció dels consumidors i usuaris, sinó que específicament recalca la necessitat del consentiment de les parts per a la validesa del contracte:

"... Els contractes celebrats per via electrònica produiran tots els efectes previstos per l'ordenament jurídic, quan concorrin el consentiment i els altres requisits necessaris per a la seva validesa..."<sup>36</sup>.

Això és així en tota relació comercial, però el fet que el legislador ho recalqui novament en parlar del comerç electrònic, dóna idea de la importància del consentiment en aquest tipus de comerç.

Alguns aspectes de la venda a distància estan regulats a Espanya pel Reial Decret 225/2006, de 24 de febrer, pel qual es regulen determinats aspectes de les vendes a distància i la inscripció en el registre d'empreses de vendes a distància.

---

<sup>35</sup> Article 1.1 de la Llei 34/2002, de 11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

<sup>36</sup> Article 23.1 de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

---

No obstant això, el comerç electrònic no és una mera venda a distància, sinó que presenta unes característiques pròpies, que fan molt més complex aquest mitjà. Això fa que el legislador especifiqui detalladament obligacions com les de la informació que el venedor ha de proporcionar al comprador. Les prevencions, tant en les legislacions nacionals, com a les autonòmiques en el cas d'Espanya, il·lustren els riscos que el comerç electrònic pot presentar per al consumidor<sup>37</sup>.

La protecció jurídica del consumidor enfront de possibles abusos per part de les empreses està teòricament molt reforçada, per la legislació i per la jurisprudència actual, per això en el cas del comerç electrònic també es dóna naturalment aquesta protecció prioritària:

---

<sup>37</sup> Un exemple d'això el podem trobar en el primer apartat de l'article 222-2 de la Llei 22/2010, de 20 de juliol, del Codi de consum de Catalunya: "...Tota proposta de contractació a distància ha d'incloure, de manera clara i inequívoca, informació sobre els aspectes següents: a) La identitat de l'ofertor del bé o servei; b) La identificació de la proposta de contractació. La manca de resposta a la proposta no n'implica l'acceptació; c) El procediment que cal seguir i els requisits necessaris per formalitzar el contracte; d) El cost de l'ús de la tècnica de comunicació a distància, si aquest és superior a les tarifes bàsiques del servei; e) La informació relativa al bé o servei que s'ofereixi, amb la descripció suficient de la naturalesa, la quantitat, la qualitat i les possibilitats de consum o d'ús del dit bé o servei; f) El preu total, d'acord amb el que estableix la normativa aplicable. L'import corresponent a les despeses de lliurament s'ha de consignar de manera separada si aquestes són a càrrec de la persona consumidora; g) La modalitat i el termini màxim de lliurament del bé o d'execució del servei des del moment de recepció de la comanda. Amb aquesta finalitat, l'empresari o empresària ha de fer arribar a la persona consumidora un justificant de recepció de la comanda en el termini de tres dies a partir de la data de recepció; h) La informació que l'article 211-15 estableix amb relació al dret de desistiment, quan correspongui el dret de desistiment a la persona consumidora; i) El sistema de devolució del bé en cas de manca de conformitat. S'ha de fer constar expressament que, en aquest cas, les despeses de devolució són a càrrec de l'empresari o empresària; j) Les modalitats de pagament; k) Les garanties i els serveis postvenda...".

"... en la demanda s'exercita l'acció individual d'un consumidor, factor determinant d'una interpretació favorable al mateix d'acord amb la Directiva 93/13/CEE del Consell, de 5 d'abril de 1993, la més correcta transposició al dret intern, després de la sentència del Tribunal de Justícia de les Comunitats Europees de 9 de setembre de 1994, s'ha dut a terme per la Llei 44/2006, de 29 de desembre, de millora de la protecció dels consumidors i usuaris..."<sup>38</sup>.

A més del marc normatiu específic sobre consum, la protecció legal d'usuaris i consumidors de comerç electrònic, ve recollida en la legislació general sobre telecomunicacions<sup>39</sup>. En la legislació espanyola es recullen les directives de la Unió Europea sobre aquesta protecció. Així, a part del marc regulador comunitari que ja estava inclòs en l'anterior Llei General sobre Telecomunicacions<sup>40</sup>, aquesta nova llei també té com a marc

---

<sup>38</sup> Fonament de dret únic de la interlocutòria de la Sala Civil del Tribunal Suprem 6623/11 de 31 de maig de 2011.

<sup>39</sup> Llei 9/2014, de 9 de maig, General de Telecomunicacions.

<sup>40</sup> La Llei 32/2003 de 3 de novembre, General de Telecomunicacions tenia com a marc regulador comunitari la Directiva 2002/21/CE, del Parlament Europeu i del Consell, de 7 de març de 2002, relativa a un marc regulador comú de les xarxes i els serveis de comunicacions electròniques, la Directiva 2002/20/CE, del Parlament Europeu i del Consell, de 7 de març de 2002, relativa a l'autorització de xarxes i serveis de comunicacions electròniques, la Directiva 2002/22/CE, del Parlament Europeu i del Consell, de 7 de març de 2002, relativa al servei universal i els drets dels usuaris en relació amb les xarxes i els serveis de comunicacions electròniques, la Directiva 2002/19/CE, del Parlament Europeu i del Consell, de 7 de març de 2002, relativa a l'accés a les xarxes de comunicacions electròniques i recursos associats, i a la seva interconnexió, la 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; la Directiva 2002/77/CE, de la Comissió, de 16 de setembre de 2002, relativa a la competència en els mercats de xarxes i serveis de comunicacions electròniques; i, finalment, la Decisió número 676/2002/CE, del Parlament Europeu i del Consell,

regulador comunitari, tal com la mateixa exposició de motius de la Llei General de Telecomunicacions especifica la Directiva 2009/136/CE, del Parlament Europeu i del Consell, de 25 de novembre de 2009, relativa als drets dels usuaris i la Directiva 2009/140/CE, del Parlament Europeu i del Consell, de 25 de novembre de 2009, sobre una millor regulació de les xarxes.

Es desenvolupa en diferents normatives aquesta protecció especial als consumidors, en regular per exemple les condicions per a la prestació de serveis de comunicacions electròniques, el servei universal i la protecció dels usuaris<sup>41</sup>, la carta de drets dels usuaris dels serveis de comunicació electrònica<sup>42</sup> o les condicions de qualitat que han de tenir les comunicacions electròniques<sup>43</sup>.

## Les activitats del comerç electrònic

El comerç electrònic abasta un variat nombre d'activitats complementàries però diferents entre si. Analitzar la utilització de tecnologies d'intel·ligència artificial en aquest comerç electrònic i la seva

---

de 7 de març de 2002, sobre un marc regulador de la política de l'espectre radioelèctric a la Comunitat Europea.

<sup>41</sup> Reial Decret 424/2005, de 15 d'abril, pel qual s'aprova el Reglament sobre les condicions per a la prestació de serveis de comunicacions electròniques, el servei universal i la protecció dels usuaris, modificat pel Reial Decret 726/2011, de 20 de maig.

<sup>42</sup> Reial Decret 899/2009, de 22 de maig, pel qual s'aprova la carta de drets de l'usuari dels serveis de comunicacions electròniques.

<sup>43</sup> Ordre IET/1090/2014, de 16 de juny, per la qual es regulen les condicions relatives a la qualitat de servei en la prestació dels serveis de comunicacions electròniques.

influència en els nivells de responsabilitat, implica analitzar separatament cadascuna de les activitats que l'integren. Per tal de conèixer les tendències actuals en aquesta atribució de responsabilitats cal analitzar la legislació i la jurisprudència desenvolupada en cadascuna de les activitats que formen part del comerç electrònic.

En totes les activitats realitzades pels principals grups dedicats al comerç electrònic, com poden ser eBay, Alibaba i altres grans organitzacions com Amazon i d'altres semblants, s'utilitzen cada vegada més tecnologies de *Big Data* i d'intel·ligència artificial, donat l'ingent volum de dades que mouen diàriament. En aquest sentit, és simptomàtic que aquest fet es doni en empreses provinents d'entorns culturals diferents, com es pot veure en els dos grups empresarials de comerç electrònic més importants en l'actualitat: eBay, d'origen Nord-americà i Alibaba, d'origen Xinès. Això planteja directament la importància del tema de la responsabilitat per les accions realitzades per sistemes autònoms, sense la intervenció directa de cap ésser humà. Es tracta d'una qüestió que en un món globalitzat com el representat per Internet s'ha d'abordar, fins i tot, més enllà de les possibles diferències culturals.

Un dels principals grups dedicats al comerç electrònic és eBay. En realitat eBay està formada per diverses filials que actuen en països fora dels Estats Units, d'on és originària l'empresa matriu, que es dediquen a facilitar les vendes de productes per part de tercers a través dels seus recursos tecnològics.

El grup corporatiu eBay Inc. té nombroses empreses filials o subsidiades al llarg del món. Les més importants es presenten agrupades en quatre grans àrees: eBay Marketplaces; PayPal; eBay Enterprise i X.commerce. A



la taula següent s'explica l'activitat principal a què es dedica cadascuna d'elles.

**Taula 4.1 - Principals empreses del grup eBay Inc.**

eBay Marketplaces	<b>Agrupa aquelles empreses dedicades específicament a la compravenda a través de comerç electrònic.</b>
eBay	Connecta a través de la seva plataforma a compradors i venedors globals, amb unes transaccions anuals d'aproximadament 62 bilions de dòlars anuals.
WHI	Proporciona aplicacions d' <i>e-business</i> per a la indústria del transport mitjançant tecnologies <i>cloud computing</i> , incloent comerç electrònic, catàleg electrònic, gestió de la distribució i intel·ligència comercial.
<u>StubHub</u>	Permet l'adquisició d'entrades per a esports, espectacles i concerts. Els particulars poden vendre les seves entrades quan no les poden utilitzar.
Zvents	Ofereix una plataforma en la què es puguin publicitar esdeveniments locals i ofertes de promoció. El seu catàleg presenta més de tres milions d'esdeveniments generats per venedors i promotors locals.
Milo	Plataforma perquè minoristes locals ofereixin els seus productes en temps real. Permet escanejar inventaris, localitzar articles i conèixer el seu preu.
eBay Advertising	Plataforma per generar anuncis personalitzats d'empreses i anunciants gràcies als seus recursos de dades, plataforma i tecnologia.
Half.com	Ofereix un mercat en línia per a la compra de llibres de text, llibres, música, pel·lícules i videojocs, nous i de segona mà, a preus reduïts.
brands4friends	Club de compres d'Alemanya per a articles de luxe seleccionats amb fins a un 70% de descompte.
Critical Path	Centrat en el desenvolupament de programari per a mòbils, és responsable de moltes de les aplicacions per a comerç electrònic mitjançant mòbils d'eBay Inc.

GittiGidiyor.com	Filial d'eBay Inc. amb seu a Turquia. És present en 43 països amb set milions d'usuaris registrats i més de 500 mil visitants diaris, amb vendes que arriben als 14 milions de consumidors.
Hunch	Plataforma que ofereix recomanacions personalitzades als seus usuaris en funció dels seus gustos individuals. La tecnologia de predicció patentada de Hunch -també coneguda com "gràfic gust"- utilitza senyals de tota la web per mapejar els usuaris per la seva afinitat a productes i serveis.
<u>eBay Classifieds Group</u>	Anuncis classificats en línia de marques i empreses de tot el món. El grup està integrat per diferents companyies orientades a comunitats específiques.
alaMaula	Dirigit al mercat llatinoamericà ofereix una xarxa d'anuncis classificats en línia de llocs locals en espanyol i portuguès.
BilBasen	Dedicada exclusivament als anuncis de vehicles a Dinamarca, incloent anuncis de vídeo i un fòrum de compradors.
Dbn	Dedicada als anuncis a Dinamarca de tot tipus de productes, ofertes de treball i avisos personals.
Gumtree	Lloc d'anuncis classificats líder al Regne Unit, Irlanda, Austràlia i Sud-àfrica, amb una forta presència a Hong Kong, Singapur, Nova Zelanda i Polònia.
Kijiji	Lloc d'anuncis classificats gratuïts de Canadà. Ofereix una plataforma per intercanviar béns i serveis entre particulars, o perquè aquests reciclin coses que ja no fan servir.
Marktplaats.nl	Lloc per reciclar productes usats i ajudar els clients a trobar el que necessitaven a preus raonables. És el lloc de comerç electrònic més popular als Països Baixos.
Mobile.de	Permet connectar compradors de vehicles de tot tipus amb els concessionaris a Alemanya. Té mercats addicionals a Itàlia, França, Polònia i Romania.
eBay Classifieds	Ofereix una plataforma lliure de classificats per a l'intercanvi de béns, ofertes de treball i tot tipus de serveis. Amb sucursals a diferents països, com: Espanya (eBay Anuncis), Alemanya (Kleinanzeigen), Itàlia (eBay Holiday), Estats Units, etc.

PayPal	<b>Agrupa aquelles empreses dedicades a facilitar el pagament i a rebre ingressos en línia de forma segura.</b>
PayPal	Plataforma per realitzar pagaments segurs sense l'intercanvi d'informació financera. Permet el comerç electrònic global amb més de 100 milions de comptes actius en 190 mercats i 25 divises a tot el món.
BillMeLater	Ofereix una forma de pagar pels béns, ja sigui en línia o per telèfon, sense necessitat de targeta de crèdit.
WHERE	Ofertes de restauració i oci en les destinacions locals a través d'una aplicació per a mòbil. Permet a les petites i mitjanes empreses crear un portal d'autoservei i administrar campanyes de publicitat, cupons i ofertes.
Zong.com	Permet el pagament de les compres en línia amb el telèfon mòbil, a través del seu mateix número.
eBay Enterprise	<b>Agrupa aquelles filials dedicades a facilitar a altres empreses tot tipus de solucions de comerç especialitzat.</b>
eBay Enterprise	Proveïdor de serveis de comerç electrònic i de màrqueting interactiu per a marques i minoristes. Cobreix tots els aspectes del negoci en línia, incloent solucions de tecnologia, logística i atenció al client.
True Action	Serveis de màrqueting estratègic per a les marques i els minoristes. Amb una àmplia gamma de recursos per crear estratègies en línia, continguts i programes per arribar als consumidors de manera rendible i sostenible.
VendorNet	Solucions de programari de gestió per a la cadena de subministrament basades en la web, des de la gestió de comandes fins a tota la cadena de subministrament (magatzems, proveïdors de tercers i botigues).
X.commerce	<b>Agrupa aquelles filials dedicades a donar suport tecnològic a empreses de comerç electrònic de totes les mides.</b>
Magento	Solució de comerç electrònic de codi obert que ofereix als comerciants una total flexibilitat i control sobre l'aparença, contingut i funcionalitat de la seva botiga en línia, així com marxandatge i altres eines de gestió.

X.commerce	Proveïdor de serveis de suport a empreses en totes les seves activitats de venda, des de la comanda fins al lliurament del producte. Dissenyat per incorporar totes les formes de compra utilitzades pels consumidors.
------------	--

Font: Adaptació pròpia a partir de les pàgines web corporatives del Grup eBay Inc.

Una altra plataforma destacada en comerç electrònic és el Grup Alibaba, (集團阿里巴巴) radicat a la Xina, però amb milions de compradors i proveïdors a tot el món. Aquest grup disposa de diferents filials que actuen de manera subsidiària per especialitzar la seva oferta d'acord a les principals activitats implicades en el comerç electrònic.

Així, una d'aquestes filials s'especialitza en el pagament electrònic, una altra en màrqueting, una altra en logística, varies més centrades en diferents segments de comerç com poden ser el majorista, el minorista, les marques d'alt nivell o les ofertes econòmiques. Algunes de les principals empreses filials del grup Alibaba són les següents:

#### Taula 4.2 - Principals empreses del grup Alibaba

Alibaba.com (阿里巴巴国际交易市场) (www.alibaba.com)	Plataforma per al comerç majorista global a través de la qual les petites empreses poden vendre els seus productes a empreses d'altres països. (Especialment els fabricants i distribuïdors amb seu a la Xina i altres països com l'Índia, el Pakistan, Estats Units i Tailàndia.
AliExpress (全球速賣通) (www.aliexpress.com)	Ofereix una plataforma per al mercat minorista i global destinat als consumidors a tot el món per a comprar directament a majoristes i fabricants de la Xina.

<p>Tmall.com (天猫) (www.tmall.com)</p>	<p>Proporciona una plataforma perquè gran nombre de marques i minoristes internacionals i xinesos estableixin botigues des d'on oferir mercaderies d'alta qualitat per als consumidors xinesos.</p>
<p>Juhuasuan (聚划算) (www.juhuasuan.com)</p>	<p>Plataforma que ofereix productes de qualitat a preus reduïts mitjançant l'agregació de la demanda dels nombrosos consumidors. Posa al mercat productes a preus especials durant un període de temps limitat. És el mercat electrònic més popular a la Xina.</p>
<p>Taobao Marketplace (淘宝网) (www.taobao.com)</p>	<p>Plataforma de comerç electrònic que permet triar entre centenars de milions de llistats de productes i serveis. La seva aplicació per a mòbil, Taobao App Mòbil, és l'aplicació per a comerç, mitjançant mòbil, més popular a la Xina.</p>
<p>China Smart Logistics, (o Zhejiang Cainiao Supply Chain Management Co., Ltd.) (中国智能物流骨干网)</p>	<p>Gestiona una plataforma d'informació logística, que proporciona accés en temps real a la informació per als compradors i venedors del sector del comerç electrònic i de dispositius mòbils.</p>
<p>Alipay (支付宝) (www.Alipay.com)</p>	<p>Ofereix serveis de pagament i de dipòsit en garantia. Permet fer i rebre pagaments en línia i en telèfons mòbils en les transaccions realitzades en els mercats del grup, així com a tercers a la Xina.</p> <p>És el proveïdor de serveis de pagament en línia més gran a la Xina pel volum total de pagaments.</p>
<p>Alibaba Cloud Computing (阿里云计算) (www.aliyun.com)</p>	<p>Proporciona un conjunt complet de serveis de <i>cloud computing</i> i per a la gestió de dades als venedors i clients del comerç electrònic i mòbil.</p>
<p>Alimama (阿里妈妈) (www.alimama.com)</p>	<p>Plataforma de tecnologia de màrqueting en línia que ofereix als venedors en els mercats del grup serveis de màrqueting en línia, tant per a ordinadors personals com per a dispositius mòbils.</p>

1688.com  
(www.1688.com)

Mercat en línia majorista que funciona com un canal de venda a l'engròs per als comerciants que operen com a minoristes per als productes nacionals xinesos.

Font: adaptació pròpia a partir de les pàgines web corporatives del Grup Alibaba

## Capítol cinquè: Una perspectiva jurídica

---

### Les noves tecnologies davant les branques del dret

Tradicionalment els estudis de dret s'han dividit des de l'antic dret romà, en dues grans àrees, el dret públic i el dret privat. El primer es refereix al conjunt de normes relatives a les activitats i forma d'organitzar-se els poders públics, mentre que el segon es dirigeix a regular les activitats i relacions entre particulars. Aquestes dues grans àrees es subdivideixen alhora en branques o especialitats. Així, el Dret Públic comprèn el Dret Constitucional, l'Administratiu, el Processal, Penal, el Dret Agrari, el Dret del Treball, i el Fiscal, mentre que el Dret Privat comprèn el Dret Civil i el Mercantil. D'altra banda, tant el Dret Públic com el Privat poden referir-se a la normativa interna o externa de cada Estat, de manera que quan parlem de les relacions entre diferents estats, podem distingir també entre el Dret Internacional Públic i el Dret Internacional Privat<sup>44</sup>.

També trobem noves subdivisions en funció de l'àmbit concret de l'activitat a la qual ens vulguem referir. Així, ens referim al Dret Canònic, al Militar, al Mediambiental... Aquesta classificació de les disciplines jurídiques respon a un intent d'especialització de les diferents branques

---

<sup>44</sup> Són múltiples les perspectives i constructes teòrics des dels què podem abordar la classificació del Dret. Així, podem parlar de Dret Natural o Dret Positiu; Objectiu o Subjectiu; Estatuït o Consuetudinari,...

del Dret Objectiu, però, en la pràctica, podem trobar múltiples classificacions diferents segons el país, la cultura, o l'època a la qual ens puguem referir. Encara que a grans trets aquestes classificacions tenen una certa voluntat de permanència, la veritat és que van canviant amb l'evolució de la pròpia societat.

El Dret bàsicament té com a objectiu regular la conducta i activitats humanes en cada moment i situació. No és estrany doncs que l'aparició de les noves tecnologies hagi tingut un fort impacte en l'àmbit del Dret. Tal com recull Elvira López:

"... el Dret és un ordre de la convivència humana que es fa indispensable quan els homes viuen junts i en comunitat, *«on hi ha societat, allà hi ha dret» (ubi societas, ibi ius)*. El Dret neix en i per a la convivència social humana i només va destinat a ella. El Dret d'un poble forma part de la seva història i de la seva cultura, es presenta com un concepte dinàmic en plena i en contínua evolució, com un sistema de normes a les quals la convivència s'ha d'atenir i d'acord amb les quals s'han de solucionar els conflictes que es poden suscitar entre els homes que viuen en relació..." (López 2006).

L'aparició de la informàtica ha influït naturalment en l'àmbit jurídic, però a diferència d'altres grans avenços produïts en la societat, en aquest cas la influència sobre el Dret afecta pràcticament totes les seves branques. L'espai virtual representa una nova manera de fer les activitats humanes, però ens hem de preguntar si això comporta els mateixos principis jurídics que a la resta d'espais tradicionals, o si per contra l'adaptació de les disciplines jurídiques a aquesta nova realitat implica el desenvolupament de nous principis. Així doncs, la qüestió principal és



conèixer si es tracta d'un canvi de paradigmes, o tan sols d'un canvi en l'entorn operatiu en el qual es desenvolupen les activitats.

La influència de les noves tecnologies, especialment la informàtica, en el Dret, ha fet aparèixer una branca específica relativa a la relació entre la Informàtica i el Dret. Aquesta branca al seu torn, s'ha anat especialitzant en diversos camps, especialment en l'anomenada Informàtica Jurídica, en el Dret Informàtic i en la Informàtica Legal. Així, la Informàtica Jurídica té per objecte l'aplicació de la informàtica en el món del dret, mentre que el Dret Informàtic es circumscriu a la regulació jurídica de les noves tecnologies i la Informàtica Legal a l'estudi de les tècniques que han de permetre l'aplicació correcta del dret en relació a les noves tecnologies<sup>45</sup>.

A la pràctica, podem parlar d'una major precisió en la classificació de cada un d'aquests apartats. Així per exemple, podem diferenciar la Informàtica Jurídica de Gestió (l'activitat concreta del jurista) de la Informàtica Jurídica Documental (relativa a les bases de dades, documents,...) de la Informàtica Jurídica Decisional (aportació per les noves tecnologies d'elements facilitadors de l'activitat judicial).

El desenvolupament informàtic, i l'aparició d'internet han tingut un gran impacte en múltiples camps, entre ells molt especialment, el món empresarial. Les activitats empresarials més usals avui a Internet són el comerç electrònic; l'assessoria i la consultoria; el màrqueting i la publicitat; la formació i la capacitació; l'oci i la cultura, incloent la música, el cinema, la literatura, el sexe, i similars; el turisme, incloent transport, hostaleria i restauració. No obstant això, les accions concretes

---

<sup>45</sup> Encara conceptes com Noves tecnologies, Informàtica, Tecnologies de la informació i la Comunicació (TIC) i altres similars, es refereixen a temes relacionats, però no exactament iguals, aquí ens centrem especialment en la influència de la informàtica.

realitzades a través d'Internet pels seus usuaris no representen cap canvi real en els principis, valors i paradigmes generals aplicables a aquesta activitat.

Qualsevol empresa que desitgi realitzar les seves activitats a través d'Internet, s'enfronta a la necessitat de complir un complex entramat de disposicions legals que abasten des d'aspectes merament administratius fins a altres que poden portar a responsabilitat penal. Temes com definir el nom del domini, contractar un proveïdor de serveis, dissenyar el seu lloc web, o mantenir i gestionar el lloc, es troben regulats per les pròpies normes del WWW. No obstant això, independentment de les normatives internes que puguin existir en el ciberespai, la seva activitat s'ha d'ajustar a les lleis i normes jurídiques existents en el món no virtual. La contractació, les compravendes, la publicitat, la protecció del menor, la gestió de les dades personals... es regeixen pels mateixos principis jurídics que els que es donen en aquestes mateixes activitats realitzades en altres entorns més tradicionals.

## **El dret anglosaxó i el continental**

Hi ha diferències notables entre el dret anglosaxó i el continental. Mentre el primer es genera a partir de la *equity* i el *common law*, i posa l'èmfasi en la jurisprudència vinculant per a tot el sistema judicial, més que en les pròpies normes, en el sistema continental, basat principalment en el dret romà, és prioritari el marc legislatiu i només alguns òrgans judicials creen jurisprudència, com és el cas, a l'Estat Espanyol, del Tribunal Suprem. Així, la visió predominant en cada un dels sistemes sobre aspectes característics de l'espai virtual, com pot ser el tema de la territorialitat, o

la interpretació donada a termes com a drets d'autor, o *copyright*, pot marcar algunes diferències, però la tendència predominant en l'actualitat és a una cada vegada major confluència en la pràctica entre el dret anglosaxó i el continental.

Naturalment la major dependència de la normativa en el sistema continental dota el sistema anglosaxó de més flexibilitat. No obstant això, l'aparició d'internet fa que els factors territorials siguin progressivament més difusos, el que fa cada vegada més pròxims els dos sistemes, i sorgeix amb una força encara més important tot el relatiu a l'*International Cyber Law*.

Avui, la problemàtica representada pel comerç electrònic, especialment el realitzat a través d'internet, va més enllà que la mera computació client/servidor. Aquesta problemàtica es pot abordar des de diferents perspectives en la seva regulació. No obstant això, el fet que les pròpies característiques d'internet facin que la seva activitat es desenvolupi freqüentment de manera internacional, fa que s'hagi d'acudir a un marc regulador basat fonamentalment en el dret internacional privat, o bé des del *International Cyber Law*.

L'*International Cyber Law* pretén la resolució dels conflictes mitjançant el desenvolupament d'una normativa internacional específica, que superi les limitacions territorials i les diferències existents en el dret particular de cada Estat. Tal com especifica Guillermo Díaz Bermejo:

"... Es tractaria d'una *lex mercatoria* del Ciberespai-International amb un cos de regles uniformes, institucions i principis provinents de diferents fonts que regulen les activitats dels operadors del comerç electrònic internacional.

Dins d'aquest conjunt de regles estaria un codi legislatiu que regulés el comerç electrònic a escala internacional, aplicable a les transaccions internacionals per tots els països, via tractat internacional o Codi de Conducta a Internet, *netiquettes*, polítiques d'usos a la xarxa (*Internet Use Policies*), regulacions de proveïdors d'accés a Internet, normes deontològiques, principis bàsics d'*e-business*, etc...."

Tanmateix tal com el mateix Díaz Bermejo explica: "la idea de *l'International Cyber Law* és incompatible amb la idea de sobirania nacional dels estats i aquests en última instància mai renunciaran a la seva vessant reguladora"<sup>46</sup>.

Per això, excepte en alguns supòsits vinculats estrictament amb el propi funcionament d'internet, com podria ser el de la gestió dels dominis, a la pràctica, sempre és necessària la intervenció d'un Estat quan necessitem una intervenció judicial efectiva. Per això la regulació del comerç electrònic mitjançant Internet es basa fonamentalment en el dret internacional privat, si bé adaptat a les peculiaritats d'internet.

## **Desjudicialització de conflictes i mediació en línia**

A la pràctica un gran nombre de conflictes sorgits a internet són resolts freqüentment a través de les pròpies organitzacions que gestionen aspectes concrets de la xarxa. Les matèries en què pot resultar eficaç

---

<sup>46</sup> Díaz Bermejo, Guillermo. "La resolución internacional de controversias en el comercio electrónico" E-Gov, 2012. Pot consultar-se a: <http://www.egov.ufsc.br/portal/conteudo/la-resolucion-internacional-de-controversias-en-el-comercio-electronico>.

aquest tipus d'intervencions són aquelles relatives a aspectes com el repartiment de les IP identificadores, els llenguatges de programació, així com tot el relacionat amb l'assignació i la gestió dels dominis i altres temes similars relacionats amb els protocols de funcionament d'internet. No obstant això, sempre que entren en conflicte béns jurídics protegits, és la justícia qui té, i ha de tenir, l'última paraula en la seva resolució, i fins i tot entrant a definir com s'han d'interpretar els mateixos termes tècnics utilitzats a internet:

"... Per «domini», s'entén a internet, la denominació que es dóna a la porció d'«espai» que s'ocupa «*ex novo*» en el recentment aparegut continent virtual. Quan una persona, empresa o institució desembarca en aquest «nou món», pren immediatament possessió d'una parcel·la del territori i, simultàniament, la pretén identificar, tant per a la seva pròpia seguretat com per al coneixement dels altres. El nom que atorgui a la seva nova possessió és el que -en termes cibernetes-, s'anomena «domini»..."<sup>47</sup>.

El "dret de domini" en general, i a internet en particular, té la naturalesa jurídica de dret real limitat, és a dir, és un dret que proporciona un poder no ple o limitat, immediat i directe sobre la cosa en què recau.

Un dels procediments utilitzats per a la resolució desjudicialitzada dels conflictes sorgits a Internet és l'anomenada mediació *on-line*. La mediació *on-line* consisteix en un procés de resolució de conflictes

---

<sup>47</sup> Fonament Jurídic segon de la Sentència número 517/2005 de 21 novembre de la Secció 11a de l'Audiència Provincial de Madrid.

alternatiu a la justícia tradicional, que es planteja via electrònica, almenys en les parts més importants del procés.

Els requisits bàsics per poder dur a terme el procés de mediació *on-line* és disposar d'un espai on dur a terme la discussió entre el mediador i totes les parts (*xat room*), un altre espai on el mediador pot parlar amb cadascuna de les parts per separat (*caucus*) i un espai on es puguin conservar els documents necessaris per a la mediació.

Les etapes en general que componen el procés de mediació *on-line* no difereixen de les que es poden produir en qualsevol altre procés de mediació tradicional, tot i així cada etapa té certes particularitats pel fet de realitzar-se *on-line*. Així doncs, les etapes són:

- 1) “la premeditació amb l'avantatge que no cal que el mediador informe sobre tot el que ja està a disposició en línia;
- 2) les històries de les parts amb l'única diferència que no es va disposar de la informació que aporta la comunicació no verbal;
- 3) el generar opcions amb l'avantatge d'atorgar més temps a les parts per pensar amb les opcions;
- 4) la negociació sense cap diferència per fer-se en línia;
- 5) l'acord amb l'avantatge de poder-se realitzar amb més rapidesa” (Montesinos, 2008).

Seguint Montesinos, els principals avantatges d'aquest procediment són:

- a) la rapidesa que aporta la comunicació *on-line*;
- b) l'estalvi econòmic tant pel fet de no haver-se de traslladar com altres costos que, de no fer-se en línia, es derivarien com el

conseller jurídic a l'estranger, la traducció de documents i similars;

- c) evitar el conflicte d'horaris;
- d) accés en qualsevol moment a la situació en què es troba el procés
- e) evitar l'hostilitat emocional que podria provocar un enfrontament cara a cara.

D'altra banda, els principals inconvenients d'aquest sistema són:

- a) la manca d'informació, especialment pel mediador, que aporta la comunicació no verbal;
- b) la necessitat que totes les parts tinguin un coneixement informàtic mínim per no estar en inferioritat de condicions;
- c) manca de la confiança que aporta a les parts el contacte directe amb el mediador i de control en contactar amb l'altra part
- d) problemes de seguretat i confidencialitat que produeix l'ús d'Internet.

En alguns casos aquest mitjà extrajudicial de resolució de conflictes pot ser molt útil, tal com demostrem les activitats a nivell europeu de la Xarxa de Centres Europeus dels Consumidors que s'ocupen de la mediació entre consumidors i empreses radicats en països diferents dins de la Unió Europea<sup>48</sup>. Aquesta és una manera que permet tant als consumidors com a les empreses poder expressar-se amb la seva pròpia

---

<sup>48</sup> El Centre Europeu del Consumidor a Espanya, dependent de l'Agència Espanyola de Consum, Seguretat Alimentària i Nutrició, és una oficina pública d'atenció al consumidor de qualsevol Estat membre de la Unió Europea que precisi informació o assistència en relació amb l'adquisició d'un bé o la utilització d'un servei en un país diferent al propi. Pot consultar les seves funcions i activitats a: [http://www.cec.consumo-inc.es/secciones.php?id\\_sec=1&id\\_subsec=1](http://www.cec.consumo-inc.es/secciones.php?id_sec=1&id_subsec=1).

llengua evitant malentesos i, a part, la comunicació entre parts neutrals com els Centres Europeus radicats en diferents països fa que les hostilitats emocionals es deixin de banda i amplia a més el coneixement de la legislació en cada un dels estats membres i de la Unió Europea en general.

A part, el fet de poder dur a terme la mediació de manera virtual fa que sigui molt més accessible tant per la reducció de temps com la reducció de diners que comporta aquest mitjà. En general els avantatges d'aquest sistema són molt més elevats que els possibles inconvenients que podria aportar. És especialment significativa la desjudicialització de molts conflictes sorgits entre clients i empreses, que d'altra manera carregarien encara més les sobresaturades estructures judicials. Tanmateix, la seva utilitat es dona exclusivament en aquells casos en què el conflicte no comporta fets delictius i la mediació és acceptada per totes les parts.

Això fa que alguns dels conflictes plantejats sobre els dominis es puguin resoldre al marge de la justícia, però com passa a la resta de temes, és aquesta l'encarregada d'interpretar la Llei en última instància i de garantir la protecció jurídica dels drets presumptament atacats. Així, l'atribució de responsabilitats, la interpretació del seu abast i en general tot el relacionat amb la responsabilitat com a concepte jurídic, és exclusivament competència del marc legal corresponent i són els jutges i tribunals els encarregats de la seva interpretació.

Així, la normativa que regula el comerç electrònic i els contractes electrònics en general, sempre que siguin realitzats amb consentiment de les parts i reunint tots els requisits necessaris, estableixen clarament que aquests produiran tots els efectes previstos per l'ordenament jurídic,



tal i com s'ha vist anteriorment en l'article 23.1 de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

Per analitzar de quina manera pot estar afectant l'atribució de responsabilitats en tot el que fa referència amb el comerç electrònic la progressiva generalització de la Intel·ligència Artificial, i dels sistemes autònoms en general, es fa necessari estudiar tant la legislació nacional i internacional sobre el tema, com la jurisprudència existent. Amb això es poden detectar pautes i tendències que indiquin algun tipus de variació en els paradigmes utilitzats per definir la responsabilitat.

## **Dret penal del risc**

Els anomenats delictes informàtics poden englobar genèricament en l'anomenat Dret Penal del Risc, ja que Internet és en sí mateix un fenomen de les societats de risc. De fet, la demanda social de seguretat, tal com expressa Mendoza, tendeix a veure el Dret Penal com una eina eficaç per a buscar aquesta seguretat en l'entorn virtual, tal com de fet succeeix en altres entorns de la vida real:

"... La percepció social de l'increment del risc genera una demanda igualment creixent de seguretat, que en gran mesura es dirigeix específicament al dret penal, com a forma de resposta jurídica més contundent i suposadament més eficaç..." (Mendoza, 2001).

Són molts els camps en què el Dret ha anat definint la responsabilitat en diversos camps relacionats amb l'ús d'internet. Així, la responsabilitat de pares i tutors; la dels prestadors de serveis; la dels empresaris i els

empleats pel seu ús en horari laboral; la dels usuaris de les xarxes socials; la dels prestadors i els usuaris de les comunicacions sense fils tipus wifi i molts altres similars.

No obstant això, un dels temes que més preocupen actualment, són les infraccions i les activitats delictives que més fàcilment poden produir-se a internet. Les infraccions contra els drets d'autor i la propietat intel·lectual; contra la privacitat i les dades personals; la difamació i els atacs contra la pròpia imatge; els fraus informàtics; els enganys en el comerç electrònic, en les subhastes, o en les compravendes entre particulars; la publicitat enganyosa o no desitjada; la pirateria de dominis i la usurpació d'IP o de la pròpia personalitat; els drets del menor,... Són algunes de les activitats que poden incórrer en il·lícits penals, als quals cal afegir l'ús de l'entorn virtual per cometre altres accions delictives tradicionals com les relacionades amb el terrorisme; el tràfic de drogues, el d'armes, el d'òrgans, o el de persones; les amenaces; el robatori; les estafes, i moltes altres activitats similars.

En general, gran part de les figures delictives tradicionals poden realitzar-se, o es poden potenciar a través de les noves tecnologies de la comunicació, i molt especialment d'internet. Des d'aquesta perspectiva, les implicacions que presenta sobre la responsabilitat l'aparició dels robots i altres mecanismes autònoms, així com els sistemes dotats d'Intel·ligència Artificial, és d'una importància fonamental.

## **2ª Part:**

### **Un nou espai par al comerç electrònic**



## **Capítol sisè:**

### **Big Data: superant els límits**

---

#### **Gestió de grans volums de dades**

L'objectiu de l'estratègia de les empreses de comerç electrònic i del seu pla comercial, s'ha d'orientar a trobar una manera pràctica d'aprofitar les dades dels resultats de negoci més predictibles. D'altra banda, per poder seguir l'evolució en l'ús del seu comerç és necessari tenir clar que no hi ha grans salts independents en el tractament de les dades, sinó que és una constant en evolució a partir d'una situació actual. Sempre que hi ha un avanç tecnològic apareix un nou requisit legal, o canvia el perfil dels consumidors, cal que hi hagi una adaptació i el corresponent canvi en la forma de fer aquest tractament de les dades.

Cal tenir en compte que la majoria de les empreses que actualment es dediquen d'alguna manera al comerç electrònic, han de gestionar grans volums de dades. Es tracta d'una influència altament positiva ja que seria impensable aconseguir els avenços espectaculars que en aquest tema s'estan aconseguint sense desenvolupar sistemes específics per al tractament de grans volums de dades. Això presenta un enorme potencial positiu, però també alguns inconvenients.

La gestió de grans volums de dades, com tota nova tecnologia, també presenta alguns riscos inherents al seu possible mal ús. Precisament pel

seu alt potencial positiu, el seu ús adequat pot resultar un gran benefici per a l'empresa, encara que també un perill si se'n fa un ús inadequat.

Una gran empresa com eBay utilitza Hadoop per emmagatzemar les seves dades, tant les estructurades com les no estructurades. Això ha implicat, segons la pròpia empresa, un canvi absolut en els paradigmes d'emmagatzematge de dades que desenvolupava. Altres grans companyies com WallMart, Amazon o American Apparel, utilitzen aquestes mateixes tecnologies per analitzar el comportament dels seus clients i amb això afinar els seus serveis optimitzant-los i guanyant en eficiència i competitivitat. L'ús de grans volums de dades s'està estenent molt ràpidament a tots els sectors que han de tractar molta informació. Totes aquestes tecnologies poden englobar-se en el que s'anomena *Big Data*.

El sector financer i les diverses entitats vinculades a aquest sector, com bancs, asseguradores, agències de canvi i altres similars, estan generalitzant l'ús de *Big Data* per analitzar la informació de què disposen dels seus clients, per tal de personalitzar al màxim els seus productes i obtenir dades reals que els facilitin la presa de decisions.

El banc ING Direct és una de les institucions que ha apostat més clarament per aquestes tecnologies, el mateix podem dir del Banc Sabadell, que ha realitzat una anàlisi de les xarxes socials amb eines de *Big Data* per comprendre millor als seus clients i optimitzar els seus serveis. D'altra banda, PayPal detecta operacions fraudulentas mitjançant diversos filtres basats en conjunts de dades massius analitzats a través d'eines de *Big Data*.

En el camp de les telecomunicacions podem trobar exemples com la nova unitat de Telefónica sobre l'ús de grans volums de dades anomenada Dynamic Insights. Telefónica analitza milers de dades agregades i totalment anònimes, utilitzant-les per mesurar, comparar i comprendre quins factors influeixen en el consumidor. Un altre exemple és el cas d'estudi de la Xina Telecom i Big Data, mitjançant el qual la Xina Telecom gestiona una base de clients de 250 milions de subscriptors d'ADSL, el que els ha permès desenvolupar una base de dades mitjançant la qual emmagatzema i accedeix ràpidament als registres d'aquests milions d'abonats<sup>49</sup>.

Un dels problemes amb els que s'han d'enfrontar els proveïdors de serveis vinculats amb el comerç electrònic és la quantitat ingent de dades que han de manipular, el que freqüentment supera les capacitats habituals de tractament de dades usals en els sistemes informàtics. Això fa que l'ús de grans volums de dades s'estigui convertint en una de les tendències tecnològiques actuals més importants. Les empreses busquen com poden organitzar i utilitzar aquests conjunts massius de dades per millorar i transformar els seus models de negoci.

Als anys seixanta del segle passat, les dades s'emmagatzemaven en arxius de text plans amb una estructura simple i, quan una empresa volia tenir un coneixement detallat sobre els clients, es limitava a aplicar mètodes lents i pesats per tal de poder obtenir alguna informació de valor.

---

<sup>49</sup> A Internet podem trobar nombrosos exemples d'aquesta generalització de l'ús de grans volums de dades als més diversos camps. Un exemple d'això el podem trobar a [http://bigdata.hadoop.pragsis.com/pages/2/casos\\_de\\_uso](http://bigdata.hadoop.pragsis.com/pages/2/casos_de_uso).

Posteriorment van aparèixer els models de dades relacionals i els sistemes de gestió de bases de dades relacionals. Amb això es va començar a imposar una estructura a les dades i es va poder millorar el rendiment de les cerques. Un dels avenços més importants en aquest tema va ser el llenguatge de consulta estructural (SQL) que encara avui en dia s'utilitza en pràcticament totes les bases de dades relacionals.

El model relacional va ser un avenç important i va ajudar a les empreses a organitzar millor les seves dades i a poder comparar les dades d'un lloc amb les d'un altre lloc. Tot i així, el gran volum de dades a emmagatzemar resultava car i, a part, poder accedir a aquestes dades era lent. Aquest va ser el motiu de l'aparició del model entitat-relació que va afegir una abstracció addicional per tal de poder augmentar la capacitat d'ús de les dades. En aquest model, cada element es defineix independentment del seu ús, per tant, els desenvolupadors poden crear noves relacions entre les fonts de dades sense necessitat d'utilitzar una programació complexa. Aquest va ser un gran avenç que va permetre als desenvolupadors empènyer els límits de la tecnologia i crear models més complexos que requereixen tècniques complexes per a la unió de les entitats entre si.

Tanmateix, i donat que el volum de dades no parava de créixer, es van anar generalitzant els magatzems de dades. Això permetia seleccionar un subconjunt de les dades que s'emmagatzemaven, de manera que fos més fàcil per a l'empresa el tractar-les i analitzar-les. D'altra banda, el magatzem de dades permet acumular dades d'anys anteriors, el que va permetre fer comparacions temporals, i així poder observar l'evolució de l'organització, identificar tendències i ajudar a exposar els patrons de comportament.



Però freqüentment fins i tot els magatzems de dades són massa complexos i grans i, per tant, no ofereixen la velocitat i l'agilitat que requereix l'organització. Per tal de solucionar aquesta qüestió, es va fer un refinament addicional a les dades que es gestionaven a través de mercats de dades. Així, aquests mercats de dades es centraven en qüestions específiques de l'organització i aconseguien ser més àgils i poder cobrir les necessitats de l'empresa per a poder fer consultes ràpides que els magatzems de dades no podien atendre.

## **Dades estructurades i no estructurades**

Fins aquest moment, les dades que s'estaven processant de forma correcta eren les dades estructurades, però el problema sorgia quan s'intentava analitzar dades no estructurades, per la qual cosa, es van desenvolupar els sistemes de gestió de bases de dades orientades a objectes. En aquest sistema s'inclou un llenguatge de programació i una estructura per als elements de dades de manera que sigui més fàcil manipular diversos conjunts de dades.

Avui dia, a Internet, es evident la necessitat de bases de dades distribuïdes a gran escala. Aquest fet, junt a diversos avenços tecnològics com són la virtualització, el processament paral·lel, sistemes d'arxius distribuïts, bases de dades en memòria, l'anàlisi avançat,... estant fent possible un ús real de grans volums de dades. La virtualització de les dades permet que emmagatzemar-les es faci d'una forma més eficient i, d'altra banda, el fet de basar aquest emmagatzematge en núvol fa que sigui més rendible. De forma similar, hi havia altres limitacions físiques que s'han anat eliminant, gràcies a les

milliores en la velocitat i la fiabilitat de la xarxa, fent possible el gestionar grans quantitats de dades a una velocitat acceptable. Si a aquests fets se'ls hi uneix la baixada en el preu i l'augment de la memòria dels ordinadors, es pot començar a veure com les organitzacions poden avui en dia fer un ús de grans volums de dades més elevat i eficaç.

Cal tenir en compte que les dades no estructurades són diferents de les dades estructurades en el fet que la seva estructura no es pot preveure. És a dir, les dades poden incloure documents, imatges, vídeos, correus electrònics, blogs,... Així doncs, si les organitzacions poden analitzar petabytes de dades no estructurades amb un rendiment acceptable per a poder observar patrons i anomalies, aquestes organitzacions poden començar a donar sentit a les dades de noves formes. Les empreses que aconseguixin realitzar aquest anàlisi de forma eficaç, seran les que lideraran els mercats en els pròxims anys. No s'ha d'oblidar que en el passat, com ja s'ha comentat, la majoria de les empreses no eren capaces de capturar o emmagatzemar una gran quantitat de dades, simplement perquè era massa car o massa aclaparador. Però, fins i tot si les empreses podien capturar les dades, no tenien les eines per analitzar fàcilment aquestes dades i utilitzar els resultats per prendre decisions. Molt poques eines podrien donar sentit a aquestes grans quantitats de dades, i les eines que existien eren difícils d'utilitzar i no produïen els resultats en un termini de temps raonable. Per això, les empreses que volien fer front a aquests esforços, van decidir-se per treballar amb instantànies de les dades, és a dir, amb un subconjunt del total de les dades.

Aquesta forma de fer l'anàlisi tenia el problema que deixava objectes importants fora de l'anàlisi i, per tant, aquest no era del tot eficaç com

hauria de ser. Un enfocament que s'està convertint cada vegada més valorat com una forma d'obtenir valor de negoci a partir de dades no estructurades és l'anàlisi de text, el procés d'anàlisi de text no estructurat, l'extracció de la informació pertinent, i la seva transformació en informació estructurada que pot ser aprofitada de diverses maneres. L'anàlisi i els processos d'extracció utilitza i treu profit de les tècniques que es van originar en la lingüística computacional, en l'estadística i en d'altres disciplines de les ciències de la computació.

Es important tenir en compte d'on provenen majoritàriament les dades que es volen analitzar. En l'estudi d'IBM i Oxford, 2012 Estudi d'Anàlisi: L'ús de grans volums de dades en el món real, es conclou que les quatre principals fonts de dades són: transaccions, dades de registre, esdeveniments i correus electrònics. A part, apunta que les cinc principals capacitats de l'ús de grans volums de dades estan en: la mineria de dades, la realització d'informes, la visualització de les mateixes dades, la realització de models predictius i l'optimització de resultats<sup>50</sup>.

## **El concepte de macrodades o *Big Data***

Apareix així el concepte de *Big Data*, concepte que en realitat no és més que una referència genèrica a aquests grans volums de dades, o el que

---

<sup>50</sup> IBM Institute for Business Value i Saïd Business School de l'Universitat d'Oxford, 2012 Analytics Study: The realworld use of big data. Es pot consultar a [https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=csuite-NA&S\\_PKG=Q412IBVBigData](https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=csuite-NA&S_PKG=Q412IBVBigData).

en català podem anomenar “macrodades”<sup>51</sup>. En un principi les dades conceptualitzades com a *Big Data* simplement es relacionaven fonamentalment amb la informació relativa als compradors, productes i transaccions. Tanmateix, avui en dia no és únicament el volum de dades a manipular el que representa una qüestió fonamental, sinó la pròpia complexitat d’aquestes dades, que poden procedir de la tecnologia dels telèfons mòbils; vídeos; SMS; xarxes socials; així com d’altres plataformes i sistemes.

L’ús de grans volums de dades té el potencial de canviar la forma en que les empreses utilitzen la informació per tal de millorar l’experiència que tenen els seus clients o per a transformar els seus models de negoci. Però aquesta no és una qüestió nova que acaba d’aparèixer, sinó que una evolució en la gestió i l’anàlisi de dades sempre ha obert la porta a avantatges competitiu per a les empreses pioneres, les quals han obtingut majors beneficis i han fet evolucionar la resta d’organitzacions per tal de poder competir-hi. Aquest fet es va poder observar mirant l’evolució en el tractament de les dades que han anat sorgint tant per cobrir una nova necessitat per tractar de resoldre un tipus de problema específic en la gestió de les dades o per l’arribada al mercat d’una nova solució tecnològica que va obrir noves possibilitats en aquesta gestió.

De la complexitat actual del concepte de *Big Data* és una mostra el gran nombre de referències que podem trobar sobre aquest tema. Són molts els esdeveniments convocats per analitzar aquesta complexitat, per exemple, el “Big Data Week” dedicat precisament a debatre sobre això.

---

<sup>51</sup> La definició de macrodades que podem trobar a TermCat és: “Conjunt de dades que pel seu volum, la seva naturalesa i la velocitat a què han de ser processades ultrapassen la capacitat dels sistemes informàtics habituals” (<http://www.termcat.cat/ca/Cercaterm>).

Des d'aquesta perspectiva es pot definir *Big Data* com la manipulació tecnificada d'ingents quantitats de dades, la majoria d'elles generades de forma automàtica en diverses tasques facilitades per les Tecnologies de la Informació i la Comunicació<sup>52</sup>.

Aquesta mateixa complexitat també comporta nous reptes per al legislador i per a la jurisprudència, reptes cada vegada més presents en estudis i congressos. Així, el IX Congrés Internet, Dret i Política, celebrat al mes de juny de 2013 a Barcelona, va tenir com a tema central el de "Big Data: Reptes i Oportunitats". Es va plantejar en aquest congrés l'estudi dels aspectes legals i polítics que es desprenen del tractament de grans volums de dades agrupades en el que denominem *Big Data*.

Al parlar de Big Data sorgeix vinculat a aquest concepte un vell paradigma corrent en el món de la arxivística que podríem plantejar com les teories de l'anarxiu. En essència es tracta de l'afirmació de que totes les dades es poden conservar i, per tant, es poden accedir a les mateixes en qualsevol moment per a la seva constant reutilització. Aquesta afirmació en realitat abans no deixava de ser una posició més aviat filosòfica. L'arxiu i la conservació de les dades estava fortament limitada per la pròpia limitació del suport en que aquestes dades es presentaven i pel rudimentari dels sistemes de conservació i accés. Llibres, documents, fotografies, mapes, és a dir, tots aquells suports en que es podien plasmar les informacions o, el que és el mateix, les diferents dades, eren "acumulats" en espais físics determinats com poden ser les biblioteques, les hemeroteques, i altres espais com els museus, les fototeques, i altres espais similars.

---

<sup>52</sup> Extret de: <http://bigdataweek.com/2013/04/05/monographicbibliography-on-big-data/>

Però el desenvolupament de les noves tecnologies, ha capgirat radicalment aquesta situació. El potencial de tractament de la informació que ofereix actualment la informàtica, la superació de les limitacions espacials que representen fenòmens com el d'Internet, l'aparició de nous sistemes d'intercanvi d'informació, les xarxes socials,... constitueix una realitat que era absolutament impensable fa només uns pocs anys enrere. Per això podem avui afirmar que el que abans era una utopia, qualsevol altre cosa que en la realitat no podia anar més enllà del seu tractament com un producte filosòfic, una aspiració irrealitzable pràcticament, a passat a ser avui en dia una realitat potencial tan propera que es configura cada vegada més com un nou model de negoci<sup>53</sup>.

Tanmateix, no és suficient amb comptar amb la gran capacitat tecnològica actual que ens permet l'acumulació i, fins i tot, el ràpid accés a grans quantitats de dades impensables fins fa molt poc temps. És necessari a més a més d'això, que aquestes dades puguin conservar-se i accedir-hi, de manera fàcil i comprensible per a les nostres estructures mentals i limitacions humanes. De res serveix la possibilitat de disposar de multitud d'informacions en un sistema, si no som capaços de trobar concretament aquella informació que en cada moment ens és necessària.

Les tècniques per a l'ús de grans volums de dades són una de les noves tecnologies que ens permet que la utopia de l'anarxiu sigui avui en dia una realitat. Permet la recuperació de les informacions de manera molt ràpida i, el que és més important, permet la recuperació de dades no estructurades. Si limitéssim l'accés únicament a dades ben

---

<sup>53</sup> Joan Soler Jiménez. "Big Data, l'anarxiu i l'evolució dels arxius històrics" Es pot consultar en <http://diplomaticapuntcat.blogspot.com.es/2013/04/big-data-lanarxiu-i-levolucio-dels.html>.

estructurades, per exemple mitjançant la seva indexació manual en un arxiu informatitzat, l'alt volum de dades a estructurar faria necessari un esforç immens, així com un temps fora de mida. L'ús de grans volums de dades permet recuperar informacions que, fins i tot, no són estructurades.

Aquesta tecnologia ha d'anar acompanyada d'altres com per exemple el *Cloud Computing*, que ens permet externalitzar la gestió de la memòria que ocupen les dades tractades, o el *Business Analytics* que pretén la racionalització de les informacions recuperades, de manera que es converteixin en informacions rellevants per a la finalitat perseguida<sup>54</sup>.

L'ús de grans volums de dades permet a les organitzacions emmagatzemar, administrar i manipular grans quantitats de dades de diferents tipus a una velocitat adequada i en un moment també adequat per tal de poder obtenir els coneixements necessaris per prendre decisions i establir i/o modificar l'estratègia de negoci. Per tant, com es pot observar, hi ha tres grans característiques principals a tenir en compte:

- El volum, és a dir, la quantitat de les dades. Aquest volum ha de ser prou gran per tal de ser considerat dins d'aquest grup (en certs llocs, com per exemple a IBM, es considera que el volum de dades és suficientment gran si sobrepassa 1 petabyte, és a dir, un milió de gigabytes)<sup>55</sup>.

---

<sup>54</sup> Podem trobar la vinculació d'aquestes tècniques, en articles com el publicat per Joan Soler Jiménez a <http://diplomaticapuntcat.blogspot.com.es/2011/12/podremos-confiar-en-la-triada-cloud.html?sref=tw>.

<sup>55</sup> Jean François Puget, "Big Data For Dummies", IBM developerWorks. Es pot consultar a:

- La velocitat, és a dir, la rapidesa en el processament d'aquestes dades. En aquest punt, cal tenir en consideració que les dades poden estar en moviment, és a dir, poden ser en estat real i, per tant, la forma del seu processament pot variar segons si les dades són estables o estan en moviment.
- La varietat, és a dir, els diferents tipus de dades que ens trobem. S'ha de tenir en compte que les dades poden ser text, imatges, vídeos,...

Aquestes tres característiques principals són amb les que molts autors defineixen el *Big Data* i a les que es refereixen com a les tres Vs. Tot i així, també s'ha de tenir en compte les veus crítiques amb aquesta visió, que es veu com a massa simplista, ja que els mètodes aplicats al *Big Data*, poden ser d'utilitat en el tractament d'un volum relativament petit de dades quan aquestes són molt diverses i complexes o, d'altra banda, ser utilitzat per un gran volum de dades molt simples, tant estructurades com no estructurades.

Deixant de banda aquesta crítica, també s'ha de considerar una quarta V que molts autors també apunten a l'hora de definir el concepte de l'ús de grans volums de dades, aquesta és la veracitat. La veracitat fa referència a que el resultat de l'anàlisi realitzat al gran volum de dades tingui sentit i, també, a la precisió de les dades per tal de predir unes conseqüències que puguin ser d'utilitat.

Així doncs, quan tenim grans volums de dades, ens trobem que a més a més de triar quantes dades seleccionar, de quin tipus, com processar-

---

[https://www.ibm.com/developerworks/community/blogs/jfp/entry/big\\_data\\_for\\_dummies23?lang=en](https://www.ibm.com/developerworks/community/blogs/jfp/entry/big_data_for_dummies23?lang=en).



les,... també hem de garantir que les dades siguin verificables, tant pel que fa a la seva precisió com pel que fa al context. Veiem doncs que en realitat la consideració de gran volum al referir-nos a un conjunt de dades, és relatiu, doncs en realitat està en funció de diferents variables. Considerar o no un conjunt de dades com a *Big Data* depèn, per exemple, de la capacitat real dels sistemes per a actuar sobre un gran número de dades.

És evident la importància que té el tractament adequat d'aquests conjunts de grans dades, tant per a les empreses com per a la investigació i el desenvolupament. Les tècniques de Big Data permeten una manera pràctica de tractar amb un volum gran de dades, i amb això de poder mantenir la competitivitat de l'empresa. Al fer referència al tractament de les dades, s'està tenint en compte la necessitat de desenvolupar noves maneres de capturar i analitzar el creixent volum d'informació que es té de clients, productes, serveis,...

Aquestes dades són cada vegada més complexes, algunes de les quals tenen formes estructurades però d'altres són no estructurades i, per tant, s'ha de ser capaç de tractar ambdós tipus de dades. A part, hi ha noves fonts des d'on s'obtenen les dades, n'hi ha que procedeixen de les pròpies màquines (com poden ser sensors, mitjançant xarxes socials o simplement amb la interacció amb diverses pàgines web). Per tant, per tal de poder satisfer aquestes necessitats canviant, s'exigeix que la informació sigui correcte i estigui disponible en el moment adequat.

## Responsabilitat en el tractament de *Big Data*

Actualment les empreses estan envoltades de grans volums de dades, però el problema és que sovint no saben com utilitzar pragmàticament aquestes dades per poder predir el futur, poder executar processos de negocis importants o simplement obtenir nous coneixements i, el que és més greu, poden incórrer en responsabilitat. En aquest sentit, la legislació exigeix de responsabilitat als operadors de xarxes i als proveïdors d'accés:

“... 1. Els operadors de xarxes de telecomunicacions i proveïdors d'accés a una xarxa de telecomunicacions que prestin un servei d'intermediació que consisteixi a transmetre per una xarxa de telecomunicacions dades facilitades pel destinatari del servei o a facilitar accés a aquesta no seran responsables per la informació transmesa, llevat que ells mateixos hagin originat la transmissió, modificat les dades o seleccionat aquestes o als destinataris de les dades.

No s'entén per modificació la manipulació estrictament tècnica dels arxius que continguin les dades, que té lloc durant la seva transmissió.

2. Les activitats de transmissió i provisió d'accés a què es refereix l'apartat anterior inclouen l'emmagatzematge automàtic, provisional i transitori de les dades, sempre que serveixi exclusivament per permetre la seva transmissió per

la xarxa de telecomunicacions i la durada no superi el temps raonablement necessari per això...”<sup>56</sup>.

Aquesta exempció de responsabilitat s'estén als prestadors de serveis que realitzen còpia temporal de les dades i les emmagatzemen en el seus sistemes automàticament, de manera provisional i sols per fer més eficient la seva transmissió, sempre que es compleixin els requisits establerts a la norma <sup>57</sup> . En el cas dels prestadors d'un servei d'intermediació consistent en acollir dades proporcionades pel destinatari del servei, o d'aquells que faciliten enllaços a continguts o instruments de recerca, tampoc seran responsables per la informació emmagatzemada a petició del destinatari, sempre que no tinguin coneixement efectiu que l'activitat o la informació emmagatzemada és il·lícita o que lesiona béns o drets d'un tercer susceptibles d'indemnització, o que si el tenen, actuïn amb diligència per retirar les dades o fer impossible accedir-hi. Això sempre que el destinatari del servei no estigui actuant sota la direcció, autoritat o control del prestador del servei d'intermediació<sup>58</sup>.

La presència de les tecnologies de l'ús de grans volums de dades en la nostra vida real és molt més habitual del que podem imaginar. Aspectes tan variats com la seguretat, la salut, l'educació,... ens presenten infinitat d'exemples de la necessitat de desenvolupar tecnologies de Big Data.

---

<sup>56</sup> Article 14 de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

<sup>57</sup> *Ibíd*em article 15.

<sup>58</sup> *Ibíd*em articles 15 16 i 17.

En l'àmbit de la seguretat, apareixen repetidament en la publicitat de les empreses que ofereixen protecció en les TIC, conceptes com Big Data estratègic, analítica processable, informàtica *in memory* i ecosistemes integrats són habituals. Els sistemes d'identificació basats en els trets biomètrics, utilitzen normalment Big Data. Per exemple, quan accedim a moltes de les actuals fronteres entre estats, ens identifiquem de forma documental, fotogràfica i biomètrica. En la majoria d'aquests casos estem interaccionant amb tecnologies de *Big Data*.

En salut, l'ús de grans volums de dades és cada vegada més freqüent, així podem veure cada vegada més experiències com la de l'Institut Català de la Salut, el qual, en col·laboració amb IBM, està desenvolupant un programa pilot per a l'assistència de pacients crònics complexos per mitjà de tecnologies de *Big Data*. Podem veure nombroses experiències en el mateix sentit d'orientar a la millora de la salut a partir del més eficient tractament de grans volums de dades mitjançant tecnologies Big Data.

Un d'aquests projectes és el de diagnòstic i tractament del càncer mitjançant l'aplicació d'aquestes tecnologies. Es tracta de localitzar marcadors específics en cada persona afectada de càncer i en cada tipus de tumor. També són cada vegada més freqüents els programes informàtics que, basats en tecnologia de l'ús de grans volums de dades, faciliten el tractament de grans volums d'informacions relacionades amb la millora de la salut de l'usuari. Així, aplicacions com Apixio faciliten l'accés als historials mèdics dels pacients a partir d'un motor de cerca basat en grans volums de dades.

El desenvolupament del genoma humà, els estudis de sèries històriques en els més variats camps, l'astrofísica, la biotecnologia,... són només alguns dels exemples en què el *Big Data* té una influència positiva i fonamental en la nostra societat. Tanmateix, no podem ignorar que les pròpies característiques de les tecnologies basades en Big Data presenten alguns riscos.

Pensem per exemple en els programes més o menys secrets d'espionatge a la població, com ara ECHELON, considerada la major xarxa d'espionatge i d'anàlisi de les comunicacions a nivell mundial, la qual no seria possible sense tecnologies del tipus del que representa *Big Data*. O pensem també en el poder de manipulació i influència subliminal que pot atorgar a qualsevol multinacional, el disposar d'eines amb les que pugui accedir a aquestes informacions. En definitiva, *Big Data* no és més que un altre instrument, una altra eina a la disposició de l'ésser humà. Saber utilitzar adequadament aquesta eina és, com sempre, el nostre repte i la nostra responsabilitat.



## **Capítol setè:**

### **Propietat intel·lectual de les obres**

---

#### **La protecció jurídica de la propietat intel·lectual**

La Declaració Universal dels Drets Humans, recull explícitament els drets de propietat intel·lectual dels autors en relació a les seves obres, en establir que "Tota persona té dret a la protecció dels interessos morals i materials que li corresponguin per raó de les produccions científiques, literàries o artístiques de què sigui autora"<sup>59</sup>. Aquesta Declaració té un caràcter no vinculant per als estats, però sí que és vinculant el Pacte Internacional de Drets Econòmics, Socials i Culturals, adoptat per l'Assemblea General de les Nacions Unides i signat per l'Estat espanyol, el qual estableix que "Els Estats Parts en aquest Pacte reconeixen el dret de tothom a: ... c) Beneficiar-se de la protecció dels interessos morals i materials que corresponguin per raó de les produccions científiques, literàries o artístiques de què sigui autora"<sup>60</sup>.

---

<sup>59</sup> Article 27.2 de la Declaració Universal dels Drets Humans, adoptada per Resolució 217 A (III), de l'Assemblea General de les Nacions Unides el 10 de desembre de 1948 a París.

<sup>60</sup> Article 15.1 del Pacte Internacional de Drets Econòmics, Socials i Culturals, adoptat i obert a la signatura, ratificació i adhesió per l'Assemblea General de les Nacions Unides en la Resolució 2200 A (XXI), de 16 de desembre de 1966 i que va entrar en vigor el 3 de gener de 1976. L'instrument de ratificació per l'Estat espanyol és del 13 d'abril de 1977, i va entrar en vigor el 27 juliol 1977.

Tant la Declaració Universal dels Drets Humans, com el Pacte Internacional de Drets Econòmics, Socials i Culturals, estan clarament dirigits a la protecció dels drets de les persones. En ambdós casos es fa referència específicament a la protecció dels drets dels autors sobre les seves obres, no només dels drets materials sinó també dels drets morals. La mateixa Organització Mundial de la Propietat Intel·lectual en definir aquesta propietat, la relaciona directament amb les creacions de la ment, és a dir, amb les de l'ésser humà: "La propietat intel·lectual (PI) es relaciona amb les creacions de la ment: invencions, obres literàries i artístiques, així com símbols, noms i imatges utilitzats en el comerç"<sup>61</sup>.

Tal com especifica l'Oficina Europea per als Drets d'Autor, la propietat intel·lectual té a veure amb les creacions de la ment: les invencions (patents), les obres literàries i artístiques, els símbols, els noms, les imatges i els dibuixos i models utilitzats en el comerç. Aquesta Oficina diferencia entre les dues grans categories protegides que constitueixen la propietat Intel·lectual: els drets d'autor, i la propietat industrial. El dret d'autor, abasta "les obres literàries i artístiques, com ara les novel·les, els poemes i les obres de teatre, les pel·lícules, les obres musicals, les obres d'art, com ara els dibuixos, pàgines web, pintures, fotografies i escultures, i els dissenys arquitectònics". També s'inclouen aquí els drets relacionats amb el dret d'autor, és a dir, "els drets dels artistes intèrprets o executants sobre les seves interpretacions o execucions, els drets dels productors de fonogrames sobre els seus enregistraments i els drets dels organismes de radiodifusió sobre els

---

<sup>61</sup> L'Organització Mundial de la Propietat Intel·lectual (OMPI) és un organisme de les Nacions Unides dedicat a fomentar l'ús i la protecció de les obres de l'intel·lecte humà. Es poden consultar les seves activitats i plantejaments a la seva pàgina web: <http://www.wipo.int/about-ip/es/>



seus programes de ràdio i de televisió”. D'altra banda, “la propietat industrial, que inclou les invencions (patents), marques, dibuixos i models industrials i indicacions geogràfiques d'origen”<sup>62</sup>.

Encara que tant la legislació com la jurisprudència en general, s'orienten en dotar d'una certa protecció als drets d'autor, en tots els casos s'assumeix que aquests drets corresponen a persones i es relacionen amb obres realitzades per persones. L'aparició de les noves tecnologies de la informació, i molt especialment d'Internet, no fa variar aquesta concepció. Encara que internet representa noves formes de presentació dels continguts i noves amenaces als drets autor i dels de propietat intel·lectual, l'autoria de les obres segueix considerant alguna cosa exclusivament vinculat a les persones.

És important la distinció entre els drets morals i els materials sobre les obres. De fet, la part patrimonial dels drets d'autor és transferible, cosa que no succeeix amb els drets morals. Un autor té dret que es reconegui sempre la seva autoria, així com a oposar-se a les modificacions que se'n vulgui fer en tot allò que pugui afectar la reputació de l'autor, amb independència de qui posseeixi en un moment determinat la propietat intel·lectual de l'obra:

“... Independentment dels drets patrimonials de l'autor, i fins i tot després de la cessió d'aquests drets, l'autor conservarà el dret de reivindicar la paternitat de l'obra i d'oposar-se a qualsevol deformació, mutilació o una altra modificació de

---

<sup>62</sup>.Extret de la pàgina web corporativa de l'Oficina Europea per als Drets d'Autor. Pot consultar-se en <http://www.eucopyright.com>.

l'obra o a qualsevol atemptat a la mateixa que causi perjudici al seu honor i reputació..."<sup>63</sup>

El Conveni de Berna<sup>64</sup> és el conveni per a la Protecció de les Obres Literàries i Artístiques seguit pels estats signants, entre els quals es troba l'Estat espanyol. Aquesta protecció pot arribar a aspectes merament administratius, o fins i tot responsabilitats penals.

Així, la protecció penal de la propietat intel·lectual, ve recollida en la secció primera del capítol XI del Codi Penal, dedicat als delictes relatius a la propietat intel·lectual i industrial, al mercat i als consumidors. En la seva secció primera, dedicada específicament a aquests delictes, s'especifiquen les activitats considerades punibles penalment limitant-les a aquells casos en què hi hagi ànim de lucre i es perjudiqui un tercer<sup>65</sup>:

"... Serà castigat amb la pena de presó de sis mesos a dos anys i multa de 12 a 24 mesos qui, amb ànim de lucre i en perjudici de tercer, reproduueixi, plagii, distribueixi o comuniqui públicament, en tot o en part, una obra literària, artística o científica, o la seva transformació, interpretació o execució artística fixada en qualsevol tipus de suport o comunicada a

---

<sup>63</sup> Article 6bis.1 del Conveni per a la Protecció de les Obres Literàries i Artístiques, signat a Berna, Suïssa, el 9 de setembre de 1886, incloent les revisions i afegits posteriors. L'article es refereix específicament als drets morals dels autors.

<sup>64</sup> Conveni per a la Protecció de les Obres Literàries i Artístiques, signat a Berna, Suïssa, el 9 de setembre de 1886, completat en París el 4 de maig de 1896, revisat en Berlín el 13 de novembre de 1908, completat en Berna el 20 de març de 1914 i revisat a ROMA el 2 de juny de 1928, en Brussel·les el 26 de juny de 1948, a Estocolm el 14 de juliol de 1967 a PARIS el 24 de juliol de 1971 i esmenat el 28 setembre 1979.

<sup>65</sup> Article 270.1 de la Llei Orgànica 10/1995, de 23 de novembre, del Codi Penal.

través de qualsevol mitjà, sense l'autorització dels titulars dels corresponents drets de propietat intel·lectual o dels seus cessionaris..."<sup>66</sup>.

La protecció penal de la propietat intel·lectual s'estén a qualsevol obra literària, artística o científica, però perquè la infracció es pugui considerar delictu ha de donar-se un perjudici a tercer i l'existència d'ànim de lucre. L'ànim de lucre és doncs un element fonamental del tipus penal bàsic, tal com recull repetidament la jurisprudència en nombroses sentències:

"... ànim de lucre, descrit en la jurisprudència d'aquesta Sala com «qualsevol avantatge, profit, benefici o utilitat que es proposi obtenir el reu amb la seva antijurídica conducta» (SSTS 722/99 de 6.5, 523/98 de 24.3.99), sent suficient per estimar en l'autor l'existència d'aquest element de l'injust, donada la seva àmplia interpretació que preval al sospesar l'específica intenció lucrativa, la cooperació culpable al lucre aliè, en no ser necessari un lucre propi, n'hi ha prou que sigui per beneficiar a un tercer SSTS. 629/2002 de 13.3, 287/2000 de 20.2, 577/2002 de 8.3, 238/2003 de 12.2, 348/2003 de 12.3, 28.11.2000 que referida a un delictu d'estafa necessita que no requereix que l'autor persegueixi el

---

<sup>66</sup> La Llei Orgànica 5/2010, de 22 de juny, per la qual es modifica el Codi Penal, va afegir un paràgraf a l'article 270.1 d'aquest Codi, introduint un element de proporcionalitat en delimitar els supòsits en què la infracció sigui lleu: "No obstant això, en els casos de distribució al detall, ateses les característiques del culpable i la reduïda quantia del benefici econòmic, sempre que no concorri cap de les circumstàncies de l'article següent, el jutge pot imposar la pena de multa de tres a sis mesos o treballs en benefici de la comunitat de trenta-un a seixanta dies. En els mateixos supòsits, quan el benefici no excedeixi de 400 euros, es castigarà el fet com a falta de l'article 623.5".

seu propi i definitiu enriquiment. Per contra, en aquest delictes l'ànim de lucre també és d'apreciar quan l'avantatge patrimonial antijurídica es persegueix per després beneficiar a un altre..."<sup>67</sup>.

No obstant això, fora de l'àmbit penal, aquesta exigència d'ànim de lucre no és un condicionant necessari per a l'existència d'infracció als drets de propietat intel·lectual. A l'Estat espanyol els drets d'autor es recullen especialment en el Reial Decret Legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de Propietat Intel·lectual, regularitzant, aclarint i harmonitzant les disposicions legals vigents en la matèria<sup>68</sup>. Posteriorment s'han anat incorporant a la legislació les diferents directives europees.

La generalització de les noves tecnologies i l'ús cada vegada més gran d'internet, han fet sorgir nous plantejaments en relació a la propietat intel·lectual, tendint a una major liberalització. Així, una llicència *Copyleft* permet que una obra pugui ser distribuïda, modificada, copiada lliurement o comercialitzada previ permís de l'autor<sup>69</sup>. Un altre sistema és el de les llicències *Creative Commons* permeten quatre tipus d'ús de les obres llicenciades:

- a) atribució: permet qualsevol ús de l'obra, respectant els drets morals de l'autor;

---

<sup>67</sup> Sentència núm. 416/2007 de 23 maig, de la Secció 1a de la Sala 2a Penal del Tribunal Suprem.

<sup>68</sup> Text refós de la Llei de Propietat Intel·lectual aprovada pel Reial Decret Legislatiu 1/1996, de 12 d'abril.

<sup>69</sup> Podeu consultar els diferents tipus de Copyleft a la pàgina web del Sistema Operatiu GNU, que defensa la llibertat de distribuir i modificar el programari mitjançant llicències Copyleft: <http://www.gnu.org/licenses/licenses.ca.html>

- b) compartir-igual: permet obres derivades de l'original mitjançant el mateix tipus de llicència que tingui aquell;
- c) no ús comercial: exclou l'ús amb finalitats comercials;
- d) no obres derivades: no permet cap modificació de l'obra<sup>70</sup>.

Cal destacar que entre els formats existents per expressar el tipus de llicència d'una obra, hi ha el *Digital Code*: un codi digital, presentat de manera que pugui ser llegit directament per una màquina, el que permet que els motors de cerca i altres aplicacions identifiquin l'obra i les seves condicions d'ús.

## Propietat de les obres no creades per persones

"... L'Oficina de Copyright dels Estats Units es negarà a registrar una reclamació en una obra que hagi estat creada a través de l'operació d'una màquina o procés sense cap interacció humana, inclòs si el disseny és generat aleatòriament..."<sup>71</sup>.

Aquesta negativa a reconèixer drets d'autor a les obres realitzades per màquines, es basa precisament en la necessitat que aquesta obra sigui el producte de la creació humana. La no participació de cap ésser humà en aquesta creació impossibilita el reconeixement d'uns drets que no són

---

<sup>70</sup> Creative Commons és una corporació americana sense ànim de lucre, que té com a institució afiliada a Creative Commons Espanya a la Universitat de Barcelona. Pot consultar-se les finalitats i el funcionament d'aquest tipus de llicències a <http://creativecommons.org/>

<sup>71</sup> Pàgina 577 del Compendi de pràctiques de copyright als Estats Units. Es tracta de l'esborrany de la tercera edició, editat a l'agost de 2014, per l'Oficina de Copyright dels Estats Units.

atribuïbles a cap màquina, com tampoc ho són les obres realitzades per animals o per qualsevol objecte inanimat o animat de qualsevol tipus. En aquest sentit, destaca la negativa a reconèixer drets d'autor a una autofoto, el que sovint s'anomena *selfie*, per part d'un mico.

El 2011, el fotògraf britànic David Slater estava viatjant per la selva d'Indonèsia quan un macaco va agafar la seva càmera i es va autofotografiar. Aquesta "*selfie*" va ser publicada per una tercera persona a *Wikipedia Commons* com si fos de domini públic. Slater va presentar una reclamació adduint que les imatges li pertanyien a ell, però l'Oficina del Copyright Nord-americana va dictaminar que els treballs produïts per la natura, els animals o les plantes no tenen drets d'autor i, per tant, va denegar el registre reclamat pel fotògraf, ja que l'obra no va ser realitzada per cap ésser humà, i la protecció dels drets d'autor es refereixen únicament a les concepcions intel·lectuals originals realitzades per un creador humà.

Per tal de deixar totalment clara la seva posició davant de reclamacions com la de David Slater, l'Oficina del *Copyright* va recollir entre els exemples específicament esmentats en el compendi de pràctiques de copyright, el cas de les fotografies preses per micos. De la mateixa manera, en aquest mateix compendi s'especifica que "l'Oficina no registrarà les obres produïdes per una màquina o un simple procés mecànic que operi a l'atzar o de forma automàtica sense cap tipus d'aportació creativa o la intervenció d'un autor humà"<sup>72</sup>.

Així doncs, l'Oficina del Copyright dels Estats Units no admet drets d'autor sobre obres que no siguin realitzades per éssers humans, ni tan

---

<sup>72</sup> Pàgina 55 del Compendi de pràctiques de copyright dels Estats Units.

sols es reconeixen aquests drets a les obres creades per la Divinitat, o per mitjans sobrenaturals. Només es permet el registre si l'obra es presenta com d'inspiració divina, però l'autor que rebí la inspiració divina ha de ser en tot cas un ésser humà:

"... L'Oficina de Copyright dels EUA registrarà una obra original d'un autor, sempre que l'obra fos creada per un ésser humà.

La llei de drets d'autor només protegeix «els fruits del treball intel·lectual» que «es basi en els poders creatius de la ment». *Trade-Mark Cases*, 100 US 82, 94 (1879). Com que la llei de drets d'autor es limita a «concepcions intel·lectuals originals de l'autor», l'Oficina es negarà a registrar una reclamació si determina que un ésser humà no va crear l'obra. *Burrow-Giles: Lithographic Co. v. Sarony*, 111 US 53, 58 (1884).

L'Oficina no registrarà obres produïdes per la natura, els animals o les plantes. Així mateix, l'Oficina no pot registrar una obra suposadament creada per éssers divins o sobrenaturals, tanmateix, l'Oficina podrà registrar una obra quan en la sol·licitud o en la còpia(es) de dipòsit s'estableixi que el treball va ser inspirat per un esperit diví..."<sup>73</sup>.

La posició de l'Oficina del Copyright dels Estats Units respecte als drets d'autor és doncs meridiana, fins al punt que en el compendi de pràctiques de *copyright* s'especifica que ni en el cas que un ésser Diví pretengués registrar una obra creada directament per Ell, aquesta no seria acceptada en no ser producte de la creació intel·lectual d'un ésser

---

<sup>73</sup> Pàgina 54 del Compendi de pràctiques de copyright dels Estats Units.

humà. Aquest plantejament és molt similar en el dret anglosaxó i en el dret continental. No obstant això, en els dos casos hi ha algunes diferències significatives en la concepció d'origen de la propietat intel·lectual.

Mentre que en el dret anglosaxó la protecció jurídica se centra en l'obra i en tot el que pot succeir amb ella, és a dir, en el *copyright*, en el dret continental aquesta protecció es dirigeix específicament a l'autor, és a dir, als drets d'autor. Els efectes pràctics d'aquesta diferent concepció són escassos en la pràctica, però hi ha alguns de significatius. En el cas dels drets d'autor nord-americà s'admet el registre com a autor d'obres realitzades per una persona tant física com jurídica, ja que el fonament de la protecció és essencialment econòmic, mentre que en el cas continental els drets d'autor només són atribuïbles a persones físiques, ja que es tracta d'un dret vinculat a la personalitat de l'autor (Loredo, 2006).

## **Drets d'autor en l'entorn europeu**

En principi, la Llei estableix drets d'autor exclusivament per a les persones. Només les persones poden ser creadores i, per tant, ser objecte de protecció jurídica dels seus drets sobre les obres creades per ells. Fins i tot, en els casos en què l'obra hagi estat creada per diversos autors, els drets d'autor són atribuïts a persones concretes. Així, en el cas de les obres realitzades per diversos autors en col·laboració, els drets d'autor corresponen a tots ells.



En el cas de les obres col·lectives, és a dir, aquelles construïdes a partir de les aportacions de diferents autors sense que es pugui discernir quina part correspon a cadascun, els drets corresponen a qui l'editi o divulgui sota el seu nom, llevat que s'hagi acordat prèviament un pacte en sentit contrari:

"... Es considera obra col·lectiva la creada per la iniciativa i sota la coordinació d'una persona natural o jurídica que l'edita i divulga sota el seu nom i està constituïda per la reunió d'aportacions de diferents autors la contribució personal es fon en una creació única i autònoma, per a la qual hagi estat concebuda sense que sigui possible atribuir separatament a qualsevol d'ells un dret sobre el conjunt de l'obra realitzada.

Llevat de pacte en contra, els drets sobre l'obra col·lectiva correspondran a la persona que l'editi i divulgui sota el seu nom..."<sup>74</sup>.

Aquestes situacions, però, no recullen aquells casos en què l'obra no hagi estat realitzada per una o diverses persones, sinó per un animal, un objecte inanimat o més específicament per una màquina. La incorporació de tècniques d'intel·ligència artificial a les noves tecnologies permeten la creació d'obres sense la intervenció d'éssers humans, pel que es planteja la titularitat dels drets d'autor quan l'obra ha estat realitzada per una màquina.

---

<sup>74</sup> Article 8 de la Llei de Propietat Intel·lectual, el text refós del qual va ser aprovat pel Reial Decret Legislatiu 1/1996, de 12 d'abril, regularitzant, aclarint i harmonitzant les disposicions legals vigents sobre la matèria.

A Europa, la llei concedeix la protecció del dret d'autor a les persones físiques, si bé en alguns casos pot reconèixer també a les persones jurídiques la propietat intel·lectual de l'obra. Aquest seria el cas, per exemple, dels programes d'ordinador creats per diverses persones:

"... 1. Es considerarà autor del programa d'ordinador a la persona física o grup de persones físiques que l'hagin creat o, quan la legislació dels estats membres ho permeti, a la persona jurídica que sigui considerada titular del dret per aquesta legislació.

Quan la legislació d'un Estat membre reconegui les obres col·lectives, la persona física o jurídica que segons aquesta legislació hagi creat el programa, es considerarà el seu autor.

2. Quan un programa d'ordinador es creu conjuntament per diverses persones físiques, els drets exclusius seran propietat comuna.

3. Quan un treballador assalariat creï un programa d'ordinador en l'exercici de les funcions que li han estat confiades, o seguint les instruccions del seu empresari, la titularitat dels drets econòmics corresponents al programa d'ordinador així creat correspondran, exclusivament, a l'empresari, llevat de pacte en contra..."<sup>75</sup>.

A Europa s'ha desenvolupat una àmplia normativa sobre drets d'autor. Algunes de les directives més conegudes sobre el tema són la Directiva

---

<sup>75</sup> Article 2 de la Directiva 2009/24/CE del Parlament Europeu i del Consell, de 23 d'abril de 2009, sobre la protecció jurídica dels programes d'ordinador.

2001/29/CE del Parlament Europeu i el Consell, de 22 de maig de 2001, relativa a l'harmonització de determinats aspectes dels drets d'autor i drets afins als drets d'autor en la societat de la informació, i la Directiva 2004/48/CE del Parlament Europeu i del Consell, de 29 d'abril de 2004, relativa a les mesures i procediments destinats a garantir el respecte dels drets de propietat intel·lectual.

A part d'aquestes directives, són nombroses les promulgades per harmonitzar diferents aspectes relatius al tema. Aquestes directives abasten:

- la protecció de les bases de dades<sup>76</sup>;
- la prohibició de les targetes intel·ligents i altres dispositius que permetin burlar l'accés protegit a serveis de pagament de televisió, ràdio i internet<sup>77</sup>;
- la radiodifusió d'obres via satèl·lit o mitjançant distribució per cable<sup>78</sup>;
- el termini de durada dels drets d'autor protegits<sup>79</sup>;
- el dret de participació en benefici de l'autor d'una obra d'art original<sup>80</sup>;

---

<sup>76</sup> Directiva 96/9/CE del Parlament Europeu i del Consell, d'11 de març de 1996, sobre la protecció jurídica de les bases de dades.

<sup>77</sup> Directiva 98/84/CE del Parlament Europeu i del Consell, de 20 de novembre de 1998, relativa a la protecció jurídica dels serveis d'accés condicional o basats en aquest accés.

<sup>78</sup> Directiva 93/83/CEE del Consell, de 27 de setembre de 1993, sobre coordinació de determinades disposicions relatives als drets d'autor i drets afins als drets d'autor en l'àmbit de la radiodifusió via satèl·lit i de la distribució per cable.

<sup>79</sup> Directiva 2006/116/CE del Parlament Europeu i del Consell, de 12 de desembre de 2006, relativa al termini de protecció del dret d'autor i de determinats drets afins.

- la gestió col·lectiva dels drets d'autor<sup>81</sup>;
- els drets de lloguer i préstec en l'àmbit de la propietat intel·lectual<sup>82</sup>;
- altres similars relacionades amb la protecció industrial, les marques, i la protecció intel·lectual en general.

## Drets de copyright en l'entorn anglosaxó

Des del dret anglosaxó es va popularitzar el terme *copyright*, per definir el dret exclusiu d'algú a explotar una obra literària, científica o artística, durant un temps determinat. És a dir, els drets materials sobre una obra poden correspondre a algú diferent del propi autor.

Tal i com s'ha comentat anteriorment, l'Oficina de Copyright dels Estats Units<sup>83</sup> no admet el registre d'obres realitzades per una màquina o mitjançant un procés mecànic aleatori o automàtic sense la intervenció de l'ésser humà. Fins i tot quan intervé una persona en alguna fase del procés, no s'admet el registre de l'obra si no hi ha una participació

---

<sup>80</sup> Directiva 2001/84/CE del Parlament Europeu i del Consell, de 27 de setembre de 2001, relativa al dret de participació en benefici de l'autor d'una obra d'art original.

<sup>81</sup> Directiva 2014/26/UE del Parlament Europeu i del Consell, de 26 febrer de 2014, relativa a la gestió col·lectiva dels drets d'autor i drets afins i a la concessió de llicències multiterritorials de drets sobre obres musicals per a la seva utilització en línia en el mercat interior.

<sup>82</sup> Directiva 2006/115/CE del Parlament Europeu i del Consell, de 12 de desembre de 2006, sobre drets de lloguer i préstec i altres drets afins als drets d'autor en l'àmbit de la propietat intel·lectual.

<sup>83</sup> L'Oficina de Copyright dels Estats Units és un Departament de la Biblioteca del Congrés. Aquest Departament té la responsabilitat sobre el Registre de Drets d'Autor a Estats Units i l'acompliment de totes les tasques relacionades amb aquest registre.

pròpiament de creació intel·lectual. Com exemples d'obres que l'Oficina no registrarà tenim:

"... Exemples:

- Reduir o ampliar la mida d'una obra d'autor, preexistent.
- Realitzar canvis en una obra d'autor preexistent, dictats per requisits de fabricació o de materials.
- Convertir un treball analògic a format digital, així com transferir una pel·lícula de VHS a DVD.
- Depurar o reduir el soroll en un enregistrament sonor preexistent, o convertir una gravació de so estèreo a so monoaural.
- La transposició d'una cançó de Si major a Do major.
- Les imatges mèdiques produïda pels raigs X, ultrasons, ressonància magnètica, o un altre equip de diagnòstic.
- L'acció basada en un procés de confecció mecànica que produeixi aleatòriament formes irregulars, sense cap patró discernible..."<sup>84</sup>

La Llei de drets d'autor dels Estats Units és la Llei de *copyright* que va entrar en vigor l'1 de gener de 1978, la qual va substituir la llei anterior de 1909. Aquesta llei protegeix els drets sobre les "obres originals d'autor". El títol 17 del codi legislatiu dels Estats Units (17 USC § 102 a), així com els seus reglaments d'aplicació i precedents legals

---

<sup>84</sup> Pàgina 55 del Compendi de pràctiques de copyright als Estats Units. Es tracta de l'esborrany de la tercera edició, editat a l'agost de 2014, per l'Oficina de Copyright dels Estats Units.

corresponents<sup>85</sup> estableix específicament les obres protegides, i aclareix que aquesta protecció es refereix a les obres originals realitzades per un creador, i no a possibles idees, conceptes, mètodes o aspectes similars:

"... La protecció de copyright subsisteix, de conformitat amb el present títol, en les obres d'autor originals presentades en qualsevol suport d'expressió tangible, coneguda en l'actualitat o desenvolupada posteriorment, a partir de la qual puguin percebre's, reproduir-se o comunicar-se d'una altra manera, ja sigui directament o amb l'ajuda d'una màquina o dispositiu. Les obres d'autor protegides inclouen les següents categories:

1. obres literàries;
2. obres musicals, incloses possibles textos que les acompanyen;
3. obres dramàtiques, incloent qualsevol acompanyament musical;
4. pantomimes i obres coreogràfiques;
5. obres gràfiques i obres escultòriques o pictòriques;
6. pel·lícules cinematogràfiques i altres obres audiovisuals;
7. enregistraments sonors;
8. obres arquitectòniques.

En cap cas la protecció dels drets d'autor d'una obra original d'un autor s'estén a cap idea, procediment, procés, sistema, mètode d'operació, concepte, principi o descobriment,

---

<sup>85</sup> El Codi Legislatiu dels Estats Units és la compilació oficial i la codificació de les lleis federals generals i permanents dels Estats Units d'Amèrica.

independentment de la forma en què es descrigui, expliqui, il·lustri o inclogui en aquest treball..."

Però en tots aquests casos, el reconeixement de drets d'autor es refereix sempre a autors humans. Tal i com s'ha comentat anteriorment, l'Oficina del *copyright* dels Estats Units no només nega la inscripció de drets d'autor a les obres literàries no realitzades per éssers humans, sinó que aquesta mateixa circumstància es dóna respecte a qualsevol altra obra o expressió artística realitzada per animals, màquines, o altres objectes, animats o inanimats.

Per qualificar com una obra d'autor un treball coreogràfic, aquest ha de ser creat per un ésser humà i tenir per objecte la seva execució per éssers humans. Així per exemple, les danses realitzades o destinades a ser realitzades per animals, màquines, o altres objectes, animats o inanimats, no tenen drets d'autor i no poden ser registrades a l'Oficina de Copyright<sup>86</sup>. El mateix succeeix amb les pantomimes:

"... Per qualificar com una obra d'autor una pantomima, aquesta s'ha de referir «una pantomima real de l'home real» *Kalem*, 222 US en 61-62. Les pantomimes realitzades per animals, robots, màquines, o qualsevol altre objecte, animat o inanimat, no tenen drets d'autor i no poden ser registrades a l'Oficina de Copyright..."<sup>87</sup>

---

<sup>86</sup> Pàgina 514 del Compendi de pràctiques del copyright dels Estats Units, editat a l'agost de 2014, per l'Oficina de Copyright dels Estats Units.

<sup>87</sup> *Ibidem*. pàgina 527.





## Capítol vuitè: La responsabilitat dels intermediaris

---

### Límits a la responsabilitat del proveïdor de serveis

S'acostuma a definir als que faciliten l'accés a Internet com ISP per les sigles en anglès *Internet Service Provider*. Un altre tipus de serveis són els oferts pels proveïdors de continguts així com les que permeten que els usuaris pugin continguts a la xarxa, denominades en general *Hosting ISP*. Podem trobar en aquest àmbit nombrosos tipus de Serveis diferents, com ara els *Farm Servers*; els *Mirrors*; els *Content Distribution Networks*; les Xarxes *Peer-to-peer*,... a la pràctica s'acostuma a referir com a ISP la majoria de serveis que faciliten d'alguna manera la navegació per Internet.

La quantitat de dades que gestionen, i les pròpies característiques del servei prestat pels intermediaris en la societat de la informació, fa inviable la possibilitat d'una supervisió prèvia de les dades que transmetin o que emmagatzemin els usuaris a través dels seus serveis. La pròpia legislació recull aquesta situació, establint la negativa a establir una obligació general en aquest sentit.

Per tal de clarificar la normativa sobre aquest tema es va publicar la Directiva 2000/31/CE del Parlament Europeu i del Consell, de 8 de juny de 2000, relativa a determinats aspectes jurídics dels serveis de la

societat de la informació, en particular el comerç electrònic en el mercat interior. A la secció quarta del capítol segon d'aquesta directiva, es va establir el règim de responsabilitat dels prestadors de serveis que actuen com a intermediaris de la societat de la informació. En aquesta directiva s'estableix que:

"... Els estats membres no han d'imposar als prestadors de serveis una obligació general de supervisar les dades que transmetin o que emmagatzemin, ni una obligació general de fer cerques actives de fets o circumstàncies que indiquin activitats il·lícites, respecte dels serveis previstos en els articles 12, 13 i 14..."<sup>88</sup>.

Des d'una perspectiva exclusivament legal, els límits de la responsabilitat dels prestadors de serveis a Internet (ISP) estan definits en el marc legal actual. Així per exemple, en el cas espanyol, la Llei 34/2002, de 11 de juliol, de serveis de la societat de la informació i de comerç electrònic, dedica la seva segona secció a establir el règim de responsabilitat dels prestadors dels serveis de la societat de la informació. En aquesta norma legal se situa el límit de la responsabilitat d'aquests prestadors de serveis, en el fet que no tinguin coneixement efectiu de la il·licitud o perjudici dels continguts en qüestió, o, si s'escau que actuïn diligentment per suprimir aquest contingut o l'enllaç corresponent.

És clar que el legislador es refereix tant als prestadors de serveis que des de la seva pàgina web allotgin continguts de tercers com als que des d'ella facilitin enllaços a continguts allotjats en altres pàgines. Així,

---

<sup>88</sup> Apartat 1 de l'article 15 de la Directiva 2000/31/CE del Parlament Europeu i del Consell, de 8 de juny de 2000.

l'article 16 d'aquesta llei es refereix explícitament als que alberguen dades proporcionades pel destinatari del servei i l'article 17, amb un redactat similar, ho fa en relació als que facilitin enllaços a continguts, directoris o instruments de cerca.

El mateix o semblant plantejament es recull en la majoria de les legislacions europees i nord-americanes. Aquesta homogeneïtat en els plantejaments legislatius de països diferents, no fa sinó recollir les directives i recomanacions internacionals. Així, per exemple, la Directiva 2000/31/CE del Parlament Europeu i del Consell, sobre allotjament de dades recull que:

"... Els estats membres han de garantir que, quan es presti un servei de la societat de la informació consistent en emmagatzemar dades facilitades pel destinatari del servei, el prestador de serveis no pugui ser considerat responsable de les dades emmagatzemades a petició del destinatari, a condició que: a) el prestador de serveis no tingui coneixement efectiu que l'activitat o la informació és il·lícita i, pel que es refereix a una acció per danys i perjudicis, no tingui coneixement de fets o circumstàncies pels quals l'activitat o la informació reveli el seu caràcter il·lícit, o que, b) quan tingui coneixement d'aquests punts, el prestador de serveis actuï amb promptitud per retirar les dades o fer que l'accés a ells sigui impossible..."<sup>89</sup>.

---

<sup>89</sup> Article 14 de la Directiva de la UE 2000/31, d'11 de juliol, sobre allotjament de dades.

## Un concepte d'interpretació confusa

La interpretació jurídica de la responsabilitat dels prestadors de serveis que actuen com a intermediaris de la societat de la informació no és una cosa invariable i perfectament definida. Podem comprovar divergències en la interpretació, fins i tot en un mateix país i pels mateixos fets. Així, per exemple, la sentència de 12 de juliol de 2012, de la Cort de Cassació francesa, va revocar la sentència d'apel·lació de 3 de maig de 2011 que exculpava al cercador Google de l'acusació de violar els drets d'autor, per suggerir les paraules "torrent", "megaupload" o "rapidshare" mitjançant l'anomenada "funció autocompletar" en determinades recerques de músiques o d'artistes realitzades pels usuaris.

El tribunal d'apel·lació va opinar que dirigir els usuaris cap a uns llocs especialitzats en emmagatzematge de fitxers que els usuaris poden descarregar, fins i tot infringint possibles drets d'autor, no implica responsabilitat per al navegador. Per al tribunal les pàgines de descàrregues no són il·lícites en si mateixes, ja que la responsabilitat per un ús fraudulent és en tot cas dels usuaris i no del lloc que conté els fitxers en qüestió. Des d'aquesta perspectiva, no es pot condemnar Google per suggerir l'accés a llocs que no són il·legals en si mateixos, llocs que, d'altra banda, seguirien contenint els fitxers en qüestió encara que Google no dirigís als usuaris cap a ells.

Aquesta interpretació va ser qüestionada posteriorment per la cort de cassació per no ajustar-se a dret en opinió d'aquesta Cort. Des d'aquesta nova interpretació el simple fet de suggerir als usuaris l'accés a pàgines des de les quals poden descarregar obres protegides pels drets d'autor constitueix una activitat que facilita aquesta infracció. Així doncs, s'opina

que Google proporciona els mitjans que faciliten l'accés a aquestes pàgines i, per tant, a que es cometi la infracció.

S'afegeix en aquest cas que era adequada la petició que Google suprimís l'associació automàtica amb unes paraules clau, ja que amb això es dificultaria l'accés als continguts protegits i, per tant, contribuiria a evitar la infracció. Per això la Cort torna el cas per seguir el procediment en la fase d'apel·lació.

Veiem com mentre que per a un tribunal no existeix responsabilitat, per l'altre hi ha una col·laboració que facilita la infracció, tant en orientar a l'usuari com al no suprimir aquesta orientació.

En plantejar la responsabilitat dels prestadors de serveis a la societat de la informació, són nombrosos els exemples que podem trobar d'interpretació contradictòria d'un mateix cas per part de diferents òrgans jurisdiccionals. Un cas just al revés de l'esmentat de Google França el podem veure a la sentència dictada el 2010 per part del Tribunal Suprem espanyol<sup>90</sup>, en la qual l'alt tribunal va estimar el recurs de cassació plantejat per Ruboskizo, S.L. que havia estat condemnada per intromissió il·legítima en l'honor de les persones.

El Jutjat de Primera Instància número 23 de València havia considerat en sentència de 30 de novembre de 2006 que Ruboskizo, S.L. havia incorregut en responsabilitat en la seva qualitat de titular d'una pàgina web (www.quejasonline.com) en què un usuari havia exposat uns comentaris ofensius per Mutua Madrileña Automobilista, fent-se passar per un advocat descontent d'aquesta entitat. Davant la demanda de

---

<sup>90</sup> Sentència 316/2010, de 18 de maig dictada per la Sala primera del Civil, del Tribunal Suprem.

l'advocat la personalitat del qual havia estat suplantada, el Jutjat de Primera Instància número 23 de València va apreciar que la demandada havia comès una intromissió il·legítima en l'honor del primer per la publicació del seu nom, tot i que el demandat havia retirat de la seva pàgina web la nota motiu de la demanda tan aviat com va ser requerit a fer-ho pel demandant.

Aquesta apreciació de responsabilitat va ser posteriorment ratificada per l'Audiència Provincial de València<sup>91</sup>. D'altra banda, i amb anterioritat a aquestes actuacions, s'havia instat per part del demandant la iniciació d'un procediment penal, el qual es va acabar amb l'arxiu de les actuacions, davant la impossibilitat de conèixer l'infractor i, per tant, des del àmbit penal no es va apreciar responsabilitat del demandat.

El Tribunal Suprem, va estimar en la seva sentència la no existència de responsabilitat per part del prestador del servei (en aquest cas Ruboskizo, S.L.) per la qual cosa va deixar sense efecte la sentència del Jutjat de Primera Instància número 23 de València, així com la de la Secció Sisena de l'Audiència Provincial de la mateixa comunitat. L'argument principal del Tribunal Suprem va ser que Ruboskizo, S.L. no coneixia, ni va poder conèixer raonablement, tant directament com indirectament, que s'estava utilitzant indegudament el nom del demandat amb l'ànim de perjudicar. Afegeix l'alt tribunal que no es pot al·legar negligència, atès que tan aviat com va rebre el requeriment del perjudicat va retirar el comentari de la seva pàgina web:

---

<sup>91</sup> Sentència dictada, el dia 29 de juny de 2007, per la Secció Sisena de l'Audiència Provincial de València, en la que va resoldre el recurs d'apel·lació número 138/2007 provenint de la interlocutòria número 627/2006 del Jutjat de Primera Instància número 23 de València.

"... En la sentència de 9 de desembre de 2.009 ens pronunciem sobre la interpretació d'aquest article 16 (de la Llei 34/2002, de 11 de juliol, de serveis de la societat de la informació i de comerç electrònic) d'acord amb la Directiva 2.000/31/CE, pel que fa al coneixement efectiu, a l'absència de la qual es condiona, en un dels supòsits, l'alliberament de responsabilitat de la prestadora de serveis d'allotjament per la informació emmagatzemada a petició del destinatari d'aquells.

Doncs bé, l'Audiència Provincial no ha tingut en compte aquest conjunt normatiu en declarar la responsabilitat de la demandada Ruboskizo, S.L. i, per això, no ha extret cap conseqüència que aquesta societat no conegués ni pogués conèixer raonablement, directament o a partir de dades aptes per possibilitar l'aprehensió de la realitat, que qui li subministrava el contingut lesiu per al demandant no era ell, sinó una altra persona que utilitzava indegudament el seu nom amb l'ànim de perjudicar; ni que, coneixedora amb posterioritat d'aquesta realitat, gràcies al requeriment del perjudicat, retirés el comentari sense titllar-ho de negligència..."<sup>92</sup>.

La sentència recull els continguts de la Directiva 2000/31/CE del Parlament Europeu i del Consell, de 8 de juny de 2000, la qual es va elaborar en un entorn d'evidents divergències existents fins llavors en aquest tema, tant entre les normes legals dels diferents estats membres, com en la seva interpretació per part de la jurisprudència. La directiva delimitava el règim de responsabilitat dels prestadors de serveis

---

<sup>92</sup> Fonament jurídic segon de la sentència 316/2010, de 18 de maig, de la Sala Primera del Tribunal Suprem.

que actuen com a intermediaris de la societat de la informació<sup>93</sup>. Aquesta directiva, en el seu article 15, explicita que els estats no poden imposar als prestadors de serveis una obligació general de supervisar les dades allotjades per tercers.

## Principi de solidaritat entre responsables del dany

A la pràctica els tribunals han consolidat l'atribució de responsabilitat no només a l'autor material del fet, sinó també, i de manera solidària, als que podent fer alguna cosa per evitar el mal no ho van fer. Tal com assenyala Gómez Ligüerre:

"... Tot i l'absència d'una regla sobre això en el Codi civil i de les limitacions imposades a la solidaritat en els articles 1137-1148 Cc., la jurisprudència civil, i de forma molt assenyada la Sala Primera del Tribunal Suprem, no ha tingut inconvenient a responsabilitzar de forma solidària als qui, de forma més o menys directa, van poder fer alguna cosa per evitar el dany..."  
(Gómez, 2005).

Als Estats Units, la responsabilitat per fet aliè a Internet, s'aborda des de la doctrina de *Vicarious Liability* i de la de *Contributory Infringement*. La primera implica responsabilitat dels ISP en infraccions a la propietat intel·lectual comeses per un tercer, quan l'ISP té la possibilitat de supervisar l'activitat realitzada per l'infractor i quan obté algun benefici econòmic d'aquesta infracció. L'origen d'aquesta doctrina, tal com indica

---

<sup>93</sup> Especialment la secció quarta del capítol segon de la Directiva 2000/31/CE del Parlament Europeu i del Consell, de 8 de juny de 2000, sobre allotjament de dades.



Raquel Xalabarder, és la sentència Shapiro, Bernstein and Co. vs. H.L. Green Co., 316 F.2d 304 (2d Cir. 1963) (Xalabarder, 2006).

Seguint la mateixa autora, en relació a la doctrina de la *Vicarious Liability* qui:

"... amb coneixement de l'activitat infractora, indueix, causa o contribueix materialment a la conducta infractora d'un tercer, pot ser declarat responsable com infractor «contribuent»- *vid.* Gershwin vs. Columbia, 443 F.2d 1159 (2d Cir. 1971)..."

## **Teoria del coneixement efectiu**

Ara per ara, la doctrina eximeix els intermediaris de serveis de la societat de la informació de l'obligació de supervisar permanentment la idoneïtat dels continguts que els usuaris de les seves pàgines web hi emmagatzemen o dels que es troben a les pàgines amb les quals es pot enllaçar des de les mateixes. S'estima per tant que facilitar l'accés a continguts de tercers, ja sigui mitjançant l'allotjament en les pròpies plataformes com dirigint per mitjà d'enllaços a altres que els continguin, no comporta responsabilitat per al prestador del servei, excepte si coneix la il·legalitat d'aquest contingut o no impedeix l'accés als mateixos tan aviat com conegui aquesta il·legalitat. És a dir, la responsabilitat no es generaria pels actes que tercers puguin cometre, si no pel coneixement de la il·legalitat o perjudici ocasionat per aquests actes i la no adopció de les mesures necessàries per a impedir o dificultar els mateixos tan aviat com s'adquireix tal coneixement.

Aquesta posició no és més que l'aplicació de la doctrina jurisprudencial del coneixement efectiu, tal com indica Alejandro Touriño, que opina que en realitat aquesta doctrina no és més que, en les seves pròpies paraules:

"... l'aplicació a l'àmbit d'Internet de la institució clàssica de la culpa in vigilando, prevista des de temps de Justinià i que encara ens serveix d'inspiració..."<sup>94</sup>.

Tradicionalment la *culpa in vigilando* s'ha aplicat a aquelles persones a les quals s'atribueix responsabilitat pels actes comesos per aquells sobre els quals es té un especial deure de vigilància. A la pràctica, això és aplicable als pares i tutors respecte dels seus fills o tutelats; als titulars de centres docents respecte dels seus alumnes menors d'edat; als empresaris respecte dels seus empleats en l'exercici de les seves funcions,...

Es tracta en realitat de la presumpció de culpa per negligència en el compliment de l'obligació de vigilància de les persones al nostre càrrec per una relació que ho estableix així. La legislació recull en general aquest principi en normes com, per exemple, el Codi civil espanyol:

"... L'obligació que imposa l'article anterior (... El que per acció o omissió causa dany a un altre, intervenint culpa o negligència...) és exigible, no només pels actes o omissions

---

<sup>94</sup> Alejandro Touriño (2010) "*Régimen de responsabilidad de los prestadores de servicios de la sociedad de la información*". A propòsit de la STS quejasonline.com en diari Juridico.com <http://www.diariojuridico.com/opinion/regimen-de-responsabilidad-de-los-prestadores-de-servicios-de-la-sociedad-de-la-informacion.html>

propis, sinó pels d'aquelles persones de qui s'ha respondre...

"<sup>95</sup>.

Aquest mateix article després de referir-se explícitament a pares, tutors, empresaris, titulars de centres docents, especifica que aquesta responsabilitat s'acaba quan demostren que van emprar la diligència exigible per prevenir el dany. Els tribunals han anat consolidant una interpretació extensiva a altres supòsits similars del "principi de responsabilitat per fet aliè", que es deriva de la lectura d'aquest article del Codi civil.

A priori, semblaria lògic que aquesta interpretació extensiva del principi de responsabilitat per fet aliè, es limités a aquells casos en què hi ha una clara relació de dependència entre el vigilat i l'obligat a vigilar. No obstant això, els tribunals venen consolidant uns criteris no gaire ben definits sobre en què consisteix aquesta dependència. Així, el Tribunal Suprem espanyol, en la relació ocupador-empleat, ve admetent com dependència no només quan una persona realitza un treball per encàrrec d'una altra, sinó també quan aquest treball el realitza amb el seu consentiment o autorització.

En relació als prestadors de serveis d'intermediació, aquest coneixement efectiu és fonamental per a la definició de la seva responsabilitat. L'article 16 de la Llei 34/2002, de 11 de juliol, de serveis de la societat de la informació i de comerç electrònic, que incorpora les disposicions de la Directiva 2000/31/CE, estableix que: "Els prestadors d'un servei d'intermediació consistent a albergar dades proporcionades pel

---

<sup>95</sup> Article 1903 del Codi Civil, aprovat pel Reial Decret del 24 de juliol de 1889, i actualitzat amb nombroses modificacions des de llavors.

destinatari d'aquest servei no seran responsables per la informació emmagatzemada a petició del destinatari, sempre que: a) No tinguin coneixement efectiu que l'activitat o la informació és il·lícita o lesiona béns o drets d'un tercer susceptible d'indemnització, o b) Si ho tenen, actuïn amb diligència per retirar les dades o fer impossible l'accés a ells".

Diferents sentències han anat aclarint posteriorment el concepte de "coneixement efectiu" per tal de delimitar la responsabilitat. En la sentència 773/2009, de 9 de desembre de 2009, la Sala de la Civil del Tribunal Suprem espanyol, es va pronunciar afirmant que l'absència de coneixement efectiu allibera de responsabilitat a la prestadora de serveis d'allotjament per la informació emmagatzemada a petició del destinatari d'aquells.

En aquesta mateixa sentència el Tribunal va deixar clara la interpretació que s'ha de fer, d'acord amb la Directiva 2000/31/CE, de l'article 16 de la Llei 34/2002, de 11 de juliol, de serveis de la societat de la informació i de comerç electrònic en parlar del coneixement efectiu. Aquest article 16 estableix que: "S'entendrà que el prestador de serveis té el coneixement efectiu a que es refereix el paràgraf a) quan un òrgan competent hagi declarat la il·licitud de les dades, ordenant la seva retirada o que s'impossibiliti l'accés als mateixos, o s'hagués declarat l'existència de la lesió, i el prestador conegués la corresponent resolució, sens perjudici dels procediments de detecció i retirada de continguts que els prestadors apliquin en virtut d'acords voluntaris i d'altres mitjans de coneixement efectiu que poguessin establir-se". "Altres mitjans" implica que es pot inferir que el prestador del servei tenia coneixement del fet sempre que es pugui deduir per inferències lògiques a l'abast de qualsevol:

"... A més a més de que el mateix article 16 permet aquesta interpretació favorable a la Directiva - en deixar al marge la possibilitat d'«*altres mitjans de coneixement efectiu que poguessin establir-se*» -, no es pot prescindir de que la mateixa atribueix el mateix valor que al «*coneixement efectiu*» a aquell que s'obté pel prestador del servei a partir de fets o circumstàncies aptes per possibilitar, encara que mediatament o per inferències lògiques a l'abast de qualsevol, una efectiva aprehensió de la realitat de que es tracti..."<sup>96</sup>.

---

<sup>96</sup> Fonament jurídic 4 de la sentència 773/2009 de 9 de desembre de 2009 la Sala de Civil del Tribunal Suprem.



## **Capítol novè: Plataformes d'intermediació**

---

### **Plataformes d'intermediació: L'exemple d'eBay**

El comerç en general, i per tant també el comerç electrònic, necessita un espai concret per poder desenvolupar-se adequadament. Un dels espais oferts és el de les plataformes d'intermediació, si bé la seva utilització requereix una gran seguretat jurídica i una clara delimitació dels aspectes de protecció dels consumidors i de la resta de participants en les transaccions comercials. Això implica que la legislació i la interpretació jurídica de les normes, donguin respostes a totes aquelles circumstàncies que en aquest camp es vagin produint, la qual cosa és sens dubte cada vegada més complex<sup>97</sup>.

Encara que no s'entri a valorar els aspectes tecnològics del comerç electrònic i la utilització que es pugui fer de les plataformes d'intermediació, sí que és evident que aquests aspectes tecnològics provoquen canvis substancials en l'entorn en què es produeix el mateix, pel que cada avenç de la tecnologia comporta freqüentment un avenç en

---

<sup>97</sup> Es segueix en aquest sentit la classificació dels diferents prestadors de serveis elaborada per Marquez Lobillo, P., "Prestadores de servicios de intermediación: Algunas especialidades de su estatuto jurídico". Revista de Contratación Electrónica. N° 88, desembre 2007. Citat per Moncada Florez, J.P. "La responsabilidad de los prestadores de servicios de intermediación en la sociedad de la Información" (Tesi Doctoral) editorial de la Universidad de Granada. Granada, 2010.

el marc jurídic que el regula. Un exemple d'aquesta necessitat de constants noves respostes legals i jurídiques als nous reptes que el comerç electrònic va configurant, el representa la sentència del Tribunal de Justícia de la Unió Europea de 12 de juliol de 2011 en l'assumpte C-324/09, és a dir, en el conflicte que va plantejar la multinacional L'Oréal contra alguns aspectes del sistema amb el que la també multinacional eBay facilita, mitjançant la seva plataforma d'intermediació, aquest comerç electrònic per Internet.

Per situar el conflicte entre les dues multinacionals, hem de tenir en compte que eBay és en realitat un conglomerat d'empreses que es dedican a ofertar diferents tipus de serveis als seus usuaris. En aquest cas el tema en qüestió és específicament el relacionat amb el comerç electrònic. Es tracta d'una empresa dedicada a donar serveis d'intermediació, inclosos plenament en el que la legislació enten sota aquest concepte:

“...«Serveis d'intermediació»: servei de la societat de la informació pel qual es facilita la prestació o utilització d'altres serveis de la societat de la informació o l'accés a la informació.

Són serveis d'intermediació la provisió de serveis d'accés a Internet, la transmissió de dades per xarxes de telecomunicacions, la realització de còpia temporal de les pàgines d'Internet sol·licitades pels usuaris, l'allotjament en els propis servidors de dades, aplicacions o serveis subministrats



---

per altres i la provisió d'instruments de cerca, accés i recopilació de dades o d'enllaços a altres llocs d'Internet..."<sup>98</sup>.

Els usuaris d'eBay, tant els que volen vendre un producte a través de les plataformes que eBay ofereix, com els que volen adquirir aquests productes, són clients de l'empresa que es pot considerar plenament com a intermediària en la seva qualitat de proveïdora de serveis als seus clients, tant si són venedors com compradors.

En principi aquesta tasca d'intermediació no presenta especials dificultats jurídiques, doncs la venda en un entorn virtual es asimilable a la venda per correspondència que ja fa anys que ha consolidat una sòlida cobertura legal<sup>99</sup>. A l'Estat espanyol les vendes a distància estan regulades en la legislació general de comerç. Així, la Llei 7/1996, de 15 de gener, d'ordenació del comerç minorista, regula entre altres les vendes a distància. Ampliat posteriorment pel Reial Decret 225/2006, de 24 de febrer, pel qual es regulen determinats aspectes de las vendes a distància i la inscripció en el registre d'empreses de vendes a distància.

També podem assimilar la tasca d'intermediació realitzada per eBay a l'oferta de lloguer d'espais i serveis que una gran superfície comercial pot prestar a diferents empreses venedores per a que s'instal·lin allà per

---

<sup>98</sup> Lletre b de l'annex de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

<sup>99</sup> A finals del segle XIX empreses com Montgomery Ward, Sears i altres similars van posar en funcionament a Estats Units la venda per catàleg. Posteriorment, al començament dels anys 70 van aparèixer les primeres vendes que utilitzaven els ordinadors per transmetre les ordres de compra. La dècada següent es va popularitzar l'anomenada "venda directa" com una nova forma de venda per catàleg que es publicitava per televisió en què el client contractava el producte per telèfon i pagava amb targetes de crèdit. Aquestes experiències van anar generant un marc legal avui molt consolidat internacionalment.

ofertar els seus productes. Tanmateix, en el comerç electrònic es donen unes circumstàncies especials que, en el cas dels serveis oferts per eBay, fan la situació molt més complexa.

En un principi eBay era una empresa que va començar oferint una pàgina web on terceres persones podien realitzar la compra i venda de productes. Aquesta compra i venda es podia realitzar mitjançant una subhasta a través d'Internet, o bé establint per part del venedor un preu fix pel producte ofertat. Posteriorment eBay va anar afegint altres serveis als seus usuaris, fins a convertir-se en un referent en el mercat de compra i venda per Internet.

Quan la venda es realitza mitjançant el sistema de subhastes, el venedor posa un preu de sortida, així com el període de temps durant el qual l'anunci estarà obert per acceptar ofertes. Durant aquest termini, els compradors poden anar licitant pel producte i, al finalitzar el termini d'ofertes, el licitador més alt s'emporta l'article sota les condicions de lliurament i devolucions imposades pel venedor. Aquestes condicions han d'ajustar-se al marc de les condicions generals que eBay té establertes i que els usuaris han d'acceptar per poder utilitzar els seus serveis.

En el cas de la venda a un preu fix, el que eBay anomena "Compra-ho ja!", serveix perquè els compradors puguin adquirir immediatament l'article al preu establert pel venedor sense tenir que licitar per ell. Es tracta en definitiva d'una venda directa en la que un comprador decideix adquirir un producte ofert per un venedor a un preu determinat, utilitzant tots dos un proveïdor de serveis, en aquest cas eBay, com a plataforma d'intermediació.

En ambdós casos, les transaccions que es realitzen són entre el venedor i el comprador i, per tant, eBay no forma part directa de la transacció. La seva funció es la d'oferir l'entorn adequat per que venedor i comprador puguin realitzar les seves transaccions. Per oferir aquest servei eBay cobra al venedor una petita quantitat per cada producte que es posa a la venda en la seva pàgina web i, d'altra banda, cobra un percentatge prèviament establert del preu final de cada venda que es realitza utilitzant els seus serveis.

## **Polítiques de privacitat**

Aquest sistema de comerç presenta moltes aventatges tant pels compradors com pels venedors, i naturalment per al proveïdor de serveis que possibilita les transaccions. Tanmateix, els gestors de les companyies que ofereixen plataformes d'intermediació són plenament conscients de que aquest mateix sistema de venda presenta nombrosos riscos d'incorre en responsabilitat si no s'adopten les màximes precaucions en el desenvolupament de l'activitat comercial a través dels seus serveis. Per aquest motiu, en el cas d'eBay, el desenvolupament del sistema s'ha orientat de manera que es minimitzin aquests riscos, i quedi protegida al màxim la responsabilitat de la companyia.

Un d'aquests riscos és el de l'ús de les dades personals dels usuaris i la facilitat amb que en un moment donat es pot incorre en responsabilitat per infraccions a la legislació de protecció de dades vigent als diferents països. És per això que un dels aspectes als que eBay es compromet en els seus documents és garantir una adequada protecció de les dades personals dels seus usuaris.

Cal tenir en compte que, tant per ser venedor com per ser comprador en el servei d'eBay, es necessari procedir a l'enregistrament en aquest servei i, per tant, donar accés a dades personals com poden ser el nom, adreça, número de telèfon i adreça de correu electrònic i, en el cas dels venedors i en certs casos pels compradors, també es necessari la identificació mitjançant una targeta de crèdit o de dèbit. La protecció de dades personals es converteix així en una font potencial de riscos per a l'empresa. Per aquest motiu eBay ha desenvolupat un procediment de tractament de les dades que ha de ser llegit i acceptat pels usuaris abans de poder accedir als seus serveis. Sota el títol de "Política de privacitat"<sup>100</sup> es presenta als usuaris un extens recull de normes i compromisos de privacitat que aquests han d'acceptar per poder utilitzar els seus serveis.

Amb això eBay busca cobrir la seva responsabilitat en tot el relatiu al tractament de dades personals dels seus usuaris. Però conscients de la dificultat de garantir totalment aquesta privacitat, donat el constant avanç de les tecnologies de la comunicació que fa vulnerable qualsevol dada situada a Internet, és pel que en la versió anterior d'aquesta política de privacitat <sup>101</sup> acabaven eximint-se expresament de qualsevol responsabilitat davant d'un ús inadequat per part de tercers:

"... La teva informació s'emmagatzema en els nostres servidors ubicats als Estats Units. Tractem les dades com un actiu que ha de ser protegit i utilitzem un gran nombre d'eines (xifrat,

---

<sup>100</sup> En vigor en el seu actual format des del dia 31 de juliol de 2014. Podem trobar aquest document a la pàgina oficial de la companyia <http://pages.ebay.es/help/policies/privacy-policy.html>.

<sup>101</sup> En vigor des del dia 11 d'octubre de 2012 fins el 30 de juliol de 2014 per a usuaris nous i fins el 10 de setembre de 2014 per a usuaris ja existents.

contrasenyes, seguretat física, etc.) per protegir la teva informació personal contra l'accés i la revelació no autoritzats. Tanmateix, com probablement sàpigues, és possible que terceres parts aconseguixin interceptar il·legalment les transmissions o les comunicacions privades o tenir accés a elles, i que altres usuaris puguin fer un ús malintencionat de la teva informació personal que recopilin des del lloc web. Així doncs, encara que intentem per tots els mitjans possibles protegir la teva privacitat, no et prometem que la teva informació personal i les teves comunicacions privades siguin sempre confidencials..."<sup>102</sup>.

En l'actual política de privacitat d'eBay també es pot observar que s'inclouen tant les dades proporcionades pel propi usuari com les recopilades automàticament pel sistema com són les dades següents:

"... Quan visites els nostres llocs, uses les nostres aplicacions, serveis i eines, o interactues amb la nostra publicitat o contingut, recopilem automàticament les dades que ens envia el teu ordinador, dispositiu mòbil o un altre dispositiu d'accés. Aquestes dades s'associen a tu personalment només si t'identifiques com a usuari registrat, i inclouen:

- identificador del dispositiu o identificador únic, tipus de dispositiu, informació sobre l'ordinador i la connexió, estadístiques sobre visites a pàgines, trànsit cap a altres

---

<sup>102</sup> Apartat "Seguretat" de la política de privacitat d'eBay en vigor des del dia 11 d'octubre de 2012 fins el 30 de juliol de 2014 per a usuaris nous i fins el 10 de setembre de 2014 per usuaris ja existents.

llocs i des d'ells, URL de referència, dades sobre anuncis, adreça IP i informació de registre web estàndard, així com

- informació anònima recopilada mitjançant l'ús de cookies i balises web..."<sup>103</sup>.

## Possibles il·legalitats i responsabilitat de l'intermediari

Un altre dels riscos que eBay tracta d'evitar, és la possibilitat de que els seus usuaris realitzin les seves activitats comercials incumplin alguna norma legal o perjudicant altres persones o empreses. Els usuaris són informats en la pròpia pàgina web de la necessitat de complir els requisits legals exigibles a aquestes activitats. Igual que succeeix amb la Política de privacitat, els usuaris han d'acceptar aquestes limitacions, recollides en el document "Condicions d'ús del servei"<sup>104</sup> que inclou, entre altres coses, que no es violarà cap llei i que no es vendran articles falsificats o que d'una o un altra manera puguin infringir els drets d'autor, marques o altres drets de tercers. Per a convertir-se en usuari d'eBay, l'usuari ha de llegir i acceptar tots els termes i condicions que apareixen en aquestes Condicions d'ús.

Per tal de controlar el compliment de les condicions d'ús per part dels usuaris, eBay té instal·lat filtres per identificar anuncis que incompleixin les

---

<sup>103</sup> Apartat "Recopilació de dades personals" de la política de privacitat d'eBay en vigor.

<sup>104</sup> Podem trobar aquest document a la pàgina oficial de la companyia <http://pages.ebay.es/help/policies/user-agreement.html?ssPageName=f:f:ES>.

---

condicions d'ús del servei i també ha desenvolupat un programa denominat "VeRO" (*Verified Rights Owner*, o el que podriem traduir per "Titular de Drets Verificat"). Aquest programa permet als titulars de drets de propietat intel·lectual o industrial sol·licitar la retirada dels anuncis d'ofertes de productes, quan considerin que vulneren els seus drets legítims de propietat intel·lectual o industrial.

Un cop eBay rep una notificació de vulneració de drets de propietat intel·lectual o industrial s'investiga el cas i, en cas de confirmar la possible vulneració de drets, retira l'anunci de la seva pàgina web i pren les mesures que considera pertinents en contra del venedor que va realitzar l'anunci. Cal tenir en compte que, segons les propies condicions d'ús d'eBay:

"... Sense perjudici de qualsevol altre dret, podem limitar, suspendre o cancel·lar els nostres Serveis i comptes d'usuari, restringir o prohibir l'accés als nostres Serveis, i les activitats que hi desenvolupis, cancel·lar licitacions i retirar anuncis, retardar o eliminar els continguts allotjats, eliminar qualsevol estatus especial associat amb el compte, reduir o eliminar qualsevol descomptes, i adoptar les mesures tècniques i legals necessàries per evitar l'ús per la teva part dels nostres Serveis, si:

- considerem que estàs creant problemes o possibles responsabilitats legals;
- considerem que aquestes restriccions milloraran la seguretat de la comunitat eBay o reduiran l'exposició a responsabilitats econòmiques tant per part d'eBay com de qualsevol altre usuari;

- considerem que estàs infringint els drets de terceres parts;
- considerem que estàs actuant de manera incompatible amb la lletra o l'esperit d'aquestes Condicions d'ús o de les nostres polítiques, o actuant de manera abusiva respecte dels nostres empleats o usuaris;
- malgrat els nostres esforços raonables, no podem verificar o autenticar qualsevol informació que ens proporciones; o
- no facis el pagament complet de les tarifes pendents pels nostres Serveis en la data de venciment del pagament.

Quan sorgeix un problema amb un comprador o un venedor, podem tenir en compte l'historial de rendiment de l'usuari i les circumstàncies específiques en l'aplicació de les nostres polítiques. Podem optar per ser més flexibles en l'execució de les polítiques, i fer el correcte tant per als compradors com per als venedors..."<sup>105</sup>.

Aquestes mesures de prevenció desenvolupades per eBay, tenen per finalitat exonerar la companyia de tota responsabilitat en cas d'un mal ús dels seus serveis. Això s'exten als diferents serveis complementaris ofertats als seus clients. Així per exemple, per ajudar als venedors a potenciar les seves vendes, eBay ofereix diversos serveis extres a canvi d'un suplement que inclouen entre altres la visibilitat de l'anunci a nivell internacional. D'aquesta forma, el venedor es pot assegurar, mitjançant el pagament d'una taxa per país, que l'anunci serà automàticament introduït

---

<sup>105</sup> Apartat "Abusos a eBay" de les condicions d'ús d'eBay en vigor.



en les cerques en els llocs d'eBay en altres països seleccionats pel venedor.

En aquest sentit, a la pàgina d'ajuda on s'explica els avantatges d'utilitzar el servei de visibilitat de l'anunci a nivell internacional, s'inclou una alerta pels usuaris. En aquesta alerta es recomana al venedor que verifiqui que està complint amb les lleis sobre comerç dels països als que vol accedir. Aquestes legislacions poden diferir de les lleis locals i representar algun tipus de limitació o restriccions en les vendes de productes ofertats.

Així i tot, a pesar de totes aquestes prevencions, l'entorn virtual és de tal complexitat que es pràcticament impossible cubrir tots els riscos possibles. Així per exemple, entre els advertiments als usuaris d'eBay, no es fa cap menció específica als venedors de fora de l'Espai Econòmic Europeu sobre el fet que la venda de productes originals comercialitzats fora d'aquest territori i dirigits a compradors residents en el mateix pot comportar la violació de drets del comerç.

En la seva qualitat de subministrador de serveis a Internet, eBay proporciona un suport necessari perquè els usuaris puguin accedir als productes oferts pels venedors. No obstant això, la responsabilitat dels continguts recau sobre els autors i els subministradors de contingut. Així, la Directiva 2000/31/CE del Parlament Europeu i del Consell, de 8 de juny de 2000, relativa a determinats aspectes jurídics dels serveis de la societat de la informació, en particular el comerç electrònic en el mercat interior, dedica la seva secció quarta al tractament de la responsabilitat dels prestadors de serveis intermediaris.

L'article 14 de la Directiva es refereix als prestadors de serveis la activitat dels quals consisteix a "allotjament de dades" proporcionades pel

destinatari. Es tracta en definitiva de serveis d'intermediació, pel que en el mateix article s'especifiquen les circumstàncies per les que aquests prestadors no poden ser considerats responsables de les dades allotjades per altres persones. Això és així, excepte en aquells casos en què els prestadors de serveis tinguin coneixement efectiu de la il·licitud de les dades que allotgen i que en cas de tenir coneixement no actuïn amb diligència per retirar les dades o fer impossible l'accés a elles:

“...Els estats membres han de garantir que, quan es presti un servei de la societat de la informació consistent en emmagatzemar dades facilitades pel destinatari del servei, el prestador de serveis no pugui ser considerat responsable de les dades emmagatzemades a petició del destinatari, a condició que:

- a) el prestador de serveis no tingui coneixement efectiu que l'activitat a la informació és il·lícita i, pel que es refereix a una acció per danys i perjudicis, no tingui coneixement de fets o circumstàncies per les quals l'activitat o la informació reveli el seu caràcter il·lícit, o que,
- b) quan tingui coneixement d'aquests punts, el prestador de serveis actuï amb promptitud per retirar les dades o fer que l'accés a ells sigui impossible...”<sup>106</sup>.

Les activitats d'eBay entren de ple en aquesta categoria d'intermediació pel que, aparentment, sempre que no tingui un coneixement efectiu del

---

<sup>106</sup> Article 14.1 de la Directiva 2000/31/CE del Parlament Europeu i del Consell, de 8 de juny de 2000.

---

caracter il·legal dels fets, o quan ho tingui retiri ràpidament els productes afectats de la seva plataforma, no hi hauria cap responsabilitat per possibles accions irregulars en les activitats comercials realitzades pels seus usuaris, especialment si tenim en compte les mesures de prevenció preses per eBay, que inclouen mecanismes per garantir el compliment de la normativa en relació a la venda de productes falsificats.

Destaca entre aquestes mesures la implantació del sistema VeRO, a través del que qualsevol persona que consideri vulnerats els seus drets intel·lectuals o industrials pot prendre mesures per fer eliminar ràpidament el producte de que es tracti de la pàgina web<sup>107</sup>.

La impossibilitat de conèixer les activitats concretes realitzades per venedors i compradors en la seva plataforma web, es desprèn de la ingent quantitat de dades que s'hi mouen diàriament. A la pràctica, la recerca del producte sol·licitat per l'usuari i el seu redireccionament cap a aquells venedors que ofereixen el producte sol·licitat, es realitza directament pel sistema, sense participació directa de cap persona.

És la pròpia màquina la que en base als algorismes preestablerts, i als termes expressats durant la recerca per part de l'usuari, és capaç fins i tot de detectar les seves preferències i presentar-li directament els productes que millor puguin satisfer les seves expectatives, encara que aquests no hagin estat sol·licitats expressament pel mateix. La total automatització del procés fa que en aquesta funció de mera intermediació, el titular de la plataforma no pugui ser considerat responsable de les dades emmagatzemades a petició del destinatari.

---

<sup>107</sup> Es pot consultar la relació d'empreses afiliades al sistema VeRO, i les condicions de protecció de drets de cada una d'aquestes marques, a: <http://vero.ebay.com/>

Tanmateix, la sentència de 12 de juliol de 2011 del Tribunal de Justícia de la Unió Europea en el procediment obert per denúncia de L'Oréal, S.A. contra eBay International, va introduir una perspectiva nova en el concepte de responsabilitat per part dels proveïdors de serveis a Internet.

## L'Oréal vs. eBay

La plataforma informàtica utilitzada per eBay a fi de permetre la compra i venda per Internet entre persones físiques que accedeixen al sistema, ofereix un poderós motor de cerca, un sistema segur de pagament i una àmplia cobertura geogràfica, de manera que encara que no participa en la venda directament, ofereix els mitjans necessaris per una ràpida connexió entre venedors i compradors.

Un dels serveis que proporciona eBay per facilitar les tasques dels clients de la seva pàgina web, i per tal de promocionar els productes que s'hi venen, es l'utilització d'un sistema remunerat de referenciació a Internet (com AdWords de Google)<sup>108</sup>. Amb la compra de paraules clau que activen enllaços patrocinats en els motors de cerca de tercers, com potser Google, MSN i Yahoo, eBay facilita que amb la introducció d'aquesta paraula clau en el motor de cerca per part d'un usuari, aparegui un anunci amb un enllaç patrocinat que porta directament al producte identificat amb aquesta paraula clau en el mercat electrònic d'eBay. Si l'usuari clica en aquest enllaç el motor de cerca el redirigirà a la pàgina web d'eBay i,

---

<sup>108</sup> Es pot consultar el funcionament del programa AdWords de Google a: <http://www.google.es/adwords/start/?channel=ha&sourceid=awo&subid=es-ca-ha-aw-bkhp0~34757493295&gclid=CPe99d6Mvb8CFWfHtAodb34AXA>.

---

per cada clic a un enllaç patrocinat, eBay paga una certa quantitat al proveïdor del servei.

Aquest fet va ser interpretat per la Companyia L'Oréal<sup>109</sup> com a participació en la venda, per la qual cosa va demanar responsabilitat a eBay per les possibles irregularitats que es poguessin donar en la venda dels seus productes a través d'aquesta plataforma, incluint falsificacions, venda en mercats no autoritzats o situacions similars. L'Oréal va demandar a eBay, a més de a tots aquells clients del seu mercat electrònic que presumptivament van utilitzar els serveis d'eBay per a realitzar vendes de productes, infringint els drets de marca de L'Oréal, a altres usuaris del mateix servei d'eBay.

La part demandant van ser diverses filials de L'Oréal, empresa que es dedica a la producció i venda, entre altres, de productes de perfumeria i cosmètica d'alta qualitat. L'Oréal divideix el seu negoci en cinc divisions diferents, dues de les quals són la divisió de productes de luxe i la divisió de productes per a professionals. Per a aquestes dues divisions, L'Oréal opera sota una xarxa de distribució selectiva tancada en la qual L'Oréal manté el control de la distribució mitjançant els contractes de distribució que restringeixen als distribuïdors autoritzats el subministrament de productes a distribuïdors no autoritzats.

Cal tenir en compte que L'Oréal no participa en el programa VeRO d'eBay al considerar que aquest pateix d'una sèrie de defectes. Així, per exemple, en opinió de L'Oréal, el sistema només permet al propietari dels drets de prendre mesures un cop el titular dels drets és conscient de la llista

---

<sup>109</sup> Es poden veure les marques comercialitzades per L'Oréal a: [http://www.loreal.es/\\_es/\\_es/index.aspx?](http://www.loreal.es/_es/_es/index.aspx?).

d'anuncis que vulneren el seu dret. Per tant, aquestes mesures només es poden produir després de que s'hagi produït la publicació de l'anunci a la pàgina web i, fins i tot, en el moment en que el titular dels drets es capaç de notificar eBay de la vulneració dels seus drets i aquest de prendre les mesures pertinents, el producte probablement ja s'haurà venut.

A part, la forma d'actuar en el programa VeRo col·loca la càrrega de buscar i controlar els anuncis que infringeixen els drets sobre el titular d'aquests drets i, tenint en compte de la gran quantitat d'anuncis que es publiquen diàriament en la pàgina web d'eBay, aquest control és molt costós per a aquest titular.

Una altra queixa fa referència a que el programa es centre amb les entrades d'anuncis individuals i no al perfil del venedor. Això provoca que, tot i que es retiri un anunci després de la queixa de la vulneració de drets per part del titular d'aquests drets, no hi ha res que impedeixi que el venedor torni a col·locar posteriorment un altre anunci amb el mateix producte ni tampoc atura les conductes de vulneració de drets per part del venedor que les ha comés anteriorment.

Aquest fet provoca que, en opinió de L'Oréal, les sancions aplicades als venedors no siguin efectives, ja que en alguns casos la sanció únicament consisteix en la retirada de l'anunci i, per tant, el venedor pot tornar a vulnerar els drets de marca amb la inclusió d'un altre anunci sobre el mateix producte.

En altres casos la sanció prevista per eBay consisteix en la realització d'un tutorial sobre els drets de propietat intel·lectual. Tot i així, en opinió de L'Oréal, per a la superació d'aquest tutorial no és necessari contestar correctament cap de les preguntes que hi ha. Fins i tot, afegeix la

---

empresa demandant, en els casos en que la sanció consisteix en la suspensió de forma permanent del compte del venedor, aquest pot obrir un nou compte amb un nom d'usuari diferent i seguir utilitzant els serveis d'eBay excepte quan eBay detecti que el nou compte està vinculat amb el compte suspès.

D'altra banda, L'Oréal incidia en el fet de que s'ha de tenir en compte que els titulars dels drets no coneixen inicialment la identitat real del venedor i, per tant, no poden iniciar cap actuació en contra d'aquest. Per tal d'obtenir aquestes dades, el titular dels drets han d'aconseguir una ordre judicial o signar un acord d'informació personal amb eBay. En ambdós casos, això suposa un altre cop, una càrrega per al titular dels drets.

Algunes de les primeres qüestions sobre les quals es va haver de pronunciar el Tribunal de Justícia de la Unió Europea són: si l'activitat d'eBay està coberta dins de l'article 14 de la Directiva sobre el comerç electrònic<sup>110</sup> i si L'Oréal es pot considerar perjudicada en virtut de l'article 11 de la Directiva 2004/48/CE del Parlament Europeu i del Consell, de 29 d'abril de 2004, relativa al respecte dels drets de propietat intel·lectual.

Tot i així, segons la sentència del Tribunal de Justícia, l'operador d'un mercat electrònic només es pot acollir a aquesta exempció de responsabilitat sempre i quan tingui un paper neutral, és a dir, que es limiti a un tractament merament tècnic i automàtic de les dades que no li permeti adquirir coneixement o control sobre les mateixes. És una qüestió nacional de cada Estat membre el determinar si l'assistència que presta

---

<sup>110</sup> Directiva 2000/31/CE del Parlament Europeu i del Consell, de 8 de juny de 2000, relativa a determinats aspectes jurídics dels serveis de la societat de la informació, en particular el comerç electrònic en el mercat interior.

eBay per a optimitzar o promoure determinades ofertes de venda es pot considerar una posició neutral o si en canvi és un paper actiu i, per tant, fora de l'àmbit d'exempció de l'article anterior.

Tot i que es consideri que l'actuació d'eBay és neutral i, per tant exempta de responsabilitat d'acord amb l'article 14 de la Directiva 2000/31/CE, no s'ha d'oblidar que eBay seguirà sent responsable en cas de tenir coneixement efectiu de que una activitat o informació és il·lícita o si no actua de forma immediata per a retirar o impossibilitat l'accés a aquestes dades. Així, el Tribunal estableix que el fet d'utilitzar paraules clau del motor de cerca de Google, corresponents a marques de L'Oréal, fa que a la pràctica eBay s'estigui comportant com a anunciant del producte esmentat:

“... 84.- Dels antecedents de fet del litigi principal, resumits en els anteriors apartats 39 a 42, es desprèn que eBay, mitjançant la selecció en l'operador del motor de cerca Google de paraules clau corresponents a marques de L'Oréal, fa aparèixer, cada vegada que coincideixen tals paraules amb les contingudes en la cerca efectuada per un internauta a través d'aquest motor de cerca, un enllaç publicitari al lloc [www.ebay.co.uk](http://www.ebay.co.uk) acompanyat d'un missatge publicitari sobre la possibilitat de comprar a aquest lloc web productes de la marca buscada. Aquest enllaç publicitari es mostrava en l'apartat «anuncis», que figura a la banda dreta o a la part superior de la pantalla de resultats de la cerca presentats per Google.



85.- No resulta controvertit que, en el context d'aquesta situació, l'operador del mercat electrònic és un anunciant. Aquest operador encarrega la publicació d'enllaços i missatges que, tal com va assenyalar el Fiscal General en el punt 89 de les seves conclusions, constitueixen una publicitat no només de determinades ofertes de venda en aquest mercat electrònic sinó també del propi mercat electrònic. Els anuncis publicitaris esmentats, entre altres exemples, per l'òrgan jurisdiccional remitent i exposats en els anteriors apartats 40 i 42 il·lustren aquesta pràctica..."<sup>111</sup>.

---

<sup>111</sup> Sentència de 12 de juliol de 2011 del Tribunal de Justícia de la Unió Europea en el procediment L'Oréal SA vs. eBay International.



## **Capítol desè: Protecció de la marca**

---

### **Infraccions contra els drets de marca**

La sentència de 12 de juliol de 2011 del Tribunal de Justícia de la Unió Europea en el procediment L'Oréal, S.A. vs. eBay International, va marcar clarament la responsabilitat dels prestadors de serveis d'Intermediació, al considerar activitat publicitària la utilització de paraules clau en els motors de cerca.

Tanmateix, el contingut d'aquesta sentència també es refereix a la seva responsabilitat per l'ús fraudulent de una marca registrada que puguin fer els seus usuaris, encara que tot el procés, com es el cas, estigui completament automatitzat, i per tant sense la intervenció física de cap persona del proveïdor de serveis d'intermediació, és a dir, eBay en aquest cas.

L'Oréal considerava que les persones físiques demandades havien venut béns infringint el seu dret de marca. En concret, el tribunal va tenir en compte que hi havia casos diferents en aquestes possibles infraccions dels drets de marca de L'Oréal. Aquestes infraccions es poden classificar en quatre categories:

- 1) venda de productes falsificats;

- 2) venda de productes dins l'Espai Econòmic Europeu els quals no estaven destinats a aquest mercat;
- 3) venda de productes de mostra destinats a la distribució entre els consumidors com a mostres gratuïtes;
- 4) venda de productes sense l'embalatge original.

L'Oréal considerava a eBay com a responsable solidari de les possibles infraccions en el seu dret de marca comeses pels seus usuaris. En aquest sentit, L'Oréal també veia com a responsable principal a eBay per l'ús de les marques amb la compra de paraules clau, que activen enllaços patrocinats, (és a dir, publicitaris) en els motors de cerca de tercers, en tant que aquests enllaços dirigeixen directament cap als productes infractors del dret de marques en totes aquelles de les que L'Oréal es titular<sup>112</sup>.

Per tal de demostrar el gran abast del problema de la vulneració de drets de marca de L'Oréal en els llocs web d'eBay, tant L'Oréal com altres empreses contractades a tal efecte, van realitzar durant els anys 2006, 2007 i 2008 estudis sobre la presència de productes de L'Oréal en la pàgina web d'eBay i compres de productes de prova a l'atzar per tal de comprovar si eren falsificacions o si vulneraven alguna altre norma del dret de marques. Els resultats d'aquests estudis van ser:

- 1) que hi havia una gran quantitat de productes de L'Oréal a la venda en la pàgina web d'eBay destinada al públic del Regne Unit;
- 2) que aquesta quantitat estava augmentant;

---

<sup>112</sup> Algunes de les marques més conegudes comercialitzades per L'Oréal són: L'Oréal Paris, L'Oréal Professionnel, Lancôme, Maybelline, Garnier, Vichy, Ralph Lauren, Giorgio Armani, Biotherm, Redken, Helena Rubinstein, Cacharel, La Roche-Posay, Kiehl's, Softeen-Carson, Matrix i la japonesa Shu Uemura.

3) que la majoria d'aquests productes eren o falsificacions o productes no destinats a la venda dins l'Espai Econòmic Europeu.

Com a conseqüència d'aquesta demanda, es va produir una petició de decisió prejudicial plantejada per la High Court of England and Wales, Chancery Division (Regne Unit) davant del Tribunal de Justícia de la Unió Europea, el que va donar peu a aquesta sentència<sup>113</sup>.

## La protecció de les marques

Entre la normativa en que es va recolzar aquesta sentència, es troba la Primera Directiva 89/104/CEE del Consell, de 21 de desembre de 1988, relativa a la aproximació de les legislacions dels estats membres en matèria de marques i el Reglament (CE) n° 40/94 del Consell, de 20 de desembre de 1993, sobre la marca comunitària. S'ha de tenir en compte que aquestes normes van ser derogades per la Directiva 2008/95/CE del Parlament Europeu i del Consell de 22 d'octubre de 2008 i el Reglament (CE) n° 207/2009 del Consell, de 26 de febrer de 2009, però els articles citats segueixen vigents en la nova normativa.

Així doncs, segons l'article 5, sobre drets conferits per la marca, de la Directiva 89/104/CEE esmentada, podem llegir el següent:

---

<sup>113</sup> Es poden consultar les conclusions de l'Advocat General, presentades el 9 de desembre de 2010, en les que s'analitza en profunditat el cas, a: [http://curia.europa.eu/juris/document/document\\_print.jsf;jsessionid=9ea7d0f130de0e178a2289424ff9b84ae2606065d2ad.e34KaxiLc3eQc40LaxqMbN40aNyQe0?doclang=ES&text=&pageIndex=0&docid=83750&cid=44947](http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d0f130de0e178a2289424ff9b84ae2606065d2ad.e34KaxiLc3eQc40LaxqMbN40aNyQe0?doclang=ES&text=&pageIndex=0&docid=83750&cid=44947).

“... 1. La marca registrada confereix al seu titular un dret exclusiu. El titular estarà facultat per a prohibir a qualsevol tercer l'ús, sense el seu consentiment, en el tràfic econòmic:

- a) de qualsevol signe idèntic a la marca per a productes o serveis idèntics a aquells per als quals la marca està registrada;
- b) de qualsevol signe que, per ser idèntic o similar a la marca i per ser idèntics o similars els productes o serveis designats per la marca i el signe, impliqui per part del públic un risc de confusió, que comprèn el risc d'associació entre el signe i la marca...”

Per tant, per tal de determinar si s'han vulnerat els drets del titular d'una marca el tribunal ha d'analitzar que es compleixin les sis condicions següents:

- 1) Que es faci ús d'un signe per un tercer;
- 2) Que l'ús sigui en el tràfic econòmic;
- 3) Que sigui sense el consentiment del titular de la marca;
- 4) Que sigui un signe idèntic a la marca;
- 5) Que tingui relació amb productes o serveis idèntics a aquells per als quals està registrada la marca;
- 6) Que afecti o pugui afectar les funcions de la marca, en particular, la seva funció essencial de garantir als consumidors l'origen dels béns o serveis.

Tant en els anuncis que es publicaven en la plataforma d'eBay com en el moment que eBay comprava noms de marques com a paraules clau de

Google per obtenir un lloc destacat en les cerques, s'estava utilitzant signes de tercers per a promocionar la venda dels productes situats a la seva plataforma per tercers, i amb aquesta acció es donava un benefici econòmic a partir de l'ús d'aquest signe.

D'acord a l'article 14, apartat 1, de la Directiva 2000/31/CE del Parlament Europeu i del Consell, de 8 de juny de 2000, relatiu a determinats aspectes jurídics dels serveis de la societat de la informació, en particular el comerç electrònic en el mercat interior, l'operador del mercat electrònic, en aquest cas eBay en la seva qualitat de prestador de serveis d'intermediació, no pot ser considerat responsable per les possibles irregularitats comeses per tercers. Tanmateix, aquesta manca de responsabilitat només es aplicable si el proveïdor de serveis no té cap actuació que li permeti contribuir activament a l'accés als continguts il·legítims per part de l'usuari, conèixer raonablement aquest contingut, o no actuar diligentment per a la seva retirada tan aviat com tingui coneixement d'aquesta il·licitud.

El Tribunal Suprem, fent-se ressò de la normativa, tan nacional com europea, en repetides sentències ha deixat clara aquesta exigència de diligència en la retirada dels continguts il·lícits:

"... Aquest deure de diligència en la ràpida retirada de dades il·lícites o impedir-ne l'accés necessàriament ha de posar-se en relació amb l'apartat (42) dels seus antecedents segons el qual «...Les exempcions de responsabilitat en la present Directiva només s'apliquen a aquells casos en què l'activitat del prestador de serveis de la societat de la informació es limita al procés tècnic d'explotar i facilitar l'accés a una xarxa de comunicació

mitjançant la qual la informació facilitada per tercers és transmesa o emmagatzemada temporalment, per tal de fer que la transmissió sigui més eficient. Aquesta activitat és de naturalesa merament tècnica, automàtica i passiva, el que implica que el prestador de serveis de la societat de la informació no té coneixement i control de la informació transmesa o emmagatzemada». Segons el seu apartat (46) «Per beneficiar-se d'una limitació de responsabilitat, el prestador d'un servei de la societat de la informació consistent en l'emmagatzematge de dades haurà d'actuar amb promptitud per retirar les dades de què es tracti o impedir-ne l'accés quan tingui coneixement efectiu d'activitats il·lícites...»<sup>114</sup>.

En el cas del litigi entre L'Oréal i eBay, el Tribunal de Justícia de la Unió Europea, va considerar que existeix aquesta responsabilitat des de el moment que amb la utilització per part d'eBay d'aquestes marques com a paraula clau en els buscadors de cerca, col·labora en facilitar publicitàriament l'accés a aquests productes per part de l'usuari. Aquesta acció, es realitza sense cap consentiment del titular dels drets a l'ús de les marques referides<sup>115</sup>.

---

<sup>114</sup> Sentència número 72/2011, de 10 de febrer de 2011, de la Sala Primera del Tribunal Suprem, per la publicació per un tercer d'unes expressions i d'unes fotografies injurioses a la pàgina Web Alasbarricadas.org.

<sup>115</sup> Els articles 5, apartat 1, lletra a), de la Directiva 89/104 i 9, apartat 1, lletra a), del Reglament número 40/94 s'han d'interpretar en el sentit que el titular d'una marca està facultat per prohibir a l'operador d'un mercat electrònic fer publicitat, a partir d'una paraula clau idèntica a aquesta marca i que ha estat seleccionada per aquest operador en el context d'un servei de referenciació a Internet, de productes de tal marca que es posen a la venda en aquest mercat electrònic quan aquesta publicitat no permet o tot just permet a l'internauta normalment informat i raonablement atent determinar si aquests productes procedeixen del



El Tribunal va analitzar les diverses situacions denunciades en aquest cas, per tal de considerar fins a quin punt es podia considerar infraccions cadascuna d'elles i, per tant, la possible responsabilitat d'eBay en les diferents infraccions que es poguessin derivar de les actuacions dels venedors.

Pel que fa al cas del productes directament falsificats, està clara l'existència d'infracció, ja que els consumidors es veuen induïts a engany, de manera que no coneguin la falsificació dels béns o serveis que s'estan fent passar per originals.

## **La territorialitat a Internet**

Una altra situació que podria constituir una infracció, de entre les esmentades per L'Oréal en la seva demanda, és el cas de la venda dins l'Espai Econòmic Europeu, de productes que en el seu origen no estaven destinats a aquest mercat. En la seva exposició, eBay sostenia que el titular de la marca registrada en un Estat membre o d'una marca comunitària no pot aduir exclusivitat per impedir que s'ofereixin aquests productes en un tercer Estat.

"... quan els productes designats per la mateixa i oferts a la venda en un mercat electrònic es troba en un tercer Estat i no es destinin necessàriament al territori cobert per aquesta marca [...] les normes de la Directiva 89/104 i del Reglament nº 40/94 s'apliquen quan es posa de manifest que l'oferta de

---

titular de la marca o d'una empresa econòmicament vinculada a aquest o si, per contra, procedeixen d'un tercer.

venda del producte de marca que es troba en un tercer Estat està destinada a consumidors situats al territori cobert per la marca..."<sup>116</sup>.

Es important considerar quan l'activitat del venedor està dirigida a l'estat on te el seu domicili el consumidor. A Europa, el Tribunal de Justícia explicita els que constitueixen indicis suficients:

"... Els següents elements, la llista no és exhaustiva, poden constituir indicis que permeten considerar que l'activitat del venedor està dirigida a l'Estat membre del domicili del consumidor: el caràcter internacional de l'activitat, la descripció d'itineraris des d'altres estats membres al lloc en què està establert el venedor, la utilització d'una llengua o d'una divisa diferents de la llengua o la divisa habitualment emprades en l'Estat membre en el qual està establert el venedor, amb la possibilitat de reservar i de confirmar la reserva en aquesta altra llengua, la menció de números de telèfon amb indicació d'un prefix internacional, les despeses en un servei de remissió a pàgines web a Internet per tal de facilitar l'accés al lloc del venedor o del seu intermediari a consumidors domiciliats en altres estats membres, la utilització d'un nom de domini de primer nivell diferent del de l'Estat membre en què està establert el venedor i l'esment

---

<sup>116</sup> Sentència de la Gran sala de 12 de juliol de 2011 n°C-324/2009 que té per objecte una petició de decisió prejudicial plantejada, conforme a l'article 234 CE, per la High Court of Justice (England & Wales) Chancery Division (Regne Unit), mitjançant resolució de 16 de juliol de 2009, rebuda al Tribunal de Justícia el 12 d'agost de 2009 en el procediment entre L'Oréal & Lancome i eBay Internacional.

d'una clientela internacional formada per clients domiciliats en diferents estats membres. Correspon al jutge nacional comprovar si hi ha aquests indicis..."<sup>117</sup>.

En la sentència en el cas L'Oréal vs. eBay, el Tribunal fa esment de la necessitat d'observar el que diu l'article 7, de la Primera Directiva 89/104/CEE del Consell, de 21 de desembre de 1988, relativa a l'aproximació de les legislacions dels estats membres en matèria de marca:

"... 1. El dret conferit per la marca no permet al seu titular prohibir-ne l'ús per a productes comercialitzats a la Comunitat amb aquesta marca pel titular o amb el seu consentiment.

2. L'apartat 1 no s'aplica quan hi hagi motius legítims que justifiquin que el titular s'oposi a la comercialització ulterior dels productes, en especial quan l'estat dels productes s'hagi modificat o alterat després de la seva comercialització..."

Aquesta situació va ser considerada pel Tribunal, conclouent que el dret conferit per la titularitat de la marca es extensible a aquells casos en que els productes s'han posat a la venda fora de l'Espai Econòmic Europeu, però que no s'ha posat a la venda ni s'ha autoritzat aquesta venda dins d'aquest espai. Tot i així, s'ha de tenir en compte que en el cas del

---

<sup>117</sup> Sentència del Tribunal de Justícia (Gran Sala) de 7 de desembre de 2010 (peticions de decisió prejudicial plantejades per l'Oberster Gerichtshof - Àustria) - Peter Pammer / Reederei Karl Schlüter GmbH & Co KG (C-585/08), Hotel Alpenhof GesmbH / Oliver Heller (Assumptes acumulats C-585/08 i C-144/09).

comerç electrònic aquests productes poden ser adquirits des d'aquest espai europeu.

Igualment, si s'analitza juntament amb l'article 9, sobre el dret conferit per la marca comunitària, del Reglament (CE) n° 40/94 del Consell, de 20 de desembre de 1993, sobre la marca comunitària:

"... 1. La marca comunitària confereix al seu titular un dret exclusiu. El titular habilitat per prohibir a qualsevol tercer, sense el seu consentiment, l'ús en el tràfic econòmic:

- a) de qualsevol signe idèntic a la marca comunitària, per a productes o serveis idèntics a aquells per als quals la marca està registrada;
- b) de qualsevol signe que, per ser idèntic o similar a la marca comunitària i per ser els productes o serveis protegits per la marca comunitària i pel signe idèntics o similars, impliqui un risc de confusió per part del públic; el risc de confusió inclou el risc d'associació entre el signe i la marca;
- c) de qualsevol signe idèntic o similar a la marca comunitària, per a productes o serveis que no siguin similars a aquells per als quals estigui registrada la marca comunitària, si aquesta fos notòriament coneguda a la Comunitat i si l'ús sense justa causa del signe s'aprofités indegudament del caràcter distintiu o de la notorietat de la marca comunitària o fos perjudicial per als mateixos..."

Es pot veure com també afecta als casos en que, tot i que el producte estigui comercialitzat dins l'Espai Econòmic Europeu, el titular de la

marca s'oposi a la seva venda per un motiu legítim com pot ser que el producte hagi estat reempaquetat de forma que no contingui tota la informació necessària per a la venda del producte o que aquest nou empaquetament afecti la imatge de la marca. Per tant, es veu que també es compleix en el cas de la venda de productes sense l'embalatge original. Especialment, s'ha de tenir en compte que la venda de productes cosmètics sense l'embalatge original pot comportar la vulneració d'obligacions marcades per la Directiva de Productes Cosmètics i els Reglaments de seguretat d'aquests productes.

### **Altres aspectes relatius al dret d'ús de la marca**

També s'esmenta en la sentència del Tribunal de Justícia de la Unió Europea una altra situació, que és la venda de productes de mostra destinats a la distribució entre els consumidors com a mostres gratuïtes; el debat es centra principalment en determinar si l'Oréal va obtenir valor econòmic del fet de posar al mercat mostres dels seus productes. Tenint en compte que l'Oréal oferia, de forma gratuïta als seus distribuïdors autoritzats, mostres per repartir entre els consumidors, aquesta no obtenia un retorn econòmic d'aquesta entrega.

Tot i això, per part d'eBay s'al·legava que l'entrega de mostres gratuïtes fa augmentar el nombre de ventes del producte. En aquest punt, el tribunal constata que l'entrega gratuïta per a promocionar la venda de productes no significa una comercialització per part del titular de la marca. A part, el Tribunal de Justícia ja havia declarat amb anterioritat que el fet que les mostres facin mencions com "prova" o "prohibida la

seva venda” impedeix que es reconegui que el seu titular presta el seu consentiment a la comercialització d’aquests productes.

Un últim punt a que fa referència aquesta sentència és la interpretació de l’article 11, sobre manaments judicials, de la Directiva 2004/48/CE del Parlament Europeu i del Consell, de 29 d’abril de 2004, relativa al respecte dels drets de propietat intel·lectual:

“... Els estats membres garantirán que, quan s’hagi adoptat una decisió judicial en constatar una infracció d’un dret de propietat intel·lectual, les autoritats judicials puguin dictar contra l’infractor un manament judicial destinat a impedir la continuació d’aquesta infracció. Quan així ho disposi el dret nacional, l’incompliment d’un manament judicial està subjecte, quan sigui procedent, al pagament d’una multa coercitiva, destinada a assegurar la seva execució. Els estats membres garantiran així mateix que els titulars de drets tinguin la possibilitat de sol·licitar que es dicti un manament judicial contra els intermediaris els serveis dels quals hagin estat utilitzats per tercers per infringir un dret de propietat intel·lectual, sense perjudici del que disposa l’apartat 3 de l’article 8 de la Directiva 2001/29/CE...”

Concretament determina que els manaments judicials poden demanar a l’operador d’un mercat electrònic actuacions per tal d’evitar futurs actes il·líicits. Tot i això, el tribunal remarca que les mesures que plantegin els manaments han de ser efectives, proporcionades, dissuasives i no han de crear obstacles al comerç electrònic. Per tant, tot i que les mesures han de ser determinades per la legislació nacional de cada Estat membre, hi

ha certs límits dins la Directiva 2004/48/CE com són que no es pot exigir el control de totes les ofertes de vendes que es publiquin en el mercat electrònic ni tampoc prohibir la venda en aquest mercat electrònic de productes de les marques de l'Oréal. Tanmateix, no es pot considerar que tots els productes venuts per comerç electrònic es dirigeixen a qualsevol país, pel fet de que es pugui accedir a ells a través d'una pàgina web, o en la que s'utilitzi una llengua o una moneda determinada:

“... el simple fet que es pugui accedir a la pàgina web del venedor o de l'intermediari en l'Estat membre del domicili del consumidor és insuficient. El mateix passa amb la menció d'una adreça electrònica i d'altres dades o amb la utilització d'una llengua o d'una divisa que són les habitualment emprades en l'Estat membre en el qual està establert el venedor...”<sup>118</sup>.

El mateix Tribunal de Justícia de la Unió Europea, conscient de la problemàtica representada pels temes territorials, estableix, tal i com s'ha comentat anteriorment, que per afirmar que un producte ofert per Internet es dirigeix a un país o espai físic determinat, han de donar-se elements que representin indicis suficients de que aquesta era la voluntat del venedor.

En les diferents sentències que fan referència als aspectes territorials, o als de protecció de marques, no s'apunta en cap cas la possible exempció de responsabilitat pel fet que tot el procés d'intermediació es realitzi de manera automatitzada i sense la intervenció directa de cap

---

<sup>118</sup> Apartat 94 de la Sentència del Tribunal de Justícia de la Unió Europea de 7\_de\_desembre de 2010 en els assumptes acumulats C-585/08 i C-144/09.

persona. L'exempció de responsabilitat només es dóna quan l'intermediador desconeix la il·licitud del fet que es tracti, o un cop en tingui coneixement no adopti les mesures per a la seva correcció.

En el litigi entre l'Oréal i eBay, com es recull en el capítol anterior, la responsabilitat d'eBay només es pot produir quan hi ha una participació com l'establerta pel Tribunal. El direccionament automàtic de l'usuari a determinats productes oferts per tercers, quan fa clic en el seu navegador sobre les paraules clau contractades per eBay, fa responsable no només el venedor en qüestió, sinó en aquest cas també a l'intermediari en tant que el sistema pren part activa en la publicitat del producte i, per tant, participa en la responsabilitat de les possibles irregularitats que aquests productes poguessin presentar. La total automatització del procediment, ineludible davant la gegantina quantitat de dades a gestionar, obliga a una cada vegada més sofisticada i professional implementació de tècniques d'intel·ligència artificial, però això no afecta en res la consideració legal de la responsabilitat com una cosa específicament humana.



**3<sup>a</sup> Part:**  
**Les amenaces als drets personals**



## **Capítol onzè: La protecció de dades personals**

---

### **Obtenció i tractament de dades personals**

El funcionament operatiu del comerç electrònic presenta molts aspectes positius, tal com explicita la mateixa Directiva 2000/31/CE sobre el comerç electrònic. En aquesta directiva es planteja que: "El desenvolupament del comerç electrònic en la societat de la informació ofereix importants oportunitats per a l'ocupació a la Comunitat, especialment per a les petites i mitjanes empreses, que facilitarà el creixement de les empreses europees..."<sup>119</sup> i més endavant afegeix: "És important que el comerç electrònic pugui beneficiar-se plenament del mercat interior i que s'arribi a un alt grau d'integració comunitària..."<sup>120</sup>.

Però al mateix temps és necessari compatibilitzar la necessària eficiència en el desenvolupament del comerç electrònic amb la màxima seguretat jurídica: "És fonamental per garantir la seguretat jurídica i la confiança dels consumidors que la present Directiva estableixi un marc clar i de

---

<sup>119</sup> Considerant 2 de la Directiva 2000/31/CE del Parlament Europeu i del Consell, de 8 de juny de 2000, relativa a determinats aspectes jurídics dels serveis de la societat de la informació, en particular el comerç electrònic en el mercat interior.

<sup>120</sup> Considerant 4 de l'esmentada Directiva 2000/31/CE.

caràcter general per a determinats aspectes jurídics del comerç electrònic en el mercat interior"<sup>121</sup>.

En aquest sentit, l'obtenció o el tractament de dades personals és moltes vegades imprescindible per a les activitats de comerç electrònic, però com que afecta el dret de les persones a la seva pròpia intimitat, cal garantir com i perquè es poden obtenir i utilitzar. Això és encara més important si considerem que moltes de les tecnologies actuals d'obtenció i tractament d'aquestes dades personals es poden realitzar mecànicament i sense supervisió directa de ningú.

Un tema previ fonamental és la necessitat de definir el propi concepte de dades de caràcter personal objecte de protecció legal. Aquest concepte no s'estén únicament a les dades íntimes de la persona, sinó a "qualsevol informació sobre una persona física identificada o identificable".<sup>122</sup>

La 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<sup>123</sup> planteja la conservació de les dades de connexió per part dels estats membres a l'efecte de vigilància policial. Així mateix, prohibeix l'enviament de missatges electrònics no sol·licitats, la

---

<sup>121</sup> Considerant 7 de l'esmentada Directiva 2000/31/CE.

<sup>122</sup> Article 2, lletra a) de la Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació de aquestes dades.

<sup>123</sup> Modificada per la Directiva 2006/24/CE del Parlament Europeu i del Consell, de 15 de març de 2006, i per la Directiva 2009/136/CE del Parlamento Parlament Europeu i del Consell, de 25 de novembre de 2009.

utilització no autoritzada de les anomenades «galetes» (*cookies*) i la inclusió de dades personals en les guies públiques.

Hem d'entendre per tractament de dades personals "qualsevol operació o conjunt d'operacions, efectuades o no mitjançant procediments automatitzats, i aplicades a dades personals"<sup>124</sup>.

Il·lustra la intenció que es garanteixi la privacitat de les dades personals les nombroses actuacions sancionadores per part de les institucions encarregades de vigilar aquests temes. Així per exemple, l'Agència de Protecció de Dades Espanyola, va sancionar per falta greu a l'Organització de Consumidors i Usuaris (OCU) la qual havia publicat a la seva pàgina web i en la seva publicació en paper "OCU SALUT" un article titulat "Enquesta a consultes Mèdiques i Farmàcies" en el qual s'inclouïa un llistat de metges, amb la inicial dels seus noms i el primer cognom, l'adreça on exerceixen la seva activitat professional i una valoració subjectiva de la seva actuació professional realitzada a partir d'uns qüestionaris emplenats pels enquestadors després de fer-se passar per pacients en una mostra aleatòria de centres mèdics.

Davant aquesta sanció l'OCU va presentar un recurs contenciós-administratiu davant el qual la Sala del Contenciós-Administratiu de l'Audiència Nacional va establir que la recollida, tractament i ús de dades de caràcter personal s'han d'atènyer als principis establerts en la llei, i que la garantia de la vida privada de la persona i la seva reputació tenen una dimensió positiva que es tradueix en un dret al control sobre les pròpies dades:

---

<sup>124</sup> En aquest sentit veure l'article 2, lletra b) de la repetida Directiva 95/46/CE.

"... Com dèiem també en la sentència de data 24 de març de 2004 (rec. 445/2002), els principis generals continguts en el Títol II de la Llei Orgànica 15/1999 defineixen les pautes a què s'ha d'atenir la recollida, tractament i ús de dades de caràcter personal.

Aquests principis pretenen concretar el dret fonamental que es recull en l'article 18.4 de la CE, amb la referència a l'ús de la informàtica, i que estén la seva protecció no a les dades íntimes de la persona -que es protegeixen en el dret a la intimitat- sinó a les dades de caràcter personal (STC 292/2000), per tant, la garantia de la vida privada de la persona i la seva reputació tenen una dimensió positiva que excedeix de l'àmbit de l'article 18.1 CE i que es tradueix en un dret al control sobre les pròpies dades. Es pretén garantir ara a la persona mitjançant el control sobre les seves dades personals, sobre el seu ús i destí amb el propòsit d'impedir el seu tràfic il·lícit i lesiu per a la dignitat de l'afectat... "<sup>125</sup>.

## **El consentiment per al tractament de dades personals**

Freqüentment l'objectiu d'obtenir les dades personals esta relacionat amb la publicitat. En alguns casos la publicitat s'adreça al públic en general, sense importar les seves característiques o preferències, però

---

<sup>125</sup> Fonament jurídic cinquè de la sentència 61/2007 de la Secció Primera de la Sala del Contenciós de l'Audiència Nacional, de 12 de gener de 2007.

en altres casos el públic diana al qual es pretén dirigir específicament la publicitat és un grup ben definit al qual es destina el missatge. Això fa que sigui important per adaptar el missatge al públic diana al que es pretén dirigir aquest missatge, que es coneguin les dades de les persones que en principi podrien reunir les característiques que ens permeten definir-lo com a públic diana.

La transposició a la legislació espanyola de la Directiva Europea 2009/136/CE, per la qual es modifica, entre altres, 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, va portar el 2012 a la modificació de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic<sup>126</sup>.

Aquesta modificació va recollir específicament la necessitat de garantir el consentiment dels usuaris quan s'utilitzin arxius o programes informàtics, que permetin l'emmagatzematge i recuperació de dades en els seus equips terminals, entre els quals cal incloure les denominades "galletes" o "delators", més coneguts pel seu nom en anglès *cookies*. Així, l'article 22.2 de l'esmentada Llei 34/2002 va quedar redactat de la següent manera:

“...Els prestadors de serveis podran utilitzar dispositius d'emmagatzematge i recuperació de dades en equips terminals dels destinataris, a condició que aquests hagin donat el seu consentiment després que se'ls hagi facilitat informació clara i

---

<sup>126</sup> Reial Decret-Llei 13/2012, de 30 de març, per la que es transposen directives en matèria de mercats interiors d'electricitat i gas i en matèria de comunicacions electròniques, i pel que s'adopten mesures per a la correcció de les desviacions per desajustaments entre els costos i els ingressos dels sectors elèctric i gasista.

completa sobre la seva utilització, en particular, sobre les finalitats del tractament de les dades, d'acord amb el que disposa la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal...”<sup>127</sup>.

Segons la LOPD, per tractar les dades, cal el consentiment de la persona afectada. El 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, ha regulat l'obtenció del consentiment i també en quins casos la Llei preveu que no cal el consentiment de l'afectat per tractar les seves dades. Així doncs, l'obtenció o el tractament informàtic de les dades personals només es pot fer si prèviament hi ha el consentiment per a això de l'usuari afectat. El principi del consentiment o autodeterminació informativa és un element bàsic per garantir el dret al control de les pròpies dades personals:

“... S'ha reiterat en nombroses sentències d'aquesta Sala que el principi del consentiment o autodeterminació informativa constitueix un dels pilars essencials de la normativa que regula el tractament automatitzat de les dades personals d'un individu. La garantia d'aquest principi rau en que l'afectat presti el seu consentiment conscient i informat, per tal que aquesta recepció de dades i el seu posterior tractament sigui lícit. Ja en l'article 6.1 de la Llei Orgànica 5/1992, de 29 d'octubre, de regulació del tractament automatitzat de les Dades de Caràcter Personal (LORTAD), s'establia el

---

<sup>127</sup> Paràgraf primer de l'article 22.2 de la Llei 34/2002, d'11 de juliol, de Serveis de la Societat de la Informació i de Comerç Electrònic.



«tractament automatitzat de dades de caràcter personal requerirà el consentiment de l'afectat, llevat que la Llei disposi una altra cosa». Precepte que es reproduïx en el nou Art. 6.1 de la Llei Orgànica 15/99, si bé per ressaltar la importància que aquest consentiment no sigui dubtós, qualifica la prestació del mateix afegint l'expressió «inequívoc», el que ratifica el que ja s'ha exposat sobre aquest requisit essencial en la present matèria (SAN, Secc.1<sup>a</sup>, 30 de juny de 2004, rec. 619/02)...”<sup>128</sup>.

Així doncs, les dades de caràcter personal únicament podran ser objecte de tractament o cessió si l'interessat hagués prestat prèviament el seu consentiment per fer-ho. El Reglament de desenvolupament de la Llei de protecció de dades estableix la forma general per obtenir el consentiment<sup>129</sup>. Aquest consisteix en que el responsable del tractament de les dades ha de comunicar al titular de les dades personals, la seva intenció de tractar les mateixes, explicant-li la seva finalitat i a qui va dirigit i indicant-li que té trenta dies per oposar-s'hi o sinó es procedirà al seu tractament. Per tal que l'afectat pugui manifestar la seva negativa al tractament de les seves dades, s'ha de tenir un mètode que asseguri la recepció de la comunicació per part de l'interessat i per a facilitar-li una

---

<sup>128</sup> Fonament jurídic cinquè de la sentència 61/2007 de la Secció Primera de la Sala del Contenciós de l'Audiència Nacional, de 12 de gener de 2007.

<sup>129</sup> L'article 14 del Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, aprovat pel Reial Decret 1720/2007, de 21 de desembre, estableix que: "...1. El responsable del tractament pot sol·licitar el consentiment de l'interessat a través del procediment establert en aquest article, excepte quan la Llei li exigeixi l'obtenció del consentiment exprés per al tractament de les dades..."

forma senzilla i gratuïta per realitzar aquesta manifestació. En tot cas no es pot tornar a demanar aquest mateix consentiment abans d'un any.

Els casos en que la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal (LOPD) preveu que no cal el consentiment de l'afectat per tractar les dades<sup>130</sup>, són aquells necessaris per portar a terme les funcions pròpies de les administracions públiques; les que figuren en els contractes o precontractes per identificar-hi les parts; i les que siguin públicament accessibles o tinguin per finalitat protegir un interès vital per a l'interessat.

## **El dret de protecció de les pròpies dades**

El dret a la protecció de dades tracta de garantir en definitiva el poder de control sobre les pròpies dades. Tal com explica Roselló Mallol<sup>131</sup>:

---

<sup>130</sup> L'article 6.2 de la LOPD especifica que: "... No cal el consentiment quan les dades de caràcter personal es recullin per a l'exercici de les funcions pròpies de les administracions públiques en l'àmbit de les seves competències, quan es refereixin a les parts d'un contracte o precontracte d'una relació comercial, laboral o administrativa i siguin necessàries per al seu manteniment o compliment; quan el tractament de les dades tingui per finalitat protegir un interès vital de l'interessat en els termes de l'article 7, apartat 6, de la present Llei, o quan les dades figurin en fonts accessibles al públic i el seu tractament sigui necessari per a la satisfacció de l'interès legítim perseguit pel responsable del fitxer o pel del tercer a qui es comuniquin les dades, sempre que no es vulnerin els drets i llibertats fonamentals de l'interessat..." Tots aquests supòsits són regulats més profundament en l'article 10 del Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (RLOPD).

<sup>131</sup> Roselló Mallol, Víctor. "Marketing y Protección de Datos" Capítol III Noticias Jurídicas setembre 2009. Es pot consultar en <http://noticias.juridicas.com/articulos/15-Derecho-Administrativo/200909-90926383465783632832.html>.

“... el dret a la protecció de dades, també conegut com a dret a l'autodeterminació informativa, consisteix, de manera resumida, en el poder de control i disposició que qualsevol titular de dades, té sobre aquestes; així en paraules del Tribunal Constitucional (STC 254/1993, de 20 de juliol) «el dret fonamental a la protecció de dades persegueix, en definitiva, garantir a la persona un poder de control sobre les seves dades personals, sobre el seu ús i el seu destí [...] el dret a la protecció de dades garanteix als individus un poder de disposició sobre aquestes dades [...] atribueix al seu titular un conjunt de poders o facultats, que es tradueixen en autèntics deures per a aquells que utilitzen les dades, garantint a la persona un poder de control sobre les seves dades personals i que són, essencialment: el dret que es requereixi amb caràcter general, el previ consentiment per a la recollida i ús de dades personals; el dret a saber i ser informat sobre el destí i ús dels mateixos; i el dret a accedir, rectificar i cancel·lar aquestes dades. Doncs només així es pot garantir el poder de disposició sobre les dades personals»...”

Aquesta descripció per part del Tribunal Constitucional dels drets de les persones a la protecció de les seves dades personals, s'operativitza mitjançant el garantir a la persona un poder de disposició i control sobre les seves pròpies dades personals. Això comporta per qui gestioni dades de caràcter personal de les persones, no sols la obligació general de protecció de dades, sino també el d'obtenir la previa autorització de l'interessat per recollir-les i per a utilitzar-les, així com també pel seu emmagatzematge i tractament. La utilització de les dades personals sense aquesta autorització del titular solsament pot donar-se en els casos específicament previstos en la

Llei i sempre de manera justificada i proporcionada. Tal com repetidament ha dit el propi Tribunal Constitucional en les seves sentències:

“... En definitiva, el contingut del dret a la protecció de dades personals incorpora un poder de disposició i control sobre les dades personals, que constitueix part del contingut del dret fonamental a la protecció de dades, i es concreta jurídicament en la facultat de consentir la recollida, l’obtenció i l’accés a les dades personals, el seu posterior emmagatzematge i tractament, així com el seu ús o usos possibles, per un tercer, sigui l’Estat o un particular. Per això, la recollida i posterior tractament de les dades de caràcter personal s’ha de fonamentar en el consentiment del seu titular, facultat que només es pot limitar en atenció a drets i béns de rellevància constitucional, de manera que aquesta limitació estigui justificada, sigui proporcionada i, a més, s’estableixi per Llei...”<sup>132</sup>.

En molts casos l’empresa anunciant ha contractat una empresa externa per realitzar la seva campanya publicitària. En aquests casos li hauria de facilitar la relació dels seus clients per portar a terme la campanya, però d’acord a l’article 12 de la LOPD l’entrega d’aquesta relació s’ha de formalitzar mitjançant el que es sol anomenar “encàrrec de tractament”.

Aquest encàrrec de tractament és un contracte que haurà de ser fet de forma que es pugui comprovar que s’ha celebrat l’encàrrec i el seu contingut. El que hauria de preveure és la forma en que el responsable del tractament

---

<sup>132</sup> Fonament jurídic quart, de la sentència del Tribunal Constitucional 17/2013, de 31 de gener de 2013.

vol que l'encarregat utilitzi aquestes dades, la finalitat del tractament de les mateixes i les mesures de seguretat que l'encarregat ha d'implementar segons la Llei. Així doncs, l'encarregat del tractament no podrà utilitzar les dades de manera diferent a les que el responsable li ha indicat ni per altres motius que els que figuren en el contracte ni els pot donar a terceres persones. En cas de fer-ho haurà comès una infracció de la que haurà de respondre personalment.

D'altre banda, s'ha de tenir en compte que en el moment d'obtenir el consentiment del titular de les dades personals pel tractament de les mateixes, aquest consentiment es dona en un context i per unes finalitats definides amb anterioritat. Així, els avisos legals que es solen presentar a l'usuari per demanar-li autorització per l'ús de les seves dades, acostuma a incloure un avís legal similar al següent: "En compliment del que s'estableix a la Llei Orgànica 15/1999 de Protecció de Dades de Caràcter Personal i el Reial Decret 1720/2007, que aprova el seu Reglament de desenvolupament, queda informat i autoritza la incorporació de les seves dades als fitxers, automatitzats o no, existents en la nostra empresa i al seu tractament, per les finalitats de comercialització de productes propis o de tercers, relacionats amb productes o activitats de la empresa o amb la promoció de la mateixa".

La possibilitat de revocació d'aquesta autorització també ha de quedar recollida en aquests avisos de manera similar al següent: Aquesta acceptació per poder tractar o cedir de la forma establerta les seves dades té caràcter revocable, sense efectes retroactius, conforme al que disposa la Llei Orgànica 15/1999, de 13 de desembre, i per revocar aquest consentiment es pot dirigir per escrit al departament responsable del fitxer automatitzat, que figura al peu, o a través del telèfon gratuït que també figura allí. Els mateixos mitjans es poden utilitzar per exercir

els drets d'accés, rectificació, cancel·lació i oposició, en els termes establerts en la legislació vigent.

## **Dades que permeten identificar l'usuari**

No s'inclou com a dades de caràcter personal qualsevol dada que procedeixi d'una persona, sinó únicament aquelles que poden vincular-se a una persona concreta, és a dir, aquelles dades que permetin la identificació de la persona física. Així per exemple, un únic número de telèfon, si no està associat a una persona física identificada o identificable, no té la consideració de dada de caràcter personal:

“... Doncs bé, el primer problema que es suscita en el present cas és si el número de telèfon mòbil es pot incloure en el concepte de «dades personals» que recull l'article 3.a) de la LOPD que identifica com a tals «qualsevol informació concernent a persones físiques identificades o identificables». És clar que un número de telèfon associat a un nom i cognoms és una dada de caràcter personal ja que ens proporciona informació sobre una persona identificada. És més, el propi número de telèfon, sense aparèixer directament associat a una persona, pot tenir la consideració de dada personal si a través d'ell es pot identificar al seu titular.

En el present cas l'Agència Espanyola de Protecció de Dades no ha raonat, i menys ha acreditat, que a través del número de telèfon mòbil se n'hagi identificat al titular o que a partir del número fos possible aquesta identificació, de manera que

l'esmentat número de telèfon, sense d'altres circumstàncies que identifiquin o poguessin permetre identificar el titular, impedeix que pugui encaixar en la definició legal de dada de caràcter personal..."<sup>133</sup>.

En la mateixa direcció, podem aplicar també aquest criteri en el cas de les adreces IP d'un ordinador concret. La utilització d'una IP determinada no és suficient per identificar la persona concreta que l'utilitza en un moment determinat. En aquest sentit, és clarificadora la Sentència emesa el 2012 per part de la Cort del Districte Est de Nova York:

"...La suposició que la persona que paga per l'accés a Internet en un lloc determinat és la mateixa que presumptament va descarregar una sola pel·lícula és poc consistent i ho és més encara amb el pas del temps. Una adreça IP proporciona només un lloc en el qual un gran nombre de dispositius poden connectar-se, igual que un número de telèfon pot ser utilitzat per altres números de telèfon ..." <sup>134</sup>.

En la mateixa sentència es fa referència al progressiu augment de les xarxes WiFi, que fa que qualsevol persona situada prop de l'ordinador o del dispositiu que facilita el senyal, pugui accedir-hi. Els encaminadors sense fils solen estar protegits per contrasenyes, però això no garanteix que superada aquesta barrera qualsevol pugui utilitzar la IP d'un usuari concret i navegar per Internet des d'aquesta IP.

---

<sup>133</sup> Sentència 3250/2008 de la Secció Primera de la Sala del Contenciós-Administratiu de l'Audiència Nacional, de 17 de setembre de 2008.

<sup>134</sup> Sentència de l'1 de maig de 2012, del Jutge Gary R. Brown, Jutge del Districte Est de New York, en el cas per infracció dels drets de *copyright* per descàrregues de pel·lícules mitjançant Bittorrent Adult Film.

Així doncs, la especial protecció de les dades personals no es refereix a les dades en si mateixes, sinó a la seva possibilitat d'atribuir-se a persones concretes. El protegit és la identificació d'aquestes dades amb els seus propietaris, no les dades en si mateixes.

Tanmateix, es possible avui en dia la identificació de l'usuari sense necessitat d'utilitzar galetes (*cookies*). La empremta digital que deixa cada ordinador fa que s'utilitzin cada vegada més sistemes que sense utilitzar directament dades personals, poden identificar l'ordinador des del que es connecta, mitjançant aquesta empremta digital. La configuració de cada ordinador, així com la del navegador utilitzat, el fa identificable. A partir del coneixement de dades com els tipus de lletra carregats, la resolució de pantalla utilitzada, els *plug-ins* del navegador i altres dades no personals similars<sup>135</sup>.

En aquest cas, l'important per a considerar com a dades personals la informació concreta recopilada, és la capacitat identificadora d'aquesta informació, amb independència que aquesta informació hagi estat recollida per una persona física o per un algorisme, o per qualsevol altre sistema automatitzat. L'important és que les persones que han disposat la collita d'aquesta informació, el seu arxiu i tractament i la seva ulterior possible utilització, són les responsables de tot això i no l'algorisme o la màquina des de la que s'executen aquestes accions.

El fet que aquestes persones no participin directament en la recollida o el tractament d'aquestes informacions, no els eximeix de responsabilitat.

---

<sup>135</sup> Podem veure, per exemple, l'algorisme dissenyat per Peter Eckersley capaç d'identificar un ordinador a partir de dades no personals facilitades pel navegador de l'usuari, publicat a la pàgina web de l'Electronic Frontier Foundation (<https://panoptickick.eff.org/browser-uniqueness.pdf>).



En aquest sentit no podem oblidar que, tal com indica el mateix Tribunal Suprem: “no n’hi ha prou per l’exculpació davant d’un comportament típicament antijurídic la invocació de l’absència de culpa”<sup>136</sup>.

---

<sup>136</sup> Sentència del Tribunal Suprem, de 23 de gener de 1998, parcialment transcrita en les SSTS de 9 d’octubre de 2009, rec. 5285/2005 i de 23 d’octubre de 2013, rec. 1067/2006.



## Capítol dotzè: Empremta digital i signatura electrònica

---

### L'empremta digital

En el comerç digital, són cada vegada més utilitzades tècniques que permeten segmentar i apropar als potencials clients els productes oferts. L'objectiu d'aquestes tècniques es facilitar una adequada identificació del "públic diana" que pot interessar-se més fàcilment per aquests productes. Aquesta identificació permet, a més a més, detectar les prioritats, expectatives i preferències dels usuaris. En definitiva, es pretén trobar la millor manera de convertir-los en clients. Les campanyes publicitàries i la publicitat en general, es planteja d'acord a aquesta segmentació, sempre que es disposi d'informació suficient per a fer-ho.

Un dels sistemes més utilitzats amb aquesta finalitat són les anomenades "*cookies*". Es tracta de petits programes que es carreguen a l'ordinador de l'usuari quan visita una pàgina web determinada i, que faciliten a aquest servidor un conjunt de dades necessàries per a la navegació, però que pot ser recuperada pel mateix servidor en posteriors visites. En alguns casos aquestes *cookies* es mantenen actives únicament durant la sessió, però moltes altres queden a l'ordinador de l'usuari per un temps determinat a la pròpia *cookie*.

Tanmateix, es dona una progressiva limitació legal a l'ús d'aquests programes, així com la necessitat d'obtenir l'autorització prèvia de l'usuari per a la seva implantació i per a la utilització de les dades obtingudes amb aquest sistema. D'altra banda, el propi usuari pot limitar o prohibir la incorporació de *cookies* al seu ordinador i, en tot cas, les pot eliminar del seu navegador en qualsevol moment i normalment amb molta facilitat.

Tot això ha fet que apareguin sistemes diferents per a obtenir aquestes dades de manera més eficient i sense aquestes limitacions. Tanmateix, tots els sistemes que permetin la recopilació de dades personals de l'usuari, estan sotmesos a aquesta obligació d'obtenir l'autorització prèvia de l'usuari.

Això a fet que es desenvolupin sistemes per identificar l'usuari, com poden ser els que permeten el seguiment de l'empremta digital. Es tracta de la utilització d'algorismes dissenyats per identificar ordinadors concrets sense necessitat d'accedir a dades personals. Això permet inclús la identificació de cada usuari a partir del creuament amb d'altres informacions, com les seves preferències personals, pautes de navegació i dades similars. El tractament de tota aquesta informació la realitzen els algorismes de manera automàtica, sense la participació directa de cap persona física.

L'empremta digital és un instrument que permet la individualització de cada dispositiu i, per tant, la seva identificació. Aquesta empremta permet personalitzar el dispositiu quan està connectat a Internet, però s'ha utilitzat també amb altres finalitats, com pel seguiment de

productes amb suport electrònic com pel·lícules, música, llibres i altres productes similars.

## L'empremta digital dels productes electrònics

La generalització de l'ús de programes que permeten l'intercanvi d'arxius a Internet, mitjançant l'anomenat P2P, a fet que creixin notablement les infraccions contra els drets d'autor, cosa que fa que alguns d'aquests intercanvis puguin resultar il·legals.

Un dels sistemes utilitzats per tractar de controlar les còpies il·legals de pel·lícules, fotos, música i altres continguts presentats en suport electrònic, és la utilització d'empremtes digitals (*fingerprinting*). Consisteix en la inserció d'un conjunt de bits en els continguts que es vol protegir. Amb aquests bits s'inclou informació del comprador, que permet la seva identificació i per tant detectar el possible responsable de la còpia il·legal.

Una de les utilitzacions de les xarxes P2P que atenta directament contra els drets de propietat intel·lectual, es la difusió a través d'aquest sistema de pel·lícules gravades mitjançant el denominat *screener*. Es tracta de l'enregistrament il·legal d'una pel·lícula fet mitjançant una càmera de vídeo en una sala de cine.

Encara que les productores pressionen a les sales de cine per que evitin aquestes pràctiques, el cert és que el control és més aviat baix. Per aquest motiu s'han desenvolupat tècniques de detecció que permeten saber en quina sala s'ha gravat una còpia determinada de la pel·lícula. Una de les tècniques que es pot utilitzar és la de l'empremta digital.

El que interessa a la productora és poder identificar en quina sala de cine es va enregistrar, o al menys saber a partir de quina copia s'ha realitzat l'enregistrament il·legal. Això ho pot fer mitjançant l'empremta digital de la copia enregistrada il·legalment. Primer de tot haurà de separar el flux de vídeo i el flux d'àudio de la copia. Un cop separat, cada fotograma del flux de vídeo es descomprimeix i se li aplica l'algorisme de recuperació de la marca per poder veure a partir de quina copia s'ha produït l'enregistrament il·legal de la pel·lícula.

Al tenir cada còpia una marca d'aigua encastada diferent, es podria donar el cas que tenint accés a dues còpies es barreassin les marques de les dues còpies per tal que no es pogués identificar l'autor concret de tota la còpia. Tanmateix, tots els que han participat en les gravacions cometen una il·legalitat, que el Codi penal espanyol sanciona en el seu article 270.1.

El més rellevant en aquestes pràctiques és precisament la seva consideració de comunicació pública, independentment del sistema o tècnica utilitzada per realitzar la gravació clandestina. És important aquesta consideració, donat que no importa si aquesta gravació està realitzada per una persona física, o per qualsevol sistema o avenç tecnològic que pugui sortir en el futur:

“... el veritablement integrador del tipus és la modalitat de comunicació pública, que es pot dur a terme per qualsevol dels mitjans descrits anteriorment i fins i tot, sense

necessitat de modificar el tipus, per qualsevol altre sistema o avenç tecnològic que pugui sorgir en el futur...”<sup>137</sup>.

El seguiment dels productes mitjançant la seva empremta digital, o qualsevol altra tècnica futura, té com a objectiu precisament poder atribuir possibles responsabilitats a les persones, amb independència de que estigui més o menys automatitzada la seva gravació, o la seva identificació.

## L'empremta digital dels usuaris

Podem controlar des d'un servidor qui és l'usuari que s'està connectant per Internet, senzillament mirant la seva IP que l'identifica. Tanmateix, aquest sistema no és del tot fiable, doncs pot estar connectat a una xarxa amb un única IP, pot estar connectat a un *proxy* juntament a d'altres ordenadors, o pot tractar-se d'una IP dinàmica, que en la pràctica són les més freqüents en l'àmbit particular. D'altra banda, i com els tribunals han dictaminat, una IP no identifica per si sola un ordinador<sup>138</sup>. En definitiva, la identificació de l'usuari és poc segura amb aquest sistema. D'altra banda, les *cookies* també presenten dificultats, especialment l'esmentada necessitat de demanar la prèvia autorització de l'usuari. Per això és cada vegada més utilitzada l'empremta digital de cada dispositiu.

---

<sup>137</sup> Fonament de dret segon de la sentència 876/2001 de la Sala Penal del Tribunal Suprem, de 19 de maig de 2001.

<sup>138</sup> En aquest sentit, es famosa la sentència de l'1 de maig de 2012, del Jutge Gary R. Brown, del Districte Est de New York, en el cas “Bittorrent”.

La protecció de les dades personals i la protecció de la privacitat de les persones, ha sigut repetidament expressada pels Tribunals, inclús en alguns casos contra el criteri del propi legislador. Així, el Tribunal de Justícia de la Unió Europea, va haver d'intervenir per invalidar la Directiva sobre conservació de dades generades o tractades pels proveïdors de serveis de comunicacions electròniques<sup>139</sup>. En aquesta sentència el Tribunal especifica que la manera en que aquesta norma regula la retenció de dades, representa una forta ingerència en els drets fonamentals, al respecte de la vida privada i a la protecció de dades de caràcter personal. El Tribunal va qualificar aquest fet com d'especial gravetat, afegint que aquesta ingerència va més enllà de l'estrictament necessari<sup>140</sup>:

"... les dades que s'han de conservar permeten saber amb quina persona i de quina manera s'ha comunicat un abonat o un usuari registrat, determinar el moment de la comunicació i el lloc des del qual aquesta s'ha produït i conèixer la freqüència de les comunicacions de l'abonat o de l'usuari registrat amb determinades persones durant un període concret. Aquestes dades, considerades en el seu conjunt, poden proporcionar indicacions molt precises sobre la vida privada de les persones

---

<sup>139</sup> Sentència del Tribunal de Justícia de la Unió Europea C-293/12, de 8 d'abril de 2014, declarant la nul·litat de la Directiva 2006/24/CE, de 15 de març de 2006, sobre la conservació de dades generades o tractades en relació amb la prestació de serveis de comunicacions electròniques d'accés públic o de xarxes públiques de comunicacions i per la que es modifica la Directiva 2002/58/CE.

<sup>140</sup> Al nostre país, la transposició d'aquesta directiva comunitària va ser la Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.



les dades es conserven, com els hàbits de la vida quotidiana, els llocs de residència permanents o temporals, els desplaçaments diaris o altres, les activitats realitzades, les relacions socials i els mitjans socials freqüentats..."<sup>141</sup>.

## La signatura electrònica com a identificador

La identificació de l'usuari, o inclús el dels productes electrònics, tenen uns objectius que poden resultar necessaris per facilitar la navegació al llarg de la pàgina web, dificultar les còpies no autoritzades, o per molts altres similars. Tanmateix, les transaccions realitzades electrònicament han de poder garantir amb seguretat la identitat dels participants en la transacció comercial. Un dels mitjans utilitzats actualment és el de la signatura electrònica.

La signatura electrònica avançada, sempre que estigui degudament reconeguda, té al nostre país el mateix valor que la signatura feta físicament en paper i garanteix la identitat del signant i la integritat de les dades<sup>142</sup>. Així doncs, els contractes fets per via electrònica, sempre

---

<sup>141</sup> Sentència del Tribunal de Justícia de la Unió Europea, de 8 d'abril de 2014, en els casos C-293/12 i C-594/12.

<sup>142</sup> L'article 3.2 de la Llei 59/2003, de 19 de desembre de 2003, de signatura electrònica, especifica clarament aquest valor de la signatura electrònica avançada, a la que defineix com: "...la signatura electrònica que permet identificar al signant i detectar qualsevol canvi ulterior de les dades firmades, que està vinculada al firmant de manera única i a les dades a que es refereix i que ha sigut creada per mitjans que el signant pot mantenir sota el seu exclusiu control".

que estiguin signats electrònicament, tenen plena validesa i són admissibles en un judici com a prova documental<sup>143</sup>.

Aquesta validesa jurídica de la signatura electrònica permet garantir la identitat del signant, així com l'autenticitat i confidencialitat de les dades transmeses per Internet. De la importància d'aquesta figura és bona prova l'interès del legislador en la seva regulació. El Parlament Europeu va dictar el 1993 una Directiva que pretenia precisament potenciar la creació d'un marc jurídic homogeni a nivell de la Comunitat Europea<sup>144</sup>.

La mateixa Directiva Comunitària, establia la diferència entre la signatura electrònica i la signatura electrònica avançada. Aquesta última és la també coneguda com "Signatura Digital" i que defineix com:

"... la signatura electrònica que compleix els requisits següents:  
a) estar vinculada al signant de manera única; b) permetre la identificació del signant; c) haver estat creada utilitzant mitjans que el signant pot mantenir sota el seu control exclusiu; i d) estar vinculada a les dades a què es refereix de manera que qualsevol canvi ulterior d'aquests sigui detectable..."<sup>145</sup>.

Tal com explica Díaz Bermejo, la signatura electrònica es basa en un sistema de criptografia asimètrica. Utilitzen un algorisme per codificar el missatge de manera que solament pugui ser descodificat per qui tingui la

---

<sup>143</sup> Article 24 de la mateixa Llei 59/2003, de 19 de desembre de 2003, de signatura electrònica.

<sup>144</sup> Directiva 1999/93/CE del Parlament Europeu i del Consell, de 13 de desembre de 1999, per la que s'estableix un marc comunitari per a la signatura electrònica.

<sup>145</sup> Article 2.2 de la Directiva 1999/93/CE del Parlament Europeu i del Consell, de 13 de desembre de 1999, per la que s'estableix un marc comunitari per a la signatura electrònica.

clau pública corresponent. El sistema consisteix en parells de claus de manera que la informació encriptada per una de les claus només pot ser descriptada per l'altra clau del parell.

“... El parell de claus s'associa amb un sol interlocutor, així un component del parell (la clau privada) només és coneguda pel seu propietari mentre que l'altra part del parell (la clau pública) es publica àmpliament perquè tot el món pugui veure-la (en aquest cas destaca el famós criptosistema RSA les inicials són les dels seus creadors: Rivest, Shamir i Adelman). Aquesta clau pública és donada per un tercer que és el conegut com «autoritat de certificació»...”<sup>146</sup>.

Així, per exemple, a l'Estat espanyol el tipus de signatura electrònica que incorpora el e-DNI, és la signatura electrònica reconeguda. Aquesta signatura té el mateix valor sobre el document electrònic que la signatura manuscrita sobre el paper<sup>147</sup>. Es pot utilitzar la signatura digital del DNI a les compres a Internet<sup>148</sup> i en general es pot utilitzar per signar documents privats, segons el que estableix la propia legislació<sup>149</sup>. Les aplicacions que pot tenir són molt

---

<sup>146</sup> Díaz Bermejo, Guillermo “La firma electrónica y los servicios de certificación” Portico Legal S.L. (2008) Pot consultar-se a [http://www.porticolegal.com/pa\\_articulo.php?ref=311](http://www.porticolegal.com/pa_articulo.php?ref=311).

<sup>147</sup> D'acord a l'article 1.5 del Reial Decret 1553/2005, de 23 de desembre, pel qual es regula l'expedició del document nacional d'identitat i els seus certificats de signatura electrònica, modificat pel Reial Decret 869/2013, de 8 de novembre, “La signatura electrònica realitzada a través del Document Nacional d'Identitat tindrà respecte de les dades consignades en forma electrònica el mateix valor que la signatura manuscrita en relació amb les consignades en paper”.

<sup>148</sup> L'article 1.4 del Reial Decret 1553/2005, de 23 de desembre de 2005, pel qual es regula l'expedició del document nacional d'identitat i els seus certificats de signatura electrònica.

<sup>149</sup> L'article 6.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, el document electrònic serà suport de, entre d'altres, els documents privats.

amplies, des de per fer qualsevol tràmit electrònic amb l'administració pública fins com a simple mètode d'identificació davant de qualsevol receptor. És a dir, tant es pot utilitzar per fer la declaració de la renda, o sol·licitar el canvi de domicili de correus, com per a qualsevol compra a Internet o per operar amb els propis comptes corrents. El valor probatori que tindrà el document signat amb la signatura electrònica del e-DNI dependrà del tipus de document, és a dir, serà la mateixa validessa que tindria la signatura manuscrita dels rebuts que signem en els comerços convencionals.

Els tipus de signatures electròniques que es recullen a la legislació actual són tres, la simple, l'avançada i la reconeguda<sup>150</sup>. La signatura electrònica simple és qualsevol en que s'identifica el signant, és a dir, no hi ha cap altre requeriment tècnic o de seguretat. Per a la signatura electrònica avançada s'ha de complir, a part de l'identificació del signant, els requisits d'integritat del missatge i el no repudi d'aquest. És a dir, que es pot detectar si ha hagut variació en el document un cop signat i que no es pot negar la realització de la signatura. Per últim, la signatura electrònica reconeguda és la que, a part de complir els requisits de la signatura electrònica avançada, fa servir un certificat reconegut i és generada per un dispositiu segur. Aquesta signatura és la que dóna més fiabilitat i, per això, jurídicament té l'equiparació en els documents electrònics amb la signatura manuscrita dels documents en paper.

A l'administració de justícia, s'utilitza el sistema Lexnet. Es tracta d'un sistema de comunicació processal entre aquesta administració de justícia i altres organismes o institucions relacionades. Es basa en un correu electrònic de seguretat que utilitza la signatura electrònica reconeguda. La implantació d'aquest sistema serà gradual tant pel que fa a l'introducció del sistema en les oficines judicials i altres tipus d'organismes i institucions, com pel que fa a l'accés en els diversos tipus de procediments.

---

<sup>150</sup> Article 3 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

Quan una de les parts envia un escrit o document el sistema emmagatzema el missatge a la bústia virtual del destinatari durant trenta dies i genera un resguard electrònic que acredita que s'ha fet la transmissió correctament indicant la data i hora en que s'ha realitzat. Quan el destinatari accedeix a la seva bústia virtual el sistema genera un altre resguard electrònic que acredita la recepció i també indica la data i hora en que s'ha rebut.

En tots els casos, una signatura electrònica reconeguda ha de basar-se en un certificat generat per un dispositiu segur. La generació d'aquesta signatura, és a dir, de les claus que permeten la seva encriptació i desincriptació, està feta pels corresponents algorismes. Tanmateix, la responsabilitat pel seu ús fraudulent, per la perdua o destrucció de les claus o, per qualsevol altre irregularitat, és sempre de la persona, tenint els algorismes, els dispositius o els sistemes, la consideració de mers instruments als efectes d'aquesta responsabilitat.



## Capítol tretzè:

### **Cookies un sistema d'obtenció d'informació**

---

#### **La regulació legal de les "galetes" (*cookies*)**

Un dels dispositius que permeten l'obtenció automàtica de dades de l'usuari són les galetes, també anomenats "xivatos", o més usualment coneguts per la seva denominació en anglès "*cookies*". Aquestes dades són útils per facilitar la navegació per un lloc web sense necessitat d'estar constantment repetint la nostra clau d'accés, l'idioma de preferència, o el contingut de la nostra cistella de la compra i altres informacions semblants cada vegada que canviem de pàgina dins del mateix lloc. No obstant això, aquesta informació també pot ser utilitzada per a altres activitats no tan legítimes. Per aquest motiu, el legislador posa l'accent en la necessitat que es comuniqui clarament a l'usuari la instal·lació de *cookies* al seu sistema, així com l'ús de les dades obtingudes, i també la necessitat que s'autoritzi expressament aquest ús:

"... En els casos en què aquests dispositius, per exemple els anomenats «xivatos» (*cookies*), tinguin un propòsit legítim, com el de facilitar el subministrament de serveis de la societat de la informació, cal autoritzar-ne el seu ús amb la condició que se'n faciliti als usuaris informació clara i precisa, de conformitat amb la Directiva 95/46/CE, per garantir que els

usuaris estan al corrent de la informació que s'introdueix en l'equip terminal que estan utilitzant. Els usuaris han de tenir la possibilitat d'impedir que s'emmagatzemi en el seu equip terminal un «xivato» (*cookie*) o dispositiu semblant. [...] La presentació de la informació i de la comanda de consentiment o possibilitat de negativa ha de ser tan assequible per a l'usuari com sigui possible. No obstant això, es podrà supeditar l'accés a determinats continguts d'un lloc web a l'acceptació fundada d'un «xivato» (*cookie*) o dispositiu similar, en cas que aquest tingui un propòsit legítim..."<sup>151</sup>.

No són només les galetes els dispositius capaços d'obtenir dades de l'usuari mentre aquest navega per Internet, però sí que són un dels més utilitzats. Per això el legislador es refereix explícitament als programes que un cop instal·lats en els equips dels usuaris, permeten l'emmagatzematge i posterior recuperació de dades, que és precisament la comesa de les *cookies*. En l'exposició de motius del Reial Decret Llei 13/2012 de 30 de març, es reconeix el risc que aquests dispositius poden representar per a l'usuari, ja que es tracta de: "dispositius que poden facilitar la navegació per la xarxa però amb el seu ús poden revelar aspectes de l'esfera privada dels usuaris, pel que és important que els usuaris estiguin adequadament informats i disposin de mecanismes que els permetin preservar la seva privacitat"<sup>152</sup>.

---

<sup>151</sup> Considerant 25 de la 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.

<sup>152</sup> Apartat V de l'exposició de motius del Reial Decret-Llei 13/2012, de 30 de març, pel que es transposen directives en matèria de mercats interiors d'electricitat i gas i en matèria de



Per aquest motiu el Reial Decret-Llei 13/2012, de 30 de març, va modificar la Llei 34/2002, de serveis de la societat de la informació i de comerç electrònic, introduint l'exigència del consentiment dels usuaris abans d'incloure en els seus ordinadors programes informàtics com les galetes.

Aquesta expressa protecció de dades de caràcter personal establerta pel legislador, s'ha vist repetidament consolidada per la jurisprudència en diferents sentències i, això implica a més a més, el dret a controlar l'ús que es faci de les dades obtingudes mitjançant les galetes (*cookies*). Aquest dret implica que el ciutadà pot oposar-se a que les seves dades personals siguin utilitzades amb finalitats diferents d'aquelles que van justificar la seva obtenció:

"... Així doncs, en l'enjudiciament del primer grup de preceptes impugnats haurem de partir de la nostra doctrina respecte al dret fonamental que es deriva de l'art. 18.4 CE, doctrina sistematitzada a la STC 292/2000, de 30 de novembre, resolutòria del recurs d'inconstitucionalitat núm. 1463-2000, promogut pel Defensor del Poble respecte dels arts. 21.1 i 24.1 i 2 de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (d'ara endavant, LOPD). En el fonament jurídic 5 de l'esmentada sentència vam establir, recollint la doctrina d'anteriors pronunciaments d'aquest Tribunal, que la llavors anomenada «llibertat informàtica» es configura com «un dret a controlar l'ús de les dades inserides en un programa informàtic (*habeas data*) i

---

comunicacions electròniques, i pel que s'adopten mesures per a la correcció de les desviacions per desajustaments entre els costos i ingressos dels sectors elèctric i gasista.

comprèn, entre d'altres aspectes, l'oposició del ciutadà al fet que determinades dades personals siguin utilitzades per a finalitats diferents d'aquella legítima que va justificar la seva obtenció (SSTC 11/1998, FJ 5; 94/1998, FJ 4)». D'acord amb els fonaments jurídics 6 i 7 de l'esmentada STC 292/2000, aquest dret fonamental no redueix la seva protecció a les dades íntimes, sinó que el seu objecte és més ampli, referint-se a qualsevol tipus de dada personal i venint constituït el seu contingut per un feix de facultats consistents en diversos poders que imposen a tercers deures correlatius... "<sup>153</sup>.

## **Necessitat de prèvia autorització de l'usuari**

Atès que les galetes en general poden tenir una finalitat necessària per a l'activitat del lloc, la Llei estableix els casos en què es poden utilitzar aquests dispositius sense la necessitat de la prèvia autorització de l'usuari. Aquesta excepció s'estableix en funció de l'objectiu de la galeta utilitzada:

"... Quan sigui tècnicament possible i eficaç, el consentiment del destinatari per acceptar el tractament de les dades es pot facilitar mitjançant l'ús dels paràmetres adequats del navegador o d'altres aplicacions.

Això no impedirà el possible emmagatzematge o accés de caire tècnic només amb la finalitat d'efectuar la transmissió d'una

---

<sup>153</sup> Fonament jurídic quart, de la sentència del Tribunal Constitucional 17/2013, de 31 de gener de 2013.

comunicació per una xarxa de comunicacions electròniques o, en la mesura que sigui estrictament necessari, per a la prestació d'un servei de la societat de la informació expressament sol·licitat pel destinatari..."<sup>154</sup>.

Aquesta excepció en la necessitat d'obtenir el consentiment explícit de l'usuari del servei per a l'ús de *cookies* és lògica si tenim en compte que la pròpia dinàmica de moltes pàgines web necessita mantenir determinades dades de l'usuari mentre navega per aquesta pàgina o altres vinculades. El Grup de Protecció de Dades de l'Article 29, pel que fa al tractament de dades personals, va elaborar el Dictamen 4/2012 sobre l'exempció del requisit de consentiment de *cookies*, adoptat el 7 de juny del 2012.

En el citat dictamen es fa una relació del tipus de *cookies* que no precisen autorització expressa de l'usuari, atès que es refereixen a dades que són necessàries per efectuar la transmissió, o per a la prestació del servei<sup>155</sup>. Les *cookies* que en aquest Dictamen queden exemptes de la autorització prèvia són les següents:

1. “*Cookies* d'entrada de l'usuari (identificador de sessió) per la durada d'una sessió o *cookies* persistents limitades a unes hores en certs casos.

---

<sup>154</sup> Paràgrafs segon i tercer de l'article 22.2 de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic, redactat per l'apartat cinquè de la disposició final segona de la Llei 9/2014, de 9 de maig, general de telecomunicacions.

<sup>155</sup> Es tracta d'un Grup de treball creat per la Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, és un òrgan consultiu i independent europeu que s'ocupa de la protecció de dades i la privacitat.

2. *Cookies* d'autenticació utilitzades per prestar serveis autenticats per a la durada d'una sessió.
3. *Cookies* de seguretat centrades en l'usuari que s'utilitzen per detectar abusos d'autenticació per a una durada limitada i persistent.
4. *Cookies* de sessió de reproductor multimèdia, com ara els *flash player cookies*, per a la durada d'una sessió.
5. *Cookies* de sessió per equilibrar la càrrega, per a la durada de la sessió.
6. *Cookies* persistents de personalització de la interfície d'usuari, per a la durada d'una sessió (o alguna cosa més).
7. *Cookies* de tercers per compartir continguts socials pels membres connectats a una xarxa social”.

No obstant això, l'ús de galetes de tercers amb complements de continguts socials per a finalitats diferents de la prestació d'una funcionalitat explícitament demanada pels seus propis membres requereix el consentiment, especialment si aquestes finalitats impliquen el rastreig d'usuaris per mitjà de llocs web.

Un exemple característic seria el de les cistelles de la compra, en la qual es van acumulant els productes escollits pel comprador, o en general pel que fa a l'ús de formularis web. En aquests casos es poden utilitzar les anomenades galetes de sessió i d'entrada d'usuari, que mantenen les dades fins que el comprador doni per finalitzada la seva compra o d'omplir el formulari.

Tampoc seria necessària l'autorització prèvia per a l'ús de galetes d'identificació o les d'autenticació de l'usuari, ni les anomenades de

seguretat, que tenen per objecte la identificació d'intents repetits i erronis d'accés al lloc. Una cosa semblant passa amb les galetes de personalització de la comunicació establertes per l'usuari, en la qual l'idioma seleccionat, les opcions de visualització, o en general les preferències manifestades per establir aquesta comunicació s'han de poder retenir d'alguna manera si no volem que el usuari hagi d'introduir repetidament aquestes preferències després de cada acció que realitzi durant la sessió.

Hi ha altres galetes de sessió, que per motius tècnics estan també exceptuades de la necessitat de prèvia autorització, com poden ser les que emmagatzemen dades tècniques que permeten derivar l'usuari a un o un altre servidor de reserva per tal d'equilibrar la càrrega, o les que permeten mantenir dades necessàries per a la reproducció multimèdia, com la velocitat de la xarxa, la qualitat d'imatge i altres dades similars.

El mateix passa amb els *plug-in* o galetes de complement, que serveixen per intercanviar continguts socials, és a dir, són galetes de tercers que s'utilitzen per compartir continguts socials pels membres connectats a una xarxa social. No obstant això, el Dictamen 4/2012 aclareix que "l'ús de *cookies* de tercers amb complements de continguts socials per a fins diferents de la prestació d'una funcionalitat explícitament demanada pels seus propis membres requereix el consentiment, especialment si aquestes finalitats impliquen el rastreig d'usuaris a través de llocs web".

Tal com indica Pedro de Miguel Asensio, (Miguel Asensio, 2011) les galetes constitueixen un instrument bàsic de l'anomenada publicitat "comportamental" i plantegen especials riscos en relació amb el tractament d'informació personal sobre els usuaris d'Internet. D'altra

banda, el Dictamen 2/2010 sobre publicitat comportamental en línia, del Grup de Treball de la CE sobre protecció de dades personals recorda la necessària autorització per a l'enviament d'aquest tipus de publicitat.

Pel que fa a les galetes de publicitat en aquest Dictamen 4/2012 es manifesta que:

"... Les *cookies* de tercers que s'utilitzen en la publicitat comportamental no estan exemptes del requisit de consentiment, com ja es va assenyalar en el Dictamen 2/2010 i el Dictamen 16/2010 del Grup de Treball. El requisit de consentiment s'estén de forma natural a totes les *cookies* de tercers relacionades que operin i s'utilitzin en la publicitat, incloses les *cookies* utilitzades per a finalitats de limitació de la pressió venedora, inici de la sessió financera, afiliació publicitària, clic a la detecció del frau, investigació i anàlisi de mercats, millora i depuració de producte, ja que cap d'aquestes finalitats es pot considerar relacionada amb un servei o funcionalitat d'un servei de la societat de la informació, «explícitament sol·licitat per l'usuari», com exigeix el CRITERI B..."<sup>156</sup>.

És doncs necessari el previ consentiment dels destinataris de la publicitat perquè es puguin utilitzar les seves dades obtingudes mitjançant les galetes. No obstant això, l'ús no autoritzat de les dades obtingudes mitjançant galetes, que més freqüentment es pot observar, és precisament el de la publicitat comportamental, és a dir, aquella

---

<sup>156</sup> Dictamen 4/2012 sobre l'exempció del requisit de consentiment de *cookies*, adoptat el 7 de juny de 2012.

publicitat dirigida d'acord al comportament seguit a la xarxa per part de l'usuari. Per obtenir aquesta autorització és requisit indispensable que es faciliti a l'usuari una adequada informació, tal com indica el propi Tribunal Constitucional.

El Tribunal Constitucional a la STC 292/2000, de 30 de novembre, que delimita el contingut essencial del dret fonamental a la protecció de les dades personals, ha considerat el dret d'informació prèvia com un element indispensable del dret fonamental a la protecció de dades al declarar que:

"... són elements característics de la definició constitucional del dret fonamental a la protecció de dades personals dels drets de l'afectat a consentir sobre la recollida i ús de les seves dades personals i a saber-ne d'elles. I són indispensables per fer efectiu aquest contingut el reconeixement del dret a ser informat de qui posseeix les seves dades personals i amb quina finalitat, i el dret a poder oposar-se a aquesta possessió i ús requerint a qui correspongui que posi fi a la possessió i ús de les dades. És a dir, exigint del titular del fitxer que l'informi de quines dades posseeix sobre la seva persona, accedint als seus oportuns registres i assentaments, i quin destí han tingut, el que afecta també possibles cessionaris; i, si escau, requerir-li perquè els rectifiqui o els cancel·li..."<sup>157</sup>.

---

<sup>157</sup> Fonament jurídic setè de la Sentència 292/2000, de 30 de novembre de 2000, del Tribunal Constitucional, en el recurs d'inconstitucionalitat respecte dels articles 21.1 i 24.1 i 2 de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

En tot cas, la utilització de galetes s'ha de fer d'acord amb el que estableix la legislació<sup>158</sup>.

## La política de galetes de Google

Al març de 2012, Google va modificar la seva política de privacitat i les condicions d'ús de la majoria dels seus serveis. A partir d'aquesta modificació es possibilitava que la informació facilitada per un servei, es pogués combinar amb l'obtinguda en altres i utilitzar-se amb qualsevol finalitat. Això constituïa un ús de les dades personals abusiu i no autoritzat expressament per l'usuari.

A l'abril de 2013 les autoritats de protecció de dades d'Alemanya, Espanya, França, Holanda, Itàlia i el Regne Unit van iniciar coordinadament actuacions d'investigació i procediments sancionadors d'acord a les seves respectives normatives internes nacionals, contra la política de galetes de Google.

Així, l'Agència Espanyola de Protecció de Dades, després de diferents requeriments previs a Google, va dictar una resolució sancionadora en considerar que Google vulnerava greument el dret a la protecció de les

---

<sup>158</sup> L'article 5 de la Llei Orgànica de protecció de dades de caràcter personal, estableix que: "1. Els interessats als quals se'ls hi sol licitin dades personals han de ser prèviament informats de manera expressa, precisa i inequívoca: a) De l'existència d'un fitxer o tractament de dades de caràcter personal, de la finalitat de la recollida d'aquestes i dels destinataris de la informació. b) Del caràcter obligatori o facultatiu de la resposta a les preguntes que els siguin plantejades. c) De les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les. d) De la possibilitat d'exercitar els drets d'accés, rectificació, cancel·lació i oposició. e) De la identitat i adreça del responsable del tractament o, si s'escau, del seu representant..."



dades personals reconegut a tots els ciutadans per l'article 18 de la Constitució Espanyola i regulat en la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal. En aquesta resolució l'Agència manifesta haver constatat que "Google recull i tracta il·legítimament informació personal".

"... Les actuacions d'inspecció han permès comprovar que Google recopila informació personal a través de gairebé un centenar de serveis i productes que ofereix a Espanya, sense proporcionar en molts casos una informació adequada sobre quines dades es recullen, per a quines finalitats s'utilitzen i sense obtenir un consentiment vàlid dels seus titulars. Així, per exemple, **no s'informa amb claredat** als usuaris de Gmail que es realitza un filtrat del contingut del correu i dels fitxers annexos per inserir publicitat. Quan s'informa, s'utilitza una terminologia imprecisa, amb expressions genèriques i poc clares que impedeixen als usuaris conèixer el significat real del que es planteja. [...] La manca d'informació adequada, particularment sobre les finalitats específiques que justifiquen el tractament de les dades, impedeix que es pugui considerar que hi ha un consentiment específic i informat i, en conseqüència, vàlid..."<sup>159</sup>.

Així mateix, consta acreditat que es tracta d'un incompliment de naturalesa estructural del servei, ja que amb independència de la configuració escollida pels editors en dissenyar els blogs, aquesta empresa és perfectament coneixedora de que utilitza galetes analítiques

---

<sup>159</sup> Resolució R/02892/2013 instruït a Google Inc. i Google Spain S.L. en el procediment número PS/00345/2013 de l'Agència Espanyola de Protecció de Dades.

i de publicitat en els equips terminals dels usuaris que naveguen pels llocs web creats sota la infraestructura *Blogger* sense informar d'aquest tractament de dades als esmentats editors i als visitants dels llocs web en qüestió, incomplint d'aquesta manera el requisit d'obtenir el consentiment informat dels destinataris del servei (editors i visitants) en els equips terminals dels quals s'instal·laven aquestes galetes, al no intervenir la informació prèvia, clara i completa sobre galetes requerida per poder considerar que s'ha consentit en forma vàlida l'ús d'aquests dispositius.

En aquesta resolució s'estableix que Google combina la informació personal obtinguda per mitjà de diversos serveis i la utilitza amb múltiples finalitats que no s'expliquen amb claredat. Amb això s'utilitzen les dades per a finalitats diferents d'aquelles per a les quals s'han obtingut. També es critica que Google emmagatzema i conserva dades personals per períodes de temps indeterminats o injustificats, contravenint amb això el mandat legal de procedir a la seva cancel·lació quan deixen de ser necessàries per a la finalitat que va determinar la seva recollida.

Quan és el propi sistema el que, sense la participació directa de l'anunciant, recopila les dades obtingudes mitjançant galetes (que també s'incorporen a l'ordinador de l'usuari de manera automàtica) el responsable ho és quan no ha pres les mesures adequades per evitar l'ús inadequat de les dades obtingudes, amb independència que tot el procés s'hagi realitzat de manera automatitzada, ja que el rellevant és la diligència desplegada a l'acció pel subjecte, tal com indica la mateixa Agència Espanyola de Protecció de Dades:

"... En relació amb l'absència de culpabilitat al·legada, convé recordar que des del punt de vista material, la culpabilitat consisteix en la capacitat que té el subjecte obligat per obrar de manera diferent i, per tant, d'acord amb l'ordenament jurídic. De tal manera que el rellevant és la diligència desplegada a l'acció pel subjecte, el que exclou la imposició d'una sanció, únicament sobre la base del mer resultat, és a dir al principi de responsabilitat objectiva ..."160.

---

<sup>160</sup> Fonament de Dret VIII de la Resolució R/00936/2014 instruït a Google Inc. en el procediment número PS/00320/2013 de l'Agència Espanyola de Protecció de Dades.



## Capítol catorzè: Enllaços i investigació per internet

---

### Navegació, enllaços i P2P

Un dels recursos per dirigir a l'usuari des d'un lloc concret de la web cap a un altre lloc, són els enllaços, més coneguts per la seva denominació en anglès *links*. Els enllaços són sectors d'una pàgina web que s'activen en prémer sobre ells l'usuari, dirigint al mateix cap a una altra pàgina o a un altre lloc dins de la pròpia pàgina, segons com estigui programat aquest enllaç. Normalment els enllaços estan programats sobre un text, una imatge o un espai assenyalat de la pròpia pàgina, de manera que al pitjar sobre una paraula, una frase, un dibuix o qualsevol altre lloc assenyalat, s'activa l'enllaç i porta a l'usuari al lloc previst.

A més dels enllaços simples, o enllaços HREF, hi ha diferents denominacions per als mateixos en funció de la seva comesa concreta. Així, si l'enllaç dirigeix a l'usuari cap a la pàgina d'inici del lloc, en anglès *home*, estem davant d'un enllaç de superfície o *surface link*. Si l'enllaç dirigeix a l'usuari a una pàgina interior d'un altre lloc web, es tracta d'un enllaç profund, o *deep link*. Quan en prémer sobre l'enllaç es presenten els continguts d'una altra pàgina sense sortir d'aquella en què està situat l'enllaç, estem davant d'un enllaç ensamblat, o el que es coneix com a *embedded link*.

Un cas d'enllaç especial és el dels enllaços P2P. En aquest cas, l'enllaç en lloc de dirigir l'usuari a un altre lloc, i amb això acabar la seva funció, el dirigeix a una pàgina concreta, en la qual hi ha un programa que permet compartir arxius amb altres usuaris. Els usuaris que es connecten amb aquest programa posen a disposició de la resta d'usuaris aquells fitxers que volen d'entre els que mantenen en el seu propi equip. Això permet l'intercanvi entre usuaris d'obres audiovisuals, literàries i tot tipus d'arxius, alguns dels quals poden estar protegits per drets de *copyright* de tercers<sup>161</sup>. L'intercanvi d'arxius via P2P es lícit en principi, sempre que els materials objecte de transferència no estiguin subjectes a drets exclusius de tercers o es tingui la deguda autorització dels titulars d'aquests drets:

“... Els protocols «*Peer to Peer*» (o P2P) permeten la connexió entre ordinadors i amb això el que diversos subjectes puguin compartir continguts. L'evolució d'aquests protocols ha estat, a mesura que l'avanç tecnològic ho ha permès, cap a la descentralització, de manera que ja no necessiten un servidor central que actuï d'interconnexió, sinó que la tecnologia permet que a través d'un programa informàtic els ordinadors dels usuaris es connectin directament entre si, en forma d'una xarxa, i puguin accedir als continguts que els altres connectats al sistema tenen emmagatzemats per derivar cap al disc dur de l'ordinador; cada usuari pot funcionar així com a client i com a

---

<sup>161</sup> Una xarxa *peer-to-peer* (P2P), o el que és el mateix una xarxa punt a punt, es basa en una relació entre iguals, és a dir, cadascun dels clients que demanen un recurs són alhora proveïdors d'altres recursos i es creen relacions d'igual a igual. En aquest cas les relacions no són fixes sinó que varien segons el recurs sol·licitat i el moment en què es demana però no es pot garantir que un recurs estigui sempre disponible.

servidor a la vegada. La realització d'aquests intercanvis d'arxius entre particulars constitueix una activitat perfectament lícita en la mesura en què els que siguin objecte de transferència no estiguin subjectes a drets exclusius de tercer o es compti amb l'autorització d'aquest..."<sup>162</sup>.

Així doncs, l'intercanvi d'arxius entre particulars mitjançant P2P és una activitat lícita si no concorren altres situacions. Per això, el fet de ser mers enllaçadors en aquest sistema també resulta una activitat lícita per si mateixa:

"... L'atestat policial recull que l'imputat és titular dels següents dominis, respecte dels quals percep ingressos econòmics: «maspeliculas.com», «divxonline.com.es», «emulemas.com», «divxonline.info», «seriesonline.us» i «estrenosonline.es» i que de tots ells, «maspeliculas.com» i «emulems.com» són mers enllaçadors, tenen un sistema de funcionament similar al «Sharaemula», localitzant arxius en programes P2P per facilitar la seva descàrrega (no subjectes a restriccions segons la LSSI). Es descarten, per tant, als efectes de la present investigació ..." <sup>163</sup>.

---

<sup>162</sup> Sentència 103/2014, de l'Audiència Provincial de Madrid, de 31 de març de 2014, en el recurs d'apel·lació 631/2012 de Productores de Música de España (PROMUSICAE), Universal Music Spain S.L., Warner Music Spain S.L., Sony BMG Music Entertainment Spain S.A., i Emi Music Spain S.A., contra D. Cesareo, Optisoft S.L., Piolet Networks S.L. i M Punto 2 Punto Technologies S.A.

<sup>163</sup> Fonament jurídic tercer de la Sentència 630/2010 de la Secció Tercera, de l'Audiència Provincial de València, de 26 d'octubre de 2010.

## Els enllaços com a comunicació pública

Des d'una perspectiva jurídica una de les principals qüestions és saber si els enllaços es poden considerar comunicació pública o no. Malgrat que la Directiva 2000/31/CE del Parlament Europeu i del Consell, de 8 de juny de 2000, sobre allotjament de dades, va ser incorporada en el marc legislatiu dels països membres, tot i així, la interpretació divergent sobre la responsabilitat dels prestadors de serveis segueix sent molt comú. Així per exemple, en relació a la incorporació d'enllaços a pàgines amb continguts que poden infringir la propietat intel·lectual, algunes sentències no fan responsable al proveïdor de l'enllaç, mentre que també són freqüents les resolucions que estimen el contrari, és a dir, que el proveïdor de l'enllaç és co-responsable de la infracció que es pugui haver comés.

Un exemple d'aquesta consideració el podem veure en l'assumpte dels llocs web [www.divxonline.info](http://www.divxonline.info), [www.estrenosonline.es](http://www.estrenosonline.es), així com a [www.seriesonline.es](http://www.seriesonline.es), en els quals es posaven pel·lícules a disposició dels usuaris d'Internet, o es permetia la seva descàrrega sense autorització dels titulars, algunes de les quals havien estat gravades per *streaming*.

L'Audiència Provincial de València va ratificar al 2010<sup>164</sup> la sentència condemnatòria que va imposar el Jutjat Penal número 3 de València a l'administrador d'aquestes pàgines web, per la comissió d'un delictes contra la propietat intel·lectual, en considerar el tribunal que l'activitat d'enllaçar constitueix un acte de comunicació pública tot i que la pàgina en qüestió no allotgi els continguts, si no pel simple fet d'enllaçar amb aquests. A la seva sentència el tribunal recull la definició que fa del

---

<sup>164</sup> Sentència de la Secció Tercera de l'Audiència Provincial de València de 26 d'octubre de 2010.



concepte de comunicació pública el text refós de la Llei de Propietat Intel·lectual:

"... S'entendrà per comunicació pública tot acte pel qual una pluralitat de persones pugui tenir accés a l'obra sense prèvia distribució d'exemplars a cadascuna d'elles.

No es considerarà pública la comunicació quan se celebri dins d'un àmbit estrictament domèstic que no estigui integrat o connectat a una xarxa de difusió de qualsevol tipus ..."165.

Si es consideressin els enllaços com a comunicació pública, el responsable de la seva incorporació ho seria també de les possibles infraccions que es poguessin cometre, com per exemple si s'atempta contra els drets d'autor legalment protegits. Així, la Directiva 2001/29/CE estableix en el seu articulat que:

"... Els Estats membres establiran en favor dels autors el dret exclusiu a autoritzar o prohibir qualsevol comunicació al públic de les seves obres, per procediments electrònics amb fil o sense fil, inclosa la posada a disposició del públic de les seves obres de manera que qualsevol persona pugui accedir-hi des del lloc i en el moment que triï..."166.

---

<sup>165</sup> Article 20.2 del Reial Decret Legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de Propietat Intel·lectual, regularitzant, aclarint i harmonitzant les disposicions legals vigents sobre la matèria.

<sup>166</sup> Article 3, apartat 1, de la Directiva 2001/29/CE del Parlament Europeu i del Consell, de 22 de maig de 2001, relativa a l'harmonització de determinats aspectes dels drets d'autor i drets afins als drets d'autor en la societat de la informació.

Si per contra, els enllaços no tenen la consideració de comunicació pública, estarien exempts d'aquesta responsabilitat, sempre que l'enllaç condueixi a obres que es poden consultar lliurement en una altra pàgina d'Internet. Aquesta qüestió ha estat recollida pel Tribunal de Justícia de la Unió Europea, en una recent sentència pel denominat "cas Svensson", el tribunal determina que els enllaços com els aquí esmentats, no constitueixen una comunicació pública:

"... En virtut de tot l'exposat, el Tribunal de Justícia (Sala Quarta) declara: 1) L'article 3, apartat 1, de la Directiva 2001/29/CE del Parlament Europeu i del Consell, de 22 de maig de 2001, relativa a l'harmonització de determinats aspectes dels drets d'autor i drets afins als drets d'autor en la societat de la informació, s'ha d'interpretar en el sentit que no constitueix un acte de comunicació al públic, a efectes d'aquesta disposició, la presentació en una pàgina d'Internet d'enllaços sobre els quals es pot prémer i que condueixen a obres que poden consultar lliurement en una altra pàgina d'Internet..."<sup>167</sup>.

D'acord amb aquesta sentència, per que hi hagi comunicació pública és necessari que aquesta es dirigeixi a un públic nou, diferent a aquell inclòs en l'autorització donada pels titulars dels drets d'autor per accedir a l'obra en qüestió. Donat que, a més a més, no es pot exigir una obligació general de vigilància sobre els continguts als que s'enllaça, no existiria responsabilitat al no ser el responsable de la comunicació pública. Tal com diu Andy Ramos:

---

<sup>167</sup> Apartat 42 de la Sentència de la Sala Quarta del Tribunal de Justícia de la Unió Europea, de 13 de febrer de 2014, en l'assumpte C-466/12.

“... el TJUE recorda la línia jurisprudencial de la cort, que exigeix l’existència d’un «Públic Nou» (concepte que no és nou i al que ja es feia esment en l’assumpte C-306/05, encara que és freqüent objecte de polèmica) perquè el titular de dret pugui oposar-se (o exigir una retribució) davant un determinat acte de comunicació pública. En el present cas, com la demandada dirigia als seus usuaris al web del diari on es publicava (lícitament) les obres, el Tribunal ha considerat que es dirigia al mateix públic que aquesta última, perquè «el públic destinatari de la comunicació inicial era el conjunto dels usuaris potencials de la pàgina en què es va realitzar», mitjançant la publicació d’un enllaç cap a l’obra.

Per tant, en ser qualsevol internauta el destinatari potencial de l’obra facilitada en la web del diari, qualsevol enllaç a la mateixa es considerarà un acte de comunicació, però no pública...”<sup>168</sup>.

Aquesta responsabilitat sí que existiria si el titular dels drets fa un requeriment per a que es retiri aquet enllaç perquè, per exemple, permet accedir a l’obra a més persones de les inicialment autoritzades per aquest titular, i no es fes cas d’aquest requeriment. En aquest cas el responsable de l’enllaç no podria al·legar manca de coneixement efectiu, pel que existiria responsabilitat directa pels enllaços. També hi ha responsabilitat si l’enllaç permet evitar les mesures de restricció de la

---

<sup>168</sup> Ramos, Andy. “Caso Svensson: Un Enlace de Internet constituye un acto de comunicación pública (cuando se dirige a un público nuevo)” Interiuris.com (2014) Interiuris.com es tracta d’un blog centrat en temes de propietat intel·lectual, mantingut per Andy Ramos. Pot consultar-se aquest article a: <http://www.interiuris.com/blog/?p=989>.

pàgina en què està l'obra protegida amb les que es limita l'accés a un públic concret.

## Allotjament d'arxius: El cas Megaupload

El 5 de gener de 2012, el Departament de Justícia dels Estats Units, sota la pressió de la indústria de l'entreteniment, va presentar una demanda contra Kim Dotcom i Megaupload. Les autoritats nord-americanes van acusar Kim Dotcom de conspiració per cometre una infracció de drets d'autor. Després de tancaments similars de LimeWire<sup>169</sup>, Kazaa<sup>170</sup>, Napster<sup>171</sup> i altres, el cas semblava amb un final clar però hi va haver algunes diferències crucials.

---

<sup>169</sup> En el cas *Arista Records LLC et al. v. Lime Group LLC et al.* 715 F. Supp. 2d 481 (2010), després de cinc anys en una batalla judicial i que al maig de 2010 el jutge federal dictaminés que els usuaris de LimeWire cometien "una quantitat substancial de vulneració dels drets de propietat intel·lectual" i que la companyia matriu del grup Lime "no havia pres mesures significatives per mitigar la infracció", Mark Gorton, fundador de LimeWire, va acordar en 2011 compensar els quatre majors segells discogràfics d'Estats Units per danys i perjudicis amb 105 milions de dòlars, en un acord extrajudicial.

<sup>170</sup> En el cas *Metro-Goldwyn-Mayer Studios, Inc, et al. v. Grokster, Ltd, et al.* 545 US 913 (2005), Kazaa per poder fugir de la llei va vendre la interfície a Sharman Networks (una empresa creada uns dies abans amb servidors a Dinamarca i constituïda a Vanuatu, on no s'accepten els tractats internacionals sobre els drets de propietat intel·lectual). A part el domini i els empleats estaven a nom de LEF Interactive, empresa constituïda a Austràlia, i el codi del programa va ser transferit a Blastoise Ltd, empresa constituïda a les Illes Verges Britàniques. Tot i que la demanda contra Kazaa va ser abandonada per tenir la seva seu a Vanatu, el propi fet d'estar en Vanatu li va impedir emprendre accions legals contra altres programes que clonaven al de Kazaa i que li van fer perdre els seus usuaris. El 2006 Kazaa va acceptar pagar la indústria discogràfica 115 milions i esdevenir un servei legítim, un preu superior que al seu codemandat Grokster, que el 2005 va pagar 50 milions després que la decisió de la cort

En primer lloc, a diferència d'altres llocs d'intercanvi d'arxius *peer-to-peer* (P2P), Megaupload no era més que un lloc d'allotjament d'arxius tradicional. En molts aspectes tenia molt més en comú amb serveis d'empreses com Google, Amazon o Microsoft.

En segon lloc, en el moment en què Kim Dotcom va ser detingut i els seus béns van ser confiscats el 2012, ja portava diversos mesos vivint a Nova Zelanda com a resident permanent. El fet d'un entorn internacional ha fet que sigui extremadament difícil per als Estats Units defensar els seus interessos aplicant pressió sobre el senyor Dotcom.

Després de l'acusació del Departament de Justícia dels Estats Units, la policia de Nova Zelanda va començar a espionar el senyor Dotcom mitjançant el seu servei d'intel·ligència (GCSB)<sup>172</sup>. Al cap de dues setmanes, les autoritats de Nova Zelanda van procedir a la detenció del

---

concloués que el servei podria ser considerat responsable de la infracció de drets d'autor pels seus usuaris.

<sup>171</sup> El cas *A & M Records, Inc v. Napster, Inc* 239 F. 3d 1004 (2001) es pot considerar un dels primers que va tractar sobre programes de descàrrega de xarxa punt a punt pel que la indústria discogràfica no estava molt disposada a arribar a un acord ja que volien el precedent legal. Al setembre de 2001 Napster va acordar pagar 26 milions de dòlars a la indústria discogràfica i després de dos anys de la lluita judicial, Napster va ser finalment tancat (encara que posteriorment va reaparèixer com un servei legal).

<sup>172</sup> Segons la seva pàgina web (<http://www.gcsb.govt.nz/our-work/>), el Government Communications Security Bureau (GCSB) contribueix a la seguretat nacional de Nova Zelanda, proporcionant:

- Garantia de la informació i la seguretat cibernètica per al Govern de Nova Zelanda i les organitzacions de la seva infraestructura crítica;
- Intel·ligència Estrangera per als prenedors de decisions del govern;
- Cooperació i assistència a d'altres agències del govern de Nova Zelanda.

senyor Dotcom i alguns dels seus empleats, igual que embargar els seus actius a Nova Zelanda i la congelació dels seus actius a l'estranger.

Aquesta actuació del GCSB va ser declarada il·legal pel Tribunal Superior de Nova Zelanda<sup>173</sup> i va fer que el primer ministre neozelandès hagués de disculpar-se<sup>174</sup>.

Encara queda pendent la vista sobre l'extradició o no del senyor Dotcom als Estats Units que es té prevista per al 16 de febrer de 2015. En cas que no es produeixi l'extradició, el cas estarà tancat, però de produir-se aquesta extradició, es pot preveure un cas llarg i amb un final similar al dels casos anteriorment esmentats.

## Recopilació automàtica d'enllaços i continguts

La sentència Svensson<sup>175</sup> deixà clar que, excepte en els casos esmentats, els enllaços poden comportar responsabilitat. Tanmateix, el tema

---

<sup>173</sup> La jutge de l'Alt Tribunal de Nova Zelanda, Helen Winkelman, va dictaminar el desembre de 2012 que l'espionatge que s'havia fet sobre el senyor Dotcom era il·legal i que aquest podria demandar la GCSB per danys i perjudicis. Així i tot, al juliol de 2014 la policia va donar a conèixer la seva decisió arran d'una investigació sobre la denúncia del Dr Norman a la interceptació il·legal de la GCSB de les comunicacions dels neozelandesos. En aquest informe, la policia va trobar que Kim Dotcom i el seu soci Bram van der Kolk van ser espiats il·legalment, però ja que el personal de l'GCSB no va actuar amb intenció criminal, ningú hauria de retre comptes sobre aquesta vigilància.

<sup>174</sup> John Key va fer les següents declaracions el 27 de setembre de 2012: "Demano disculpes al senyor Dotcom, demano disculpes als neozelandesos, perquè cada neozelandès que es troba dins de la categoria de tenir la residència permanent o és un ciutadà de Nova Zelanda té dret a ser protegit de la llei quan es tracta de la GCSB, i hem fracassat a proporcionar l'adequada protecció per a ell".

enjudiciat es refereix a un cas en que és el propi sistema el que recopila els enllaços que s'ofereixen al públic. Les tasques de recopilació, de notícies de premsa en aquest cas, i la seva incorporació en forma d'enllaços posats a disposició dels usuaris, era realitzada de manera automàtica pel propi sistema, sense la intervenció directa de cap esser humà. El Tribunal, però, no fa cap diferència als efectes de la possible responsabilitat, si els enllaços son recopilats automàticament o ho son directament per un esser humà. La responsabilitat és en tot cas de la persona responsable de la pàgina en la que estan incorporats els enllaços.

Pàgines com Google News, i altres recopiladors de notícies, presenten a l'usuari les primeres línies de les diferents notícies recopilades automàticament des de diferents mitjans, i en cada una d'elles situa un enllaç que condueix a l'article de la publicació en qüestió<sup>176</sup>.

En aquest sentit, encara és més complexa el cas dels sistemes automatitzats que no únicament recopilant notícies d'altres mitjans, sinó que el mateix sistema elabora aquestes notícies sense intervenció humana directa, excepte la supervisió que cada mitjà vulgui establir. A partir de les dades, estadístiques, fets succeïts i d'altres fonts recopilades pel sistema, aquest elabora les notícies a partir d'algorismes matemàtics.

Algunes de les més recents experiències en aquest camp són la de l'agència de notícies Associated Press; Secció d'esports de The New York

---

<sup>175</sup> Sentència de la Sala Quarta del Tribunal de Justícia de la Unió Europea, de 13 de febrer de 2014, en l'assumpte C-466/12.

<sup>176</sup> Es pot consultar aquesta pàgina a: <http://news.google.es/>

Times; Los Angeles Times; Forbes, i d'altres similars. Són cada vegada més nombrosos els programes que faciliten aquesta confecció automatitzada d'articles periodístics.

Narrative Science, creat a la Northwestern University; Yseop, pot escriure en anglès, castellà, francès i alemany; Flipboard pot dissenyar i compaginar revistes; Truth Teller analitza discursos; Storify crea histories des dels continguts publicats a les xarxes socials<sup>177</sup>. En tots aquests casos, tanmateix, la responsabilitat pel que s'ha publicat segueix sent de persones com poden ser l'editor, el director del mitjà, o el supervisor del sistema.

---

<sup>177</sup> Es pot consultar el funcionament d'aquests programes a:

- Flipboard: (<https://flipboard.com/>)
- Yseop: (<http://www.yseop.com/FR/home.php>)
- Narrative Science: (<http://www.narrativescience.com/>)
- Truth Teller: (<http://truthteller.washingtonpost.com/>)
- Storify: (<https://storify.com/>)



## **Capítol quinzè: Privacitat i dret a la intimitat**

---

### **Protecció jurídica de la intimitat**

L'acord de l'Organització Mundial de Comerç, el 15 d'abril de 1994, en vigor des de l'1 de gener de 1995, sobre aspectes dels drets de propietat intel·lectual relacionats amb el comerç (ADPIC) va establir el marc relatiu a la protecció d'aquests drets. Aquest acord pretenia recopilar les diferents normatives existents en aquell moment sobre drets d'autor, denominacions d'origen, marques de fàbrica, patents i en general tots aquells drets vinculats a la propietat intel·lectual.

Aquests drets de propietat intel·lectual podrien entrar en conflicte amb el dret d'informació, de manera que l'acord ADPIC deixa clar que en cas d'infracció contra la propietat intel·lectual, les autoritats judicials poden ordenar a l'infractor que faciliti al perjudicat les dades d'aquelles terceres persones que van produir o distribuir l'objecte de la infracció. Així, l'article 47 de l'acord ADPIC, que versa específicament sobre el dret d'informació, estableix:

"... Els membres podran disposar que, tret que resulti desproporcionat amb la gravetat de la infracció, les autoritats judicials puguin ordenar a l'infractor que informi al titular del dret sobre la identitat dels tercers que hagin participat en la

producció i distribució dels béns o serveis infractors, i sobre els seus circuits de distribució..."

En tots els casos, el proveïdor dels serveis ha de garantir els drets dels seus usuaris. Si d'una banda el venedor pot demanar les dades del comprador necessàries per a la plena identificació, així com els que siguin necessaris per oferir un servei adequat, no és menys cert que també ha de garantir la confidencialitat d'aquestes dades, ja que s'afecten drets fonamentals dels usuaris, com el dret al secret de les comunicacions i el dret a la intimitat personal, tal com repetidament ha vingut assenyalant la jurisprudència en diferents sentències:

"... Ambdós drets en presència -el dret al secret de les comunicacions i el dret a la intimitat personal- tenen la categoria de fonamentals i, per això, gaudeixen d'una protecció reforçada enfront de tot gènere d'intromissions, incloses les que es puguin deure a una iniciativa oficial. Això fa que qualsevol invasió d'aquest espai, personalíssim i sobreprotegit, hagi d'estar constitucional i legalment justificada, sense ombra de dubte..."<sup>178</sup>.

Quan un usuari navega per Internet, i específicament quan realitza operacions de comerç electrònic, pot revelar dades sobre la seva personalitat o del més profund de la seva intimitat. El venedor pot accedir a dades del comprador referents a la seva ideologia, les seves creences religioses, les seves aficions personals, la seva salut, les seves orientacions sexuals i altres similars. La legislació i la jurisprudència ha

---

<sup>178</sup> Fonament de dret quart de la sentència 156/2008 de la Sala del Penal del Tribunal Suprem, de 8 d'abril de 2008.

establert àmbits de protecció d'aquells béns jurídics que es puguin veure afectats per tot això. El Tribunal Constitucional, per exemple, considera que la informació que es deriva del comerç electrònic forma part de l'àmbit personal de la intimitat i, per tant, ha de ser constitucionalment protegida:

"... És evident que quan el seu titular navega per Internet, participa en fòrums de conversa o xarxes socials, descàrrega arxius o documents, realitza operacions de comerç electrònic, forma part de grups de notícies, entre altres possibilitats, està revelant dades sobre la seva personalitat, que poden afectar el nucli més profund de la seva intimitat per referir-se a ideologies, creences religioses, aficions personals, informació sobre la salut, orientacions sexuals, etc..."<sup>179</sup>.

La 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, recull específicament aquesta protecció a les dades personals.

El manteniment de la privacitat dels usuaris pot entrar en conflicte amb altres interessos. Així per exemple, el 2008 Telefónica d'Espanya es va negar a facilitar a "Productors de Música d'Espanya (Promusicae)" les dades de les persones que havien utilitzat els seus serveis per a la connexió a Internet, per tal d'identificar aquells que descarregaven obres protegides per *copyright*. El Jutjat del Mercantil número 5 de

---

<sup>179</sup> Fonament jurídic tercer de la sentència 173/2011 de la Sala Segona del Tribunal Constitucional, de 7 de novembre de 2011.

Madrid va sol·licitar una decisió prejudicial al Tribunal de Justícia de la UE, sobre l'obligació dels prestadors de serveis de mantenir i, si escau, facilitar aquestes dades. El Tribunal es va manifestar interpretant que les normes sobre el tema:

"... no obliguen als Estats membres a imposar, en una situació com la de l'assumpte principal, el deure de comunicar dades personals per tal de garantir la protecció efectiva dels drets d'autor en el marc d'un procediment civil. No obstant això, el Dret comunitari exigeix que aquests Estats membres, a l'hora d'adaptar el seu ordenament jurídic intern a aquestes Directives, procurin basar-se en una interpretació d'aquestes que garanteixi un just equilibri entre els diferents drets fonamentals protegits per l'ordenament jurídic comunitari..."<sup>180</sup>.

La mateixa sentència estableix que entre els principis generals del dret que en les esmentades normes nacionals s'han d'atendre hi ha el principi de proporcionalitat. Tal i com s'ha vist anteriorment, aquesta mateixa exigència de proporcionalitat també la recullen els acords ADPIC de la Ronda Uruguai de l'Organització Mundial de Comerç, en el seu article 47.

---

<sup>180</sup> Sentència del Tribunal de Justícia (Gran Sala), de 29 de gener de 2008, en l'assumpte C-275/06, que té per objecte una petició de decisió prejudicial plantejada pel Jutjat del Mercantil nº 5 de Madrid, en el cas Productores de Música de España (Promusicae) i Telefónica de España, S.A.U.

## La cibercensura

És una constant en el desenvolupament de les tecnologies de la informació la permanent tensió entre els usuaris dels sistemes de comunicació, que pretenen mantenir la privacitat de les seves comunicacions, i aquells que pretenen accedir o fins i tot controlar les comunicacions. Entre els segons destaquen precisament els governs de tots els colors i ideologies.

Un dels sistemes més directes per denegar l'accés de determinat usuari o grup d'usuaris a una pàgina web o un servidor en concret, és el bloqueig de la IP o d'un rang d'adreces. Això es pot fer mitjançant diferents tecnologies de filtratge, tot i que la més usual és la configuració d'un fitxer de control d'accés de manera que actuï com a barrera (*firewall*) per als usuaris que es programi o que no reuneixin les condicions d'IP establertes. Aquest bloqueig l'ha de realitzar el gestor del servei, de manera que l'administració, llevat que hi hagi una ordre judicial al respecte, només pot forçar aquest bloqueig buscant la seva cooperació. En aquells països en què la situació legal o política ho permet, es pot obligar mitjançant normatives específiques.

Els DNS (de l'anglès *Domain Name System*) són registres que permeten traduir els noms d'internet a adreces IP. En realitat un DNS utilitza una base de dades que conté informació per la qual s'associa aquesta informació a un nom. L'associació de noms de domini (intel·ligibles per a l'usuari) amb adreces IP (sèries de nombres que identifiquen cada equip) és la funció més usual dels protocols DNS. Mitjançant la manipulació dels registres DNS és possible bloquejar l'accés a determinats llocs. El projecte de llei dels Estats Units "*Stop Online*

*Piracy Act*" (SOPA) tenia com a objectiu lluitar contra la pirateria a Internet utilitzant eines com ara la manipulació dels registres DNS.

La majoria d'equips permeten filtrar les URL (localitzador uniforme de recursos, comunament anomenat adreça electrònica) que desitgi l'usuari, per bloquejar l'accés a aquest lloc des d'aquest equip. Un sistema més eficient que la configuració individual de cada equip, és per a restringir l'accés a determinats llocs web és el bloqueig d'URL mitjançant un *proxy*. Un *proxy* permet accedir a un lloc web a través d'un servidor intermedi. Un sistema per a censurar determinats llocs és el de bloquejar la URL d'aquests llocs a través d'un *proxy*.

El bloqueig de paraules clau impedeix l'accés a llocs web que tinguin aquestes paraules en les seves adreces URL. Una tècnica més avançada és la de les llistes negres, que cada vegada és més utilitzada pels governs de diferents països. Aquesta censura sol anar acompanyada de l'aprovació de lleis que prohibeixen l'ús de determinades paraules en les cerques d'internet.

En general, la censura mitjançant l'ús de filtres en els servidors, necessita la cooperació dels gestors d'aquests servidors. El sistema més conegut de filtratge és Smartfilter, fabricat per la companyia nord-americana Secure Computing.

Una recent investigació patrocinada per Open Net Initiative arriba a la conclusió que "el filtrat d'Internet es porta a terme en almenys quaranta estats de tot el món, incloent molts països d'Àsia i Orient Mitjà i del nord d'Àfrica. Altres mecanismes semblants de control de

continguts a Internet també són utilitzats en països com Canadà, els Estats Units i alguns països d'Europa"<sup>181</sup>.

Open Net Initiative<sup>182</sup> és el resultat pràctic de la col·laboració de tres institucions com el Laboratori Ciutadà de la Munk School of Global Affairs, de la Universitat de Toronto; el Berkman Center for Internet & Society, de la Universitat de Harvard; i el SecDev Group d'Ottawa, una companyia canadenca dedicada a l'anàlisi dels problemes d'inseguretat i violència al món. Es tracta d'una de les múltiples organitzacions que tenen com a objectiu respondre a la creixent amenaça de censura a internet.

A nivell internacional no hi ha una normativa que permeti censurar Internet, però existeixen a la pràctica diferents procediments per tractar de fer-ho. Algunes companyies proveïdores de serveis, especialment de motors de cerca, atenent gairebé sempre peticions dels governs, cooperen amb ells ometent alguns resultats en les seves respostes a cerques realitzades per l'usuari. Aquesta pràctica no impedeix l'accés al lloc censurat, però dificulta trobar-lo.

El trànsit internacional d'Internet s'empara avui en la Regulació de les Telecomunicacions Internacionals. Es tracta d'un acord signat per 114 països a Austràlia el 1988, per tal de facilitar la interconnexió de les diferents infraestructures de telecomunicacions, la qual cosa facilita l'accessibilitat als serveis de telecomunicacions internacionals. No

---

<sup>181</sup> Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski i Jonathan Zittrain (ed.) "Access Denied: The Practice and Policy of Global Internet Filtering" The MIT Press (2008).

<sup>182</sup> <http://access.opennet.net/about-the-opennet-initiative/>

obstant això, en la pràctica, són constants els intents de restringir la lliure circulació a Internet:

"... Països suposadament democràtics constitueixen un mal exemple en cedir a la temptació de prioritzar la seguretat per sobre d'altres preocupacions i per l'adopció de mesures desproporcionades per protegir els drets d'autor. [...] Alguns governs intensifiquen la pressió sobre els proveïdors de serveis tècnics perquè actuïn com a policies d'Internet. Les empreses especialitzades en la vigilància en línia s'estan convertint en els nous mercenaris d'una carrera armamentista *on line*..."<sup>183</sup>.

No obstant això, sota el paraigua de la defensa de valors reconeguts, els governs tendeixen a fer una interpretació extensiva de les limitacions en l'ús d'Internet. Així, per exemple, als Estats Units la Communications Decency Act, en la seva primera redacció de 1996, va ser un intent del Congrés de limitar la distribució de material pornogràfic per Internet. No obstant això, el Tribunal de Primera Instància del Districte Oriental de Pennsylvania, en el cas Reno contra ACLU<sup>184</sup>, va dictaminar que no es pot limitar innecessàriament l'accés a la informació als adults per poder protegir als menors, és a dir, no s'ha de reduir la informació a Internet a només el que sigui apropiat per als nens.

La Cort Suprema, va ratificar aquest criteri, i va establir que les disposicions de la Llei, respecte a la "transmissió indecent" i a la

---

<sup>183</sup> "Internet Enemies: Report 2012" Reporters Sense Fronteres pp.2 disponible a <http://www.rsf-es.org/informes>.

<sup>184</sup> Reno v. American Civil Liberties Union 521 U.S. 844 (1997).



---

"demostració evidentment ofensiva" coartaven la llibertat d'expressió protegida per la Primera Esmena, el que en el fons equivalia a una censura il·legal per part del Govern<sup>185</sup>.

En aquest mateix sentit, és una constant cada vegada més forta la tendència dels governs d'estendre la responsabilitat dels intermediaris proveïdors de serveis a internet, així com d'intervenir directament, tant administrativament com penalment, amb arguments com la defensa de l'estat o la més genèrica del bé comú.

Són nombrosos els casos d'interpretació extensiva de l'administració per limitar determinades activitats a Internet. Exemples d'això els podem trobar en nombroses intervencions de l'administració en el que per a alguns internautes constitueixen clars intents de cibercensura. Un d'ells és el cas WikiLeaks. Es tracta d'una organització internacional sense ànim de lucre en el que en el seu lloc web es podia publicar informes i documents confidencials amb interès públic, i tot això mantenint l'anonimat. No obstant això, sota el pretext de la "Seguretat Nacional" i per tal d'impedir la difusió d'informacions confidencials, es va accedir als servidors on estava localitzat el lloc de WikiLeaks.

Una cosa semblant va passar amb els servidors de Freedom Hosting, una plataforma que oferia servei d'allotjament de llocs web. Amb l'excusa d'una operació contra la pornografia infantil, l'FBI va confiscar aquests servidors amb tots els seus continguts. Però amb això, es va accedir simultàniament a milers de correus d'usuaris de TorMail, un servei de correu anònim de la xarxa TOR, basada precisament en la

---

<sup>185</sup> "Janet Reno, Fiscal General dels Estats Units d'Amèrica, et al, apel·lants c/ American Civil Liberties Union et al No. 96-511 - CS Estats Units d'Amèrica - (1997 U.S LEXIS 4037) - 19 de març de 1997, al·legat 26 de juny de 1997.

garantia de confidencialitat de la navegació per Internet i que també estaven allotjats en aquests servidors.

Un altre exemple recent d'aquest excés de zel el constitueix el cas Megauload. Es tracta d'una plataforma dedicada precisament a oferir als usuaris un espai on dipositar els seus arxius per poder accedir-hi des de qualsevol lloc, o per posar-los a disposició d'altres usuaris. El tema està encara pendent d'una decisió judicial, però la veritat és que des del mateix moment de la intervenció oficial, els usuaris que tenien arxius situats en el lloc, es van trobar que havien perdut tots els seus arxius i que en tractar d'accedir al lloc de la pàgina de Megauload apareixia el següent avís:



Un altre dels casos més coneguts és el de May First/People Link. Es tracta d'un grup polític progressista dels Estats Units, que per tal de

garantir la confidencialitat de les comunicacions i la navegació per Internet dels seus usuaris, compren col·lectivament els seus equips informàtics i la contractació dels serveis d'internet, de manera que no és possible identificar fàcilment l'activitat de cada usuari en particular. No obstant això, els servidors de May First/People Link van ser confiscats el 18 d'abril del 2012 pels les autoritats federals dels Estats Units.

Hi ha una constant tensió entre els defensors de l'anonimat com a garantia de la llibertat d'expressió, i els que veuen en això un espai de possible impunitat davant la comissió de fets delictius o atemptatoris contra l'anomenada Seguretat Nacional. Entre els més conspicus defensors d'aquest plantejament es troben els governs de molts països. Estats com Cuba, Laos, Xina, Corea del Nord, Iran, Aràbia Saudita, Síria, Uzbekistan, Turkmenistan i molts altres, tenen directament establerts programes de cibercensura a la xarxa. Però també altres països teòricament democràtics, com Rússia, Turquia, França o Austràlia, tenen sistemes de vigilància a la xarxa. Segons el mapa de la cibercensura a internet, publicat per WholsHostingThis la temptació d'algun tipus de cibercensura arriba a pràcticament el 90% dels països<sup>186</sup>. Per la seva banda, amb motiu del dia Internacional contra la cibercensura, l'organització Reporters sense Fronteres també ha publicat el seu propi informe sobre els "Enemies d'Internet 2014" en el què destaca el fet que entre les institucions considerades "enemigues

---

<sup>186</sup> Richard. "Internet Censorship Around the Globe" WholsHostingThis (febrer de 2014) Pot consultar-se a <http://www.whoishostingthis.com/blog/2014/02/20/internet-censorship/>

d'Internet" la majoria es tracta d'institucions governamentals i moltes d'elles directament relacionades amb la "Seguretat Nacional"<sup>187</sup>.

## El repte de l'automatització

És cada vegada més freqüent la utilització de dades personals, existents en fitxers i bancs de dades informatitzats, per a finalitats administratives i de gestió. Aquests bancs de dades comporten una ingent quantitat d'informació, de manera que cada vegada estan més presents tècniques de "*Big Data*" per a la seva gestió, i amb això una automatització basada en algorismes i en intel·ligència artificial. Per això es fa necessari disposar de sistemes de garantia dels drets i llibertats fonamentals amb vista a la protecció de les dades tractades automàticament.

La jurisprudència ha anat delimitant al llarg de la història el contingut de les amenaces a la dignitat i als drets de la persona. Amb l'aparició de les noves tecnologies s'obre una nova situació que proporciona un nou espai per delinquir mitjançant l'ús de la informàtica. Tant el legislador, com els tribunals reconeixen explícitament les peculiaritats del mitjà, el que fa que es plantegin l'ús il·legítim del tractament mecanitzat de dades:

"... D'aquesta manera, la nostra Constitució ha incorporat una nova garantia constitucional, com a forma de resposta a una nova forma d'amenaça concreta a la dignitat i als drets de la

---

<sup>187</sup>Reporters Without Borders. "Enemies of the Internet 2014" (març 2014) pot consultar-se a [http://12mars.rsf.org/wp-content/uploads/EN\\_RAPPORT\\_INTERNET\\_BD.pdf](http://12mars.rsf.org/wp-content/uploads/EN_RAPPORT_INTERNET_BD.pdf).

persona, de forma en últim terme molt diferent de com es van anar originant i incorporant històricament els diferents drets fonamentals. En el present cas estem davant d'un institut de garantia d'altres drets, fonamentalment l'honor i la intimitat, però també d'un institut que és, en si mateix, un dret o llibertat fonamental, el dret a la llibertat enfront de les potencials agressions a la dignitat i a la llibertat de la persona provinents d'un ús il·legítim del tractament mecanitzat de dades, el que la Constitució anomena «la informàtica»... <sup>188</sup>.

També les legislacions nacionals, així com els diferents tractats i convenis internacionals, incideixen en la necessitat de protegir la intimitat de les persones. Així per exemple, el primer instrument vinculant a nivell internacional, va ser el Conveni número 108 del Consell d'Europa, de 28 de gener de 1981, per a la protecció de les persones respecte al tractament automatitzat de dades de caràcter personal<sup>189</sup>. Els mateixos tribunals han anat desenvolupant les pautes interpretatives que neixen d'aquest Conveni:

"... A partir d'aquí es planteja el problema de quin ha de ser aquest contingut mínim, provisional, en relació amb aquest dret o llibertat que el ciutadà ha de trobar garantit, fins i tot en absència de desenvolupament legislatiu sobre el tema.

Un primer element, el més «elemental», d'aquest contingut, és, sens dubte, negatiu, responent a l'enunciat literal del dret: L'ús

---

<sup>188</sup> Fonament jurídic sisè de la sentència del Tribunal Constitucional 254/1993, de 20 de juliol de 1993.

<sup>189</sup> Ratificat per l'Estat Espanyol mitjançant Instrument de 27 de gener de 1984.

de la informàtica troba un límit en el respecte a l'honor i la intimitat de les persones i en el ple exercici dels seus drets. Ara bé, l'efectivitat d'aquest dret pot requerir inexcusablement d'alguna garantia complementària i és aquí on poden venir en auxili interpretatiu els tractats i convenis internacionals sobre aquesta matèria subscrits per Espanya. Doncs, com assenyala el Ministeri Fiscal, la garantia de la intimitat adopta avui un contingut positiu en forma de dret de control sobre les dades relatives a la pròpia persona. L'anomenada «llibertat informàtica» és, així, també, dret a controlar l'ús de les mateixes dades inserides en un programa informàtic (*habeas data*)..."<sup>190</sup>.

La possibilitat que les màquines autònomes obtinguin i gestionin dades personals, sense el consentiment exprés de la persona afectada, no es limita a les dades que resultin de la navegació de l'usuari. De fet, són cada vegada més nombrosos els dispositius dotats de sensors capaços de recollir les més variades informacions. Roba, calçat, complements de tot tipus,... estan sent dissenyats per obtenir informacions que poden ser transmeses automàticament, de manera sense fil, a bases de dades.

Com es descriu a la Guia de tendències en tecnologia portable de Cetemmsa<sup>191</sup>: "La propera generació de vestits o 'roba mòbil' haurà de fer front als nous conceptes i missatges de la nostra societat canviant i adaptar-se a les necessitats i expectatives dels usuaris i a la nova realitat

---

<sup>190</sup> Fonament jurídic setè de la sentència del Tribunal Constitucional 254/1993, de 20 de juliol de 1993.

<sup>191</sup> El Centre d'Innovació i Tecnologia de Mataró i el Maresme (Cetemmsa) és un centre tecnològic de serveis de R+D, que realitza recerca aplicada de materials i dispositius intel·ligents.

digital. Les tecnologies de l'electrònica impresa aplicades al món dels teixits intel·ligents, seran una resposta mitjançant solucions portables disruptives”<sup>192</sup>.

Aquesta guia presenta dispositius ja existents en l'actualitat i capaços d'obtenir automàticament dades de l'usuari sobre el seu nivell d'activitat, la seva salut o les seves preferències. En general, aquests sensors solen tenir objectius legítims i coneguts per l'usuari, però el cert és que l'automatització dels sistemes no permet garantir el ple respecte a la privacitat i el respecte a la intimitat d'aquell de qui s'obtinguin les dades personals.

---

<sup>192</sup> Cetemmsa, Technological Centre: “Wearable Technology Trendguide: Scenarios and Opportunities for Printed Electronics and Smart Fabrics” Mataró, 2014. Es tracta de l'informe sobre les perspectives 2014 en aquests camps i que es pot consultar a: <http://www.cetemmsa.com/noticias.php?id=000000012J&id2=000000019G>.





## **4<sup>a</sup> Part:**

### **De la culpa del cavall a la culpa del robot**



## **Capítol setzè:**

### **Publicitat i les seves possibles males pràctiques**

---

#### **La publicitat en Internet**

Per tal de difondre l'existència d'un producte o servei, o situar aquest competitivament en el mercat, les empreses utilitzen tècniques publicitàries en general. L'èxit dels productes que comercialitzen les empreses depèn moltes vegades que la seva publicitat arribi a un nombre suficient de potencials consumidors. La Llei 34/1988, d'11 de novembre, general de publicitat, defineix el terme publicitat com:

"... Tota forma de comunicació realitzada per una persona física o jurídica, pública o privada, en l'exercici d'una activitat comercial, industrial, artesanal o professional, amb la finalitat de promoure de manera directa o indirecta la contractació de béns mobles o immobles, serveis, drets i obligacions..."<sup>193</sup>.

Quan per tal de potenciar l'activitat de comerç electrònic es realitza la publicitat a través d'Internet els mecanismes utilitzats són específics del mitjà utilitzat, encara que l'objectiu és en tot cas el mateix que en qualsevol altra sistema de publicitat utilitzada habitualment pel comerç en general.

---

<sup>193</sup> Article 2 de la Llei 34/1988, d'11 de novembre, general de publicitat, modificada parcialment per la transposició de la Directiva 97/55/CE, en relació a la publicitat comparativa.

A la pràctica, els elements de màrqueting i de personalització de la marca del producte o del seu fabricant o distribuïdor, ja constitueix en sí mateix un element publicitari. Tots aquells logos, imatges, textos, o missatges inclosos en la pàgina web, que permeten a l'usuari reconèixer la marca o el producte, es poden considerar publicitat. Des d'aquesta perspectiva podem afirmar que la majoria de pàgines web de marca o d'empresa, que podem trobar a Internet, contenen elements publicitaris. De fet, moltes vegades la pròpia creació de la pàgina web sols té com a principal objectiu servir d'element publicitari de la marca o de la empresa de què es tracti.

Tanmateix, la publicitat realitzada a través d'Internet no es limita a la presentació de la marca o els logos en la pàgina web de la empresa anunciant, sinó que pot adoptar formes molt variades.

Són nombroses les possibilitats d'Internet per difondre missatges publicitaris en les més variades presentacions. Així, podem trobar vídeos publicitaris, jocs publicitaris, vals i llistes d'ofertes,... En tots els casos, la publicitat realitzada a través d'Internet s'ha d'ajustar als mateixos requisits legals que la resta de publicitat realitzada mitjançant altres sistemes més tradicionals.

Un dels sistemes més utilitzats a Internet per introduir missatges publicitaris és el dels bàners. Un bàner és un gràfic, una imatge, un vídeo, o un text, situat en una finestra integrada en una pàgina web i que té com a finalitat contenir un missatge publicitari. Els bàners situats en pàgines de tercers solen actuar com a enllaços que dirigeixen a la pàgina de l'anunciant quan l'usuari prem el ratolí sobre ells.

Semblant als bàners són els *pop-up* nom amb què es denomina als anuncis emergents que apareixen a la pàgina web, però independent d'aquesta, i que incorporen el missatge publicitari. La finestra que conté l'anunci emergent pot aparèixer des del moment que l'usuari accedeix a la pàgina web, o quan aquest executa alguna acció concreta. En uns casos aquesta finestra pot desaparèixer per si mateixa després d'alguns segons, o bé és necessari que l'usuari es vegi obligat a realitzar alguna acció per aconseguir aquesta desaparició.

Aquest tipus d'anuncis poden adoptar formes i complexitats diverses. Així, els anomenats *Keyword banners* són bàners que apareixen en les pàgines web dels cercadors, i que fan aparèixer uns bàners o altres en funció de les paraules de cerca introduïdes per l'usuari en el motor de cerca.

## **Personalitzant la publicitat**

Aparentment l'aparició d'uns anuncis o altres en funció de les paraules introduïdes per l'usuari en el cercador, semblaria una millora en el servei ofert a aquest en la direcció de la filosofia Web 3.0, ja que la màquina ofereix alternatives de manera automàtica en detectar la cerca de l'usuari, oferint aquells anuncis que probablement més li puguin interessar.

Des dels seus inicis els cercadors ens ofereixen una llista d'enllaços a pàgines web relacionades amb les paraules clau introduïdes per l'usuari. El que tenim com a resultat doncs, és la presentació en forma de llista de totes aquelles pàgines que contenen aquestes paraules clau. Encara

que l'ordre de presentació d'aquesta llista d'enllaços respongui a criteris i interessos molt variats, la veritat és que a l'usuari se li presenten multitud d'enllaços per escollir, però en general, d'acord amb els interessos prioritari dels anunciants.

La presentació de bàners o enllaços publicitaris a partir de les paraules clau introduïdes per l'usuari, són conegudes en la seva denominació en anglès com a *Keywords Advertising*. Aquests bàners prioritzen els interessos d'aquells anunciants que han contractat el servei. Cada motor de cerca té el seu propi sistema d'incorporació de publicitat. Així per exemple, Google utilitza com a programa publicitari basat en paraules clau, el programa AdWords<sup>194</sup>.

Per tal de mostrar els anuncis únicament als potencials clients o persones interessades en el producte concret de què es tracti, AdWords és un tipus de publicitat basada en paraules clau. Quan un usuari visita Google i formula una consulta, se li mostren diferents resultats rellevants, com vincles a articles que continguin consells relacionats amb les paraules de cerca utilitzades. Així mateix, mostra anuncis que enllacin amb empreses en línia que també ofereixin productes relacionats amb la consulta<sup>195</sup>.

---

<sup>194</sup> AdWords de Google ofereix diferents varietats de formats d'anunci. El format més habitual són els anuncis de text, seguits dels anuncis gràfics i animats. Altres formats disponibles són els anuncis de vídeo, els anuncis d'empresa local i els anuncis per a mòbils.

<sup>195</sup> Mónica Lastiri esmenta dos tipus de resultats en les cerques dels usuaris. Uns són els resultats "naturals", originats quan un usuari fa una cerca a partir d'una o varies paraules i el motor de cerca mostra els llocs que semblen ajustar-se més a aquestes paraules per ordre decreixent de pertinença en relació a la informació demanada. Un altre tipus de resultats són els derivats d'un servei remunerat com és el cas de Google amb el seu Google AdWords

Aquest sistema de publicitat a través de paraules clau presenta també alguns problemes, tal com explica Mónica Lastiri:

“... La publicitat contextual és una modalitat d’alta segmentació que es considera poc intrusiva, ja que es dirigeix a un públic que se sap, per endavant, està interessat en un producte o servei determinat. No obstant això, aquest tipus de publicitat representa un dels molts problemes que tenen els titulars de marques en l’entorn digital, ja que des de la perspectiva del dret de marques, nombrosos operadors econòmics qüestionen la legalitat de la publicitat en els motors de cerca a Internet utilitzant determinades paraules clau...” (Lastiri, 2013).

En el sistema AdWords els anunciants trien aquelles paraules clau comercialitzades per Google a través del seu servei de referenciació. Aquestes paraules clau, una vegada introduïdes per l’usuari en el cercador, fan aparèixer els anuncis o enllaços relacionats amb aquest tema. Google cobra un preu preestablert a l’anunciant per cada vegada que un usuari faci clic sobre l’enllaç en qüestió. Aquests enllaços són directament enllaços publicitaris, o el que sol anomenar-se enllaços patrocinats.

La interpretació que en fa actualment la jurisprudència sobre aquests enllaços patrocinats es nombrosa. Un exemple ho constitueix el cas

---

anomenat també *CostPer-Click (CPC) Internet Advertising Model Like AdWords*. (Lastiri, 2013).

d'Interflora vs. Mark & Spencer <sup>196</sup>. Interflora és una agrupació d'empreses de floristeria que permet que es puguin adquirir flors per Internet, les quals són lliurades al client, o a qui aquest disposi, a través del membre de Interflora més proper al domicili d'entrega de la comanda. D'altra banda, Mark & Spencer (M&S) és un detallista del Regne Unit que també envia flors adquirides per Internet. Entre les paraules de referència que M&S va adquirir a Google en el seu programa AdWords estava precisament Interflora, així com diverses variacions del mateix nom.

Davant d'aquesta situació, Interflora va interposar contra M&S un recurs per vulneració dels seus drets de marca davant la High Court of Justice (England & Wales), Chancery Division, la qual va sol·licitar al Tribunal de Justícia de la Unió Europea decisió prejudicial sobre diversos aspectes del cas. Com a resposta, el Tribunal va emetre una sentència en què avala la utilització d'una marca com a paraula clau de referència en els cercadors, sempre que això no impliqui menyscabament de cap de les funcions de la marca, i per tant, del titular de la mateixa:

“... La determinació de si la funció d'indicació de l'origen de la marca resulta menyscabada quan es mostra als internautes, a partir d'una paraula clau idèntica a aquesta marca, un anunci d'un tercer, que pot ser competidor del titular d'aquesta marca, depèn particularment de la manera en què es presenti l'anunci. L'esmentada funció d'indicació de l'origen de la marca resulta menyscabada quan l'anunci no permet o tot

---

<sup>196</sup> Aquest cas és àmpliament comentat per Mónica Lastiri Santiago, a “El tratamiento jurídico de las Keywords Advertising en la jurisprudencia del Tribunal de Justicia de la Unió Europea.” Rev. IUS vol.7 n° 31 Puebla (gener-juny 2013).



just permet a l'internauta normalment informat i raonablement atent determinar si els productes o serveis inclosos en l'anunci procedeixen del titular de la marca o d'una empresa econòmicament vinculada a aquest o si, per contra, procedeixen d'un tercer (sentències abans esmentades Google France i Google, apartats 83 i 84, i Portakabin, apartat 34)...”<sup>197</sup>.

Així doncs, la jurisprudència, i especialment la Sentència del Tribunal de Justícia de la Unió Europea, de 23 de març de 2010, en els assumptes acumulats C-236/08 a C238/08, entre Google France SARL, Google Inc. i, entre altres, Louis Vuitton Malletier SA, ha vingut deixant clar que està prohibit l'ús per part de tercers d'una marca com a paraula clau per a realitzar campanyes publicitàries.

No es pot utilitzar els elements característics d'una marca aliena de manera que es pretengui obtenir un avantatge deslleial del caràcter distintiu o del renom de la marca o es pugui causar perjudici a la mateixa al menyscabar alguna de les seves funcions. De fet, la Llei general de publicitat considera publicitat il·lícita:

“... e) La publicitat enganyosa, la publicitat deslleial i la publicitat agressiva, que tindran el caràcter d'actes de

---

<sup>197</sup> Apartat 44 de la Sentència de la Sala Primera del Tribunal de Justícia de la UE, de 22 de setembre de 2011. Interflora Inc. i Interflora British Unit contra Marks & Spencer plc i Flowers Direct Online Ltd. Com a resposta a la petició de decisió prejudicial sol·licitada per la High Court of Justice (England & Wales).

competència deslleial en els termes previstos en la Llei de competència deslleial...”<sup>198</sup>.

Si ens fixem en el capítol II de la Llei 3/1991, de 10 de gener, de competència deslleial, podem veure que entre els actes de competència deslleial: els actes d’engany, confusió, denigració, comparació, imitació, l’explotació de la reputació aliena,... No obstant això, quan es produeix una infracció a l’anterior, el proveïdor del motor de cerca no és responsable, llevat que tingui un paper actiu, o en ser advertit de la il·legalitat no actuï immediatament per retirar l’enllaç.

## **L’ús del correu electrònic per a publicitat**

Els missatges publicitaris que s’envien a potencials clients mitjançant el seu correu electrònic, només estan autoritzats si aquests han estat prèviament sol·licitats o expressament autoritzats per aquest:

“... D’altra banda, ressaltar que està prohibit l’enviament de comunicacions comercials publicitàries o comercials per correu electrònic o altre mitjà de comunicació electrònica equivalent que prèviament no hagin estat sol·licitades o expressament autoritzades pels destinataris de les mateixes, excepte quan hi hagi una relació contractual prèvia, sempre que el prestador hagi obtingut de forma lícita les dades de contacte del destinatari i las empri per a l’enviament de

---

<sup>198</sup> Article 3 de la Llei 34/1988, d’11 de novembre, general de publicitat, modificada per la Llei 29/2009, de 30 de desembre, per la qual es modifica el règim legal de la competència deslleial i de la publicitat per a la millora de la protecció dels consumidors i usuaris.

comunicacions comercials referents a productes o serveis de la seva pròpia empresa que siguin similars als que inicialment van ser objecte de contractació amb el client ...”<sup>199</sup>.

És freqüent la recepció de correus electrònics publicitaris no sol·licitats, el que es sol anomenar *Spam*. Aquests missatges publicitaris estan expressament prohibits per la legislació i, en tot cas, el destinatari ha de tenir la possibilitat de oposar-se al tractament de les seves dades amb finalitats promocionals mitjançant un procediment senzill i gratuït, tant en el moment de recollida de les dades com en cadascuna de les comunicacions comercials que li dirigeixin. En el cas de la publicitat rebuda per correu electrònic, aquest mitjà per oposar-se ha d’incloure necessàriament una direcció electrònica vàlida on pugui exercitar-se aquest dret<sup>200</sup>:

“... És a dir, que una entitat pot tenir la seva adreça de correu electrònic en una web als efectes de «contacte» i fonamentalment per oferir els seus productes i actuar en el tràfic jurídic, però que «això no implica una autorització *ad limitum* per a ser receptora de publicitat, ja que precisament aquest dret a no rebre comunicacions comercials per mitjans electrònics és el que protegeix l’article 21 de la Llei de Serveis de la Societat de la Informació»...”<sup>201</sup>.

---

<sup>199</sup> Moratalla Escudero, José Ramón. “Las diez sentencias más reveladoras de 2013” disponible a [http://www.elderecho.com/actualidad/sentencias-reveladores\\_0\\_623625032.html](http://www.elderecho.com/actualidad/sentencias-reveladores_0_623625032.html).

<sup>200</sup> Article 21 de la Llei 34/2002, d’11 de juliol de 2002, de serveis de la societat de la informació i de comerç electrònic.

<sup>201</sup> Fonament de dret quart de la sentència 3644/2013 de la Secció Primera de la Sala del Contenciós-Administratiu, de l’Audiència Nacional, de 23 de juliol de 2013.

A més a més, tal com recull l'article 20.1 de la Llei 34/2002 d'11 de juliol de 2002, de serveis de la societat de la informació i el comerç electrònic, la publicitat realitzada per via electrònica ha de ser clarament identificable com a publicitat i ha d'indicar la persona física o jurídica en nom de la qual es realitza aquesta publicitat. En el cas concret de la publicitat realitzada per correu electrònic o un altre mitjà de comunicació electrònica equivalent, s'ha d'incloure al començament del missatge la paraula "publicitat" o l'abreviatura "publi". D'altra banda, està expressament prohibit l'enviament de comunicacions comercials en què es dissimuli o s'oculti la identitat del remitent per compte de qui s'efectua la comunicació comercial<sup>202</sup>.

Un dels principals punts febles d'aquesta mena de publicitat, ho constitueix la recollida d'adreces de correu a les que trametrà aquesta publicitat. En molts casos, aquesta recollida es fa amb mitjans totalment automatitzats. Alguns programes permeten la cerca automàtica no autoritzada d'aquestes adreces a pàgines web, xats, fòrums i d'altres entorns similars. Amb aquestes adreces es configuren les bases de dades que seran utilitzades en trameses massives de publicitat no demanada. En molts cassos inclús, el sistema estructura les dades de manera que es puguin segmentar d'acord a les aficions o característiques expressades pels destinataris d'aquesta publicitat en els llocs dels que s'han extret aquestes dades.

---

<sup>202</sup> Article 20.4 de la Llei 34/2002 introduït pel Reial Decret-Llei 13/2012, de 30 de març, pel qual es transposen directives en matèria de mercats interiors d'electricitat i gas i en matèria de comunicacions electròniques, i pel qual s'adopten mesures per a la correcció de les desviacions per desajustaments entre els costos i ingressos dels sectors elèctric i gasista.

La Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, estableix en el seu article 44.3 d) que és infracció el tractament de les dades de caràcter personal o utilitzar-les posteriorment amb conculcació dels principis i les garanties que estableix la mateixa Llei, o amb incompliment dels preceptes de protecció que imposin les disposicions reglamentàries de desplegament. Aquesta mateixa Llei es refereix al principi general del consentiment, aplicat pels tribunals per valorar la procedència o no de la publicitat rebuda per aquest mitjà:

“... - L'article 6.1 (de la Llei Orgànica 15/1999) que recull el principi general del consentiment segons el qual el tractament de les dades de caràcter personal requerirà el consentiment inequívoc de l'afectat, llevat que la llei disposi una altra cosa.

- també és aplicable el que preveu l'article 30.1 en relació al tractament de dades, amb finalitat de publicitat i que estableix la forma d'actuació dels que recullin dades de les bústies (com diu l'entitat recurrent que va ocórrer en el present cas) i estableix que: «Els qui es dediquin a la recopilació d'adreces, repartiment de documents, publicitat, venda a distància, prospecció comercial i altres activitats anàlogues, utilitzaran noms i adreces o altres dades de caràcter personal quan hi figurin en fonts accessibles al públic o quan hagin estat facilitats pels mateixos interessats o s'hagin obtingut amb el seu consentiment»...”<sup>203</sup>.

---

<sup>203</sup> Fonament de dret segon de la sentència de la Secció Primera de la Sala del Contenciós-Administratiu de l'Audiència Nacional, de 18 de maig de 2006, sobre el recurs contenciós-administratiu número 01/35/2005.

La mateixa sentència recull quines són les fonts accessibles al públic citant l'apartat j) de l'article 3 de la repetida Llei Orgànica 15/1999 en el qual es defineix aquestes fonts com "aquells fitxers que poden ser consultats per qualsevol persona, no impedida per una norma limitativa o sense més exigència que, si s'escau, l'abonament d'una contraprestació". El mateix article especifica que tenen la consideració de fonts d'accés públic, exclusivament: el cens promocional; els repertoris telefònics en els termes que preveu la normativa específica; i les llistes de persones pertanyents a grups de professionals que continguin únicament les dades de nom, títol, professió, activitat, grau acadèmic, direcció i indicació de la seva pertinença al grup. Així mateix, tenen el caràcter de fonts d'accés públic els diaris i butlletins oficials i els mitjans de comunicació.

## **Requisit de consentiment previ**

En tot cas, aquesta utilització no autoritzada de l'adreça de correu electrònic per trametre publicitat no demanada, està expressament prohibida per la legislació, i així ho han recollit els tribunals:

"... La dicció literal de l'article 21.1 de la Llei 34/2002, de Serveis de la Societat de la Informació i Comerç Electrònic, no deixa lloc a dubtes sobre la prohibició de comunicacions publicitàries o promocionals per correu electrònic, que no hagin estat prèviament sol·licitades o expressament autoritzades pels seus destinataris.

És a dir, per a la remissió dels correus electrònics comercials o promocionals (en cap moment s'ha posat en dubte que l'ara analitzat pertanyi a la mateixa categoria), es requereix la prèvia sol·licitud o expressa autorització dels seus destinataris. En definitiva, l'existència d'un consentiment que el denunciant no ha atorgat a la Sra. Flora, remitent d'aquesta comunicació.

Resulta per això secundari que la direcció del destinatari procedís d'una base de dades publicada a Internet, ja que el rellevant als efectes aquí analitzats, és que el denunciant no va atorgar el seu consentiment, per la qual cosa no té cobertura per a aquesta tramesa. I és igualment indiferent, i pels mateixos motius, el fet que el destinatari d'aquest enviament pogués ser (almenys figurava així publicat a la indicada pàgina web adjuntada com documental per l'actora), una persona jurídica i no una persona física...<sup>204</sup>.

Aquesta necessitat d'autorització prèvia de l'interessat per a què es puguin utilitzar les seves dades per rebre publicitat, inclou la publicitat massiva, que és la més freqüentment utilitzada pels sistemes automatitzats. Però el responsable de qualsevol infracció comesa en aquest sentit, amb independència de que la selecció de l'adreça a on s'ha de dirigir la publicitat i, la seva remissió física, hagi estat un procés automatitzat serà en tot cas l'anunciant:

---

<sup>204</sup> Fonament de dret tercer de la sentència 3338/2008 de la Secció Primera de la Sala del Contenciós-Administratiu de l'Audiència Nacional, de 17 de setembre de 2008, sobre el Recurs contenciós-administratiu número 189/2007.

"... Afegeix que el lloc web "Alasbarricadas.org" infringeix l'obligació establerta per l'article 10 de la Llei 34/03 d'11 de juliol de serveis de la societat de la informació i de comerç electrònic (LSSICE), en no contenir cap informació a la seva pàgina web sobre la identitat del responsable o titular de la pàgina o el seu domicili per establir una comunicació directa i efectiva. Així en punxar qualsevol enllaç de la pàgina per contactar amb els responsables només es facilita el correu electrònic info@alabarricadas.org, sent necessari a l'actor contractar una agència de detectius per esbrinar la identitat del titular del lloc web que va resultar el demandat i com a tal proveïdor de continguts de l'esmentada web, responsable solidari amb els autors dels continguts publicats..."<sup>205</sup>.

La Llei 34/2002 de serveis de la societat de la informació i comerç electrònic, es refereix explícitament a aquests enviaments massius de comunicacions comercials. Així, en el seu article 38.3 c) especifica com infracció greu "l'enviament massiu de comunicacions comercials per correu electrònic o altre mitjà de comunicació electrònica equivalent, o el seu enviament insistent o sistemàtic a un mateix destinatari del servei".

---

<sup>205</sup> Sentència número 72/2011, de 10 de febrer de 2011, de la Sala del Civil del Tribunal Suprem.



## **Capítol dissetè: Creixement de la logística robotitzada**

---

### **L'automatització de la logística**

Una activitat en la qual s'està introduint ràpidament la robòtica combinada amb tecnologies d'intel·ligència artificial, és la de la logística. Incloem aquí els sistemes encarregats de la gestió i manipulació d'estoc; els dedicats a la gestió de l'emmagatzematge dels productes; els que preparen i reposen els productes sol·licitats, així com totes aquelles accions de logística necessàries per a la distribució del producte al client. Es tracta de sistemes que en general interactuen cada vegada més profundament i de manera autònoma, en un entorn i amb unes prestacions fins ara reservades a les persones.

La cadena de subministrament implica accions que faciliten la compra, producció, emmagatzematge, manteniment, transport i distribució dels productes comercialitzats. La progressiva complexitat d'aquestes activitats fa que siguin cada vegada més nombroses les empreses que han optat per robotitzar la seva logística. Algunes de les principals empreses dedicades al comerç a Internet, com Zappos, o Amazon, tenen automatitzats els seus sistemes de logística, de manera que el

moviment dels productes adquirits és gestionat mitjançant sistemes robotitzats<sup>206</sup>.

Els actuals sistemes d'automatització de magatzems permeten realitzar la majoria de les operacions de distribució d'acord a les dades recollides pels diferents sensors ubicats en el propi magatzem. Es tracta d'un sistema d'emmagatzematge que manté l'inventari permanentment actualitzat, amb control de qualitat i el sistema de compliment de l'ordre. El sistema fa servir productes de totes les formes i mides, movent-los automàticament fins als llocs o operadors establerts. Els centres de distribució automatitzats, poden recollir, empaçar i enviar qualsevol article, en qualsevol lloc i en qualsevol moment gràcies als avenços en robòtica i intel·ligència artificial.

Els robots circulen de manera autònoma per tot el magatzem, evitant xocar, actuant en els llocs d'emmagatzematge de cada producte demanat pel client, seleccionant i traslladant el producte corresponent i, d'acord a l'inventari existent, que el mateix robot s'encarrega d'actualitzar, i posteriorment reposar.

La progressió geomètrica de la robòtica en la nostra societat, es veu fortament potenciada per les pròpies administracions. Així, la mateixa Comissió Europea, conscient del paper que la robòtica pot exercir en la

---

<sup>206</sup> Zappos (<http://www.zappos.com/>) es dedica a la comercialització de productes per Internet i igual com altres empreses com Staples, (<http://www.staples.com/>) Gap, (<http://www.gap.com/>) o Amazon (<http://www.amazon.com>) gestionen la seva logística mitjançant el sistema de Kiva Systems, (<http://www.kivasystems.com/solutions/>) adquirit recentment pel propi Amazon.

societat actual, va decidir el 2012 iniciar l'associació publicoprivada SPARC per al desenvolupament de la robòtica<sup>207</sup>.

Davant l'evidència d'aquest desenvolupament, sorgeix immediatament la qüestió de la responsabilitat davant les incidències que puguin sorgir en interaccionar la robòtica en l'espai real. La ciència ficció ha tractat profusament aquest tema, però en general des del supòsit que si un robot adquireix capacitats humanes passa a ser responsable dels seus propis actes. Potser algun dia això pugui arribar a ser així, però ara per ara, a la vida real no sembla que sigui aquesta la postura del legislador, encara que estiguem desenvolupant màquines capaces de superar fins i tot les capacitats humanes.

Si partim de la base que un robot, o un sistema robotitzat capaç de realitzar autònomament determinades activitats, no deixa de ser una màquina, i per tant un objecte inanimat, podem comprovar que la jurisprudència sobre la responsabilitat del cuidador d'un objecte inanimat és antiga i ben establerta. Així, la Cort de Cassació francesa va dictar, el 18 juny 1896, sentència en l'anomenat "cas Teffaine" en què es valorava la responsabilitat davant la situació en què un empleat mecànic va quedar lesionat per l'explosió del remolcador d'una caldera. El tribunal va establir la condemna al guardià de la cosa inanimada, tot i no haver-se demostrat que en tingués directament cap culpa, amb la sola prova del vici, i establint que la responsabilitat (civil en aquest cas)

---

<sup>207</sup> Actualment formen part d'SPARC amb la pròpia Comissió Europea, més de 180 companyies i centres d'investigació superior, agrupades en euRobotics de la què en formen part centres com la Universitat Politècnica de Catalunya, o la Universitat de Girona. Pot consultar els seus objectius i programes en <http://www.eu-robotics.net/>

no desapareixia per la culpa del constructor de la cosa o el caràcter ocult dels possibles vicis que aquest objecte inanimat pogués tenir.

D'altra banda, també el Tribunal de Cassació francès va dictar, el 13 de febrer de 1930, una altra sentència establint com a doctrina legal que "per a la presumpció que estableix la llei (article 1384 paràgraf primer) no distingeix segons que la cosa que ha causat el dany hagi estat o no accionada per la mà de l'home". D'aquesta forma va quedar consagrada la responsabilitat objectiva del cuidador pels fets produïts per l'objecte inanimat.

Aquesta sentència es basava en el Codi Civil Francès, o Codi Napoleònic, aprovat per la Llei del 21 de març de 1804 que estableix en el seu article 1384: "S'ha de respondre no només pel dany que es causi per un fet propi, sinó també del causat per persones que estiguin sota la seva responsabilitat, o les coses que estan en la seva custòdia".

## **El risc de la fal·làcia androide**

Fins ara, les experiències en robòtica humanoide es limitaven a activitats molt rutinàries i limitades. Així, el robot de Toyota capaç de fer de Ciceró dels visitants de les seves instal·lacions, pot conversar amb els visitants, però amb moltes limitacions, més enllà de les 20.000 paraules japoneses que componen la seva base de dades. Un altre exemple, també de Toyota, el podem veure en el robot capaç d'interpretar música amb instruments com el violí.

No està tan lluny el moment en què les màquines siguin capaces d'interpretar emocions. De fet, SoftBank i Aldebaran Robotics van

presentar al juny de 2014 un robot capaç de comunicar-se amb persones i d'interpretar les seves emocions. La intenció és que Pepper, que així ho han anomenat, exerceixi de dependent de comerç. Els clients podran conversar amb el robot com ho farien amb un dependent humà, el qual es pot moure autònomament, així com detectar i reaccionar a les emocions dels clients<sup>208</sup>.

El robot pot reconèixer la veu humana i interpretar aspectes com el seu to i interpretar gestos facials o llenguatge corporal, de manera que això li permet interpretar emocions i interactuar en funció d'aquestes emocions. Segons els seus desenvolupadors Pepper és capaç de, entre altres coses, ballar, fer broma i aprendre per si mateix a partir de la seva interacció amb els éssers humans. Pot mantenir converses espontànies amb els clients, amb un 80% d'encert.

Els mateixos desenvolupadors de Pepper estan actualment desenvolupant tota una gamma d'autòmats per a la llar i per al camp sanitari. Si a això afegim les diferents investigacions que s'estan realitzant per a la producció de robots amb característiques basades en intel·ligència artificial, podem afirmar que la interacció de les màquines amb el món de les emocions, l'humor, o l'aprenentatge, no està massa lluny. De fet, robots com Aiko dissenyats com robots de companyia a base de silicona i amb aspecte molt realista de dona, en el seu inici limitaven les seves capacitats, però multiplicant els seus sensors i desenvolupant cada vegada més aspectes propis d'intel·ligència artificial, avui aquests robots són capaços de distingir entre diferents begudes, reconèixer i recordar els rostres i noms de les persones que li

---

<sup>208</sup> Poden veure's les capacitats desenvolupades en aquest denominat "robot social" a: <http://www.aldebaran.com/en/a-robots/who-is-pepper>.

presenten, expressar expressions humanes com la felicitat, o l'enuig i aspectes similars.

Un risc a l'abordar el tema de la responsabilitat en el camp de la robòtica, és la de oblidar precisament que els mecanismes robotitzats, és a dir els robots en sentit ampli, són màquines, i per tant objectes inanimats. Seguint a Richards i a Smart, hi ha una certa tendència a considerar els robots, especialment els que tenen una forma androide, però no només a ells, amb paràmetres semblants als que utilitzem habitualment per valorar les accions humanes.

"... Si apliquem malament les metàfores que utilitzem per als robots, les lliçons de la ciber-legalitat ens indiquen que això podria tenir conseqüències potencialment desastroses. Finalment, sostenim que ha de ser rotundament rebutjada una metàfora particularment seductora per als robots, la idea que els robots són «com les persones», i que hi ha una diferència significativa entre els robots humanoides i els no humanoides. Anomenem a aquesta idea «la fal·làcia androide»..." (Richards i Smart, 2013).

Amb la seva fal·làcia androide, Richards i Smart prevenen contra el risc d'atribuir responsabilitats humanes al que són meres màquines. Com ells mateixos assenyalen: "Aquesta projecció d'atributs humans és perillosa quan intentem dissenyar una legislació per als robots. Els robots són, i durant molts anys seguiran sent, eines".

## Responsabilitat per danys provocats per robots

Els tribunals vénen repetidament analitzant situacions en què un sistema robotitzat ha provocat danys a persones que van entrar en el seu camp d'acció i, en tots els casos, quan s'ha reconegut algun tipus de responsabilitat, aquesta sempre ha estat atribuïda a persones i mai a la pròpia màquina.

Un exemple del clar posicionament dels tribunals en l'atribució de responsabilitats davant danys produïts per un robot o per un sistema autònom, és la sentència de 20 de gener de 2010, de la Sala del Social del Tribunal Suprem en veure un recurs de cassació sobre un accident produït en ser atrapat el cap d'un treballador per una pinça d'un robot de sortida. Els fets provats són que l'accident va tenir lloc en una zona diferent d'on treballava el causant quan es va produir una avaria en el robot de sortida. Les tanques que protegien l'accés al lloc on operava el robot no impedièen totalment l'accés. El treballador es va adonar de la causa de l'aturada del robot i va entrar a la zona per tal de solucionar el problema. Al mateix temps l'encarregat, que des d'on es trobava no tenia possibilitat de veure l'accidentat, va posar en funcionament la línia d'esmaltat i el braç del robot va atrapar al treballador pel cap.

En els fonaments de dret de la mateixa sentència, s'esmenta un altre cas similar, en què la Sala del Social de Burgos, de 21 de març de 2000<sup>209</sup>, va enjudiciar un altre supòsit en el qual l'accident es va produir en una cadena d'elaboració d'articles de ceràmica quan el treballador a l'observar que la màquina estava encallada, es va introduir dins estan la màquina en marxa i, va començar a netejar un corró i la cinta

---

<sup>209</sup> Sentència 162/2000 de la Sala del Social del Tribunal Superior de Justícia de Burgos.

transportadora, atrapant-se-li el braç dret entre el corró i la cinta transportadora. En aquell cas la sentència va considerar que hi ha una relació de causalitat entre l'accident i l'incompliment de l'empresa, perquè les tanques no impedièn completament l'accés a la zona de risc, la màquina no tenia un mecanisme de parada automàtica i no s'havia proporcionat al treballador la formació oportuna. Per això, manté el reconeixement realitzat en via administrativa.

"... El que s'ha produït és una concurrència de culpes en la mesura que el dany sorgeix, d'una banda, de les infraccions de les normes de seguretat imputables a l'empresa, que la sentència recorreguda accepta i admet, però també d'una conducta de la pròpia víctima, que, amb la intenció de reparar el desperfecte, entra a la zona de risc i procedeix pel seu compte a realitzar una sèrie d'operacions en una zona a l'abast del robot. Les dues conductes tenen rellevància causal, perquè sense les infraccions de l'empresa l'accident no hagués tingut lloc, ja que el treballador no hagués entrat a la zona de risc o d'entrar s'hagués impedit l'acció de la màquina. Però tampoc s'hauria produït l'accident, si el treballador no hagués entrat a la zona de risc. Ara bé, d'acord amb una reiterada doctrina de la Sala del Civil d'aquest Tribunal, que recull també la nostra sentència del 12 de juliol de 2007, la culpa de la víctima no trenca el nexa causal que prové de l'agent extern -en aquest cas els incompliments de l'empresa-, excepte quan el dany s'ha produït de forma exclusiva per una actuació culposa imputable a la víctima. El dany és imputable també a l'empresa, perquè si no s'haguessin produït les



omissions en matèria de prevenció que li són imputables l'accident no hagués tingut lloc..."<sup>210</sup>.

En la sentència s'aprecia una concurrència de culpes en l'accident. D'una banda, l'empresa infringeix les normes de seguretat en no protegir adequadament la zona de treball del robot, ja que l'efectivitat de les mesures preventives ha de preveure la distracció o imprudència temeràries que pogués cometre el treballador. Tanmateix, hi ha també responsabilitat per part del treballador que va entrar a la zona de risc pel seu compte i sota l'abast del robot.

En cap cas es fa referència al funcionament del propi robot com a causa dels danys. La jurisprudència consolidada en tots els casos és ara per ara, que una màquina robotitzada no és susceptible de responsabilitat, per complex que sigui el seu comportament i, sigui quins siguin els danys provocats, fins i tot amb resultat de mort, com és el cas aquí esmentat.

No obstant això, la legislació i la jurisprudència existent sobre el tema de la intel·ligència artificial aplicada a robots o a sistemes autònoms capaços de realitzar tasques sense la intervenció humana, és encara molt limitada i, en general, no fa quasi diferències entre aparells teledirigits per un ésser humà, d'aquells capaços de funcionar autònomament.

Un dels robots més estesos avui dia en l'àmbit domèstic són els robots de neteja, però en l'àmbit industrial són cada vegada més variats i sofisticats. Malgrat això, és en l'àmbit militar on més s'han

---

<sup>210</sup> Fonament de dret tercer de la sentència 558/2010 de la Sala del Social del Tribunal Suprem, de 20 de gener de 2010.

desenvolupat les tecnologies d'intel·ligència artificial aplicada a robots o sistemes robotitzats. Es fa doncs necessari analitzar l'orientació legal que s'està desenvolupant en les aplicacions militars dels denominats robots autònoms letals, amb la finalitat de que per analogia preveure cap a on es podria orientar en el futur el legislador i la jurisprudència en el tractament de la robòtica combinada amb tecnologies d'Intel·ligència artificial en l'àmbit civil, i molt especialment en el de la logística. No podem oblidar, d'altra banda, que gran part de les tecnologies militars en aquest camp són, o poden ser-ho en el futur, directament aplicables a les més variades activitats civils.

## Robots autònoms letals

Un dels sistemes robotitzats més desenvolupat actualment és el dels robots autònoms letals. Es tracta de sistemes d'armes que, un cop activats, poden seleccionar i atacar objectius sense necessitat d'intervenció humana<sup>211</sup>. Els sistemes més coneguts són els anomenats drones, o avions no tripulats, equipats amb armament molt sofisticat, però els drones no són els únics sistemes actualment en desenvolupament.

---

<sup>211</sup> Es segueix aquí la definició de robots autònoms letals recollida en l'Informe de 2013 del Relator Especial sobre execucions extrajudicials, sumàries o arbitràries, presentat al Consell de Drets Humans de conformitat amb la resolució 17/5, se centra en els robots autònoms letals i la protecció de la vida: "...D'acord amb una definició àmpliament utilitzada (recolzada, entre d'altres, pel Departament de Defensa dels Estats Units i Human Rights Watch), l'expressió robots autònoms letals fa referència a sistemes d'armes robòtiques que, un cop activats, poden seleccionar i atacar objectius sense necessitat d'intervenció addicional d'un operador humà. L'important és que el robot té una «opció» autònoma pel que fa a la selecció d'un objectiu i l'ús de força letal.

Tot i que encara no s'utilitzen habitualment sistemes capaços d'adoptar decisions sobre el seu propi ús, i plena capacitat letal de manera absolutament autònoma en totes i cadascuna de les seves fases operatives, el progressiu augment d'aquest tipus d'armes ha posat de manifest la necessitat d'establir un marc legal clar i ben definit. Per tot això són cada vegada més nombrosos les crides internacionals per a la seva adequada regulació, o fins i tot per la seva prohibició<sup>212</sup>.

Així, en la Resolució del Parlament Europeu 2014/2567(RSP), de 27 de febrer de 2014, sobre l'ús de drones armats, es demana específicament a tots els estats que posseeixin tecnologia de drones armats que, entre altres coses, facin públics els fonaments jurídics que s'apliquen a l'ús dels drones, especifiquin la seva responsabilitat operativa i facilitin informació sobre les víctimes dels seus atacs, en particular, les civils. La mateixa resolució reconeix que l'ús de drones ha registrat un augment exponencial en l'últim decenni, i que els seus atacs s'han fet d'una manera en gran mesura opaca i sense assumir responsabilitats<sup>213</sup>.

---

<sup>212</sup> El Comitè Internacional per al Control de les Armes robòtiques, presenta en la seva pàgina web (<http://icrac.net>) un ampli conjunt de documents, col·laboracions i els més variats arguments en defensa d'aquesta prohibició.

<sup>213</sup> Alguns dels documents i acords internacionals que fan referència a aquest tema són esmentats en la referida Resolució del Parlament Europeu. Alguns d'ells són els informes del Relator Especial de les Nacions Unides sobre les execucions extrajudicials, sumàries o arbitràries relatiu a l'ús de vehicles aeris armats no tripulats de 28 de maig de 2010 i de 13 de setembre de 2013, i del Relator Especial de les Nacions Unides sobre la promoció i la protecció dels drets humans i les llibertats fonamentals en la lluita contra el terrorisme de 18 de setembre de 2013; l'informe de 13 de setembre de 2013 del Relator Especial de les Nacions Unides sobre les execucions extrajudicials, sumàries o arbitràries; les declaracions del secretari general de les Nacions Unides, Ban Ki-moon, de 13 d'agost de 2013 sobre l'ús de vehicles aeris armats no tripulats; l'audiència del 25 d'abril de 2013 sobre les implicacions de l'ús de vehicles aeris no tripulats pels drets humans, organitzada per la Subcomissió de Drets Humans del Parlament

La postura predominant entre la majoria d'experts i acadèmics que han abordat el tema, és que la responsabilitat última pels actes realitzats pels robots autònoms letals, ha de ser sempre humana, i que de cap manera es pot delegar aquesta responsabilitat a les pròpies màquines per sofisticades que aquestes siguin:

"... Segons el filòsof Peter Asaro, es pot considerar que estigui implícita en el dret internacional humanitari l'exigència que tota decisió relativa a l'ús de força letal sigui presa per éssers humans i no consisteixi en un procés automatitzat. D'acord amb aquest raonament, l'adopció de decisions relatives a l'ús de força letal sense intervenció de l'ésser humà és inherentment arbitrària, i les morts que es produeixen com a conseqüència d'elles constituïran una privació arbitrària de la vida..."<sup>214</sup>.

"... Aquest enfocament es basa en la creença que un ésser humà és sempre qui ha de prendre la decisió d'emprar força letal i, en conseqüència, interioritzar el cost de cada vida perduda en les hostilitats (o assumir-ne la responsabilitat), com a part de un procés deliberatiu d'interacció humana. Aquesta afirmació és aplicable fins i tot en els conflictes

---

conjuntament amb la seva Subcomissió de Seguretat i Defensa; l'estudi de 3 de maig de 2013 titulat "Aspectes de drets humans de l'ús de vehicles aeris i robots no tripulats en conflictes bèl·lics"; les Conclusions del Consell, de 19 i 20 de desembre de 2013, sobre els preparatius d'un programa europeu dels sistemes d'aeronaus pilotades a distància de gran autonomia i altitud mitjana de la propera generació en el període 2020-2025, l'article 110, apartat 2, del seu Reglament.

<sup>214</sup> Apartat 90 de l'informe de 2013 del Relator Especial sobre execucions extrajudicials, sumàries o arbitràries.

armats. La delegació d'aquest procés deshumanitza encara més els conflictes armats i impedeix parar-se a pensar en els casos en què fos possible. Les màquines són amorals i no moren, pel que no han de tenir poder de decisió sobre la vida i la mort d'éssers humans. Aquesta és una de les raons per les quals s'han prohibit les mines terrestres..."<sup>215</sup>.

El Relator Especial de les Nacions Unides sobre les execucions extrajudicials, sumàries o arbitràries, Christof Heyns, en el seu informe A/HRC/23/47 de data 9 d'abril de 2013, es pregunta sobre la responsabilitat en cas de pèrdues de vida com a conseqüència de les accions dels robots:

"... Els robots no tenen capacitat de discerniment moral, de manera que si causen pèrdues de vida no se'ls pot exigir cap tipus de responsabilitat, com seria normalment el cas si les decisions les haguessin pres éssers humans. En qui recau llavors la responsabilitat?..."<sup>216</sup>.

El mateix Relator recull en el seu informe la necessitat de crear un grup de treball que avaluï les qüestions jurídiques, ètiques i polítiques relacionades amb els robots autònoms letals, així com la idoneïtat o les deficiències dels actuals marcs jurídics internacionals i nacionals. El grup que planteja crear hauria de proposar un marc que permeti a la comunitat internacional abordar les qüestions jurídiques i polítiques relacionades amb els robots autònoms letals i formular recomanacions concretes:

---

<sup>215</sup> *Ibidem* apartat 94.

<sup>216</sup> *Ibidem* apartat 76.

"... Un supòsit bàsic en la majoria dels codis jurídics, morals i d'un altre tipus és que, quan estigui en joc la vida d'una persona o la possibilitat que pateixi altres greus conseqüències, el poder de decisió ha de correspondre a un ésser humà. La Convenció de l'Haia (IV) exigeix que qualsevol combatent tingui «al front una persona responsable». La clàusula de Martens, una norma vinculant de llarga tradició del dret internacional humanitari, exigeix específicament l'aplicació del «principi d'humanitat» en els conflictes armats. En excloure l'ésser humà de l'adopció de decisions, també es corre el risc de no aplicar el principi d'humanitat..."<sup>217</sup>.

Al reflexionar sobre la responsabilitat per les accions dels robots autònoms letals podem seguir al propi Relator de l'ONU:

"... Els experts han sostingut fermament que un enfocament regulador centrat en la tecnologia -és a dir, les pròpies armes- pot ser inadequat en el cas d'aquests dispositius, i que l'atenció s'ha de centrar més aviat en la intenció o l'ocupació..."<sup>218</sup>.

La delimitació de la responsabilitat no s'ha de centrar doncs en els majors o menors avenços de la tecnologia, sinó en la intenció que tinguin aquells que d'alguna manera participin en la posada en operativitat del sistema robotitzat, o l'ús que se'n faci.

---

<sup>217</sup> *Ibidem* apartat 89.

<sup>218</sup> *Ibidem* apartat 101.

Això no és obstacle perquè es pugui demanar també responsabilitats, almenys responsabilitats civils, a altres actors com poden ser programadors, fabricants, venedors, o similars, encara que també en aquest cas el nivell de desenvolupament legal i jurídic té uns nivells de desenvolupament molt diferents en cada país:

"... S'ha proposat que almenys s'exigeixi responsabilitat per danys i perjudicis als programadors i els fabricants, emprant un esquema similar al de la responsabilitat civil per productes defectuosos. No obstant això, la legislació relativa a la responsabilitat pels productes segueix sent en gran part inèdita en els diferents països..."<sup>219</sup>.

Si per qualsevol motiu no fos possible atribuir la responsabilitat a un ésser humà, el més raonable seria directament impedir el funcionament d'aquest sistema:

"... La qüestió de la responsabilitat legal pot ser fonamental. Si, en última instància, és inapropiat o inviable assignar responsabilitats en tots i cadascun dels casos esmentats més amunt, es produirà un buit de responsabilitat, amb la corresponent impunitat per l'ocupació de robots autònoms letals. Si la naturalesa d'una arma fa impossible exigir responsabilitats per les conseqüències del seu ús, s'ha de considerar el seu ús il·lícit i immoral i l'arma abominable..."<sup>220</sup>.

---

<sup>219</sup> *Ibídem* apartat 79.

<sup>220</sup> *Ibídem* apartat 80.

És interessant destacar, que en plantejar sistemes d'atribució de responsabilitats a persones com a conseqüència de les accions realitzades per part dels robots autònoms letals, sorgeixen propostes com l'atribució prèvia de responsabilitat (per exemple a qui posi operatiu el sistema) o l'obligació de mantenir un sistema de gravació de les activitats letals realitzades pel robot. Aquestes condicions són precisament algunes de les adoptades pel legislador en l'Estat de Nevada en regular la circulació de vehicles sense conductor per les vies públiques d'aquest Estat:

"... Cal considerar diverses formes noves d'establir la responsabilitat legal. Una de les condicions que podrien imposar-se a l'ocupació de robots autònoms letals és l'atribució prèvia de responsabilitat. Tenint en compte que la tecnologia podria permetre un seguiment i una reconstrucció més precises del que ha passat durant l'execució d'operacions letals, podria establir-se, com a condició per a la utilització d'aquestes armes, l'obligació d'instal·lar dispositius de gravació i realitzar un examen *a posteriori* de tot el material gravat, en els casos d'utilització de força letal, independentment de la condició de les persones que resultessin mortes..."<sup>221</sup>.

El criteri predominant en els nombrosos anàlisis i estudis que sobre el tema estan proliferant darrerament, remarca que en tot cas, la legitimitat en l'ús de la força, i especialment de la força letal, no es pot

---

<sup>221</sup> *Ibíd*em apartat 81.



delegar en una màquina, ja que la responsabilitat última ha de basar-se sempre en criteris morals i legals típicament humans<sup>222</sup>.

---

<sup>222</sup> Són molts els autors que sostenen aquesta postura. Així per exemple, Peter Asaro defensa que l'autoritat per utilitzar la força letal depèn sempre de les determinacions humanes i de la seva legitimitat legal i moral: "...En particular, hi ha un deure per part tant dels individus com dels estats en temps de pau, així com per part dels combatents, les organitzacions militars, i els estats en situacions de conflicte armat, pel qual no s'ha de delegar en una màquina o procés automatitzat l'autoritat o la capacitat per iniciar l'ús de la força letal de manera independent de les determinacions humanes, i de la seva legitimitat moral i legal en cada cas..."(Asaro, 2013).



## **Capítol divuitè:**

### **La mobilitat en el cicle del comerç electrònic**

---

#### **Mobilitat automatitzada de productes i persones**

En tot el cicle del comerç electrònic el lliurament del producte adquirit constitueix una fase fonamental de tot el procés. En aquest sentit, el canal utilitzat per fer arribar el producte al consumidor és diferent segons les característiques del producte o el model de negoci adoptat en cada cas. No obstant això, el més freqüent, per a aquells productes no intangibles adquirits per internet, sol ser el seu lliurament en el lloc designat pel client. En aquests casos adquireix una gran importància la mobilitat, o més concretament el medi físic utilitzat per fer arribar el producte al consumidor. La mobilitat és, des d'aquesta perspectiva, una fase fonamental en tot el procés de comercialització. Per això cobren gran importància els sistemes de mobilitat automatitzada i, més concretament els incipients sistemes de mobilitat autònoma, i amb això la resposta de la legislació i la jurisprudència davant l'aparició d'aquests sistemes.

La interacció de la intel·ligència artificial amb les tecnologies basades en la robòtica està avançant a grans passos molt ràpidament. Això comporta situacions inèdites pel que fa, per exemple, al trasllat de mercaderies del proveïdor al client; al trasllat de persones per les vies de comunicació; i en general a qualsevol tipus de mobilitat a l'entorn urbà,

sense la presència física de persones humanes que condueixin els vehicles i sistemes necessaris per a això.

Alguns dels exemples més coneguts actualment són els vehicles autònoms, és a dir, conduïts mitjançant tècniques d'intel·ligència artificial i sense la presència física del conductor. Aquests vehicles poden estar dissenyats per anar per les vies terrestres o fins i tot per l'aire, com els coneguts avions no tripulats (drones) o pel mar, com per exemple els vehicles submarins autònoms (AUV).

Un dels més recents exemples d'aquest tipus de mobilitat el constitueixen els vehicles capaços de circular per les vies públiques de manera autònoma. Aquests vehicles, que són ja una realitat, estan dissenyats per anar per les vies terrestres de manera autònoma, sense la conducció directa ni remota per part de cap ésser humà, tant per vies fèrries com per les vies públiques.

Només podem parlar amb propietat de vehicles autònoms quan poden circular sense la presència física del conductor, el que implica que disposen no només de sensors suficients, sinó, sobre tot, de tecnologies d'intel·ligència artificial. També mereix especial atenció la possible utilització en el futur dels denominats drones, els vehicles aeris autònoms, és a dir no tripulats.

Els drones es diferencien dels vehicles aeris teledirigits, precisament en aquesta capacitat de volar i dirigir-se a una destinació de manera autònoma. Encara que els drones i els vehicles aeris teledirigits han tingut el seu més fort desenvolupament amb finalitats militars, en l'actualitat s'estan estenent als més diversos camps dins de l'àmbit civil. Així recentment la companyia de missatgeria DHL, o la companyia de

vendes per internet Amazon es van plantejar la utilització d'aquest tipus de vehicles per distribuir els seus productes als clients.

Una qüestió que s'ha de tenir en compte és si es considera els drones com un avió, una aeronau o un altre tipus d'aparell<sup>223</sup>, ja que aquest punt pot determinar la normativa aplicable en aquesta matèria. Si ens fixem en Estats Units, la situació jurídica no està clara.

D'una banda, l'Administració Federal d'Aviació (FAA) considera que els sistemes d'aeronaus no tripulats estan subjectes a les seves normatives excepte quan aquests vehicles: “volin dins la línia visual de la persona que opera l'aeronau; i que sigui volat per hobby o amb finalitats recreatives” <sup>224</sup>, com per exemple les aeronaus utilitzades en l'aeromodelisme. Sota aquesta perspectiva, els drones estarien subjectes a les normatives de la FAA, el que significa que per poder operar-los es necessita un certificat de pilot, així com un certificat i matriculació de l'aeronau, que actualment no està disponible per als operadors d'aeronaus no tripulades.

D'altra banda, hi ha la sentència del jutge Patrick Geraghty, en el cas Horta v. Pirker<sup>225</sup>, que va sostenir que un drone no entrava dins de les definicions d'aeronaus de la part 1, secció 1.1, o el 49 USC secció

---

<sup>223</sup> Segons l'Institut d'Estudis Catalans, un avió és una “Aeronau amb propulsió pròpia que se sosté en l'aire per l'efecte combinat del pla de sustentació, de la velocitat i de les ales, que es mantenen fixes durant el vol”, mentre que una aeronau és qualsevol “Vehicle destinat a la navegació aèria”.

<sup>224</sup> Secció 336.c de la Llei de reforma i modernització de la FAA dels Estats Units, d'1 de febrer de 2012.

<sup>225</sup> Cas Michael P. Huerta, administrador de l'Administració Federal d'Aviació dels Estats Units, v. Raphael Pirker, de 6 de març de 2014.

40102(a)(6) i que “l’acceptació de la interpretació extralimitada de la definició d’aeronau del demandant (la FAA) resultaria *reductio ad absurdum* en l’afirmació de l’autoritat reguladora de la FAR (Regulacions de la FAA) sobre qualsevol dispositiu/objecte usat o capaç de volar en l’aire, sense importar el mètode de propulsió o la durada del vol”. Així doncs, aquesta sentència deixa entreveure que no hi ha una regulació aplicable sobre els drones comercials.

No considerem per tant en aquesta categoria aquells vehicles dirigits a distància pel conductor, o aquells sistemes que de manera autònoma realitzen alguna activitat concreta d’acord amb la informació proporcionada pels sensors incorporats al vehicle. Als efectes de delimitar qui és el responsable del vehicle en aquests casos, no hi ha cap variació respecte als vehicles tradicionals. Tot el marc legal actual i la jurisprudència en tots els casos deixen clar que el responsable de la conducció del vehicle és en tots els casos el conductor, independentment que el vehicle tingui alguna o algunes de les seves funcions totalment automatitzades.

Així, per exemple, actualment són cada vegada més nombrosos els vehicles terrestres que van incorporant sistemes automatitzats com a part del equipament normal, tant de sèrie com d’instal·lació opcional. No obstant això aquests sistemes estan pensats, en general, per facilitar la conducció del vehicle per part del conductor i no per substituir-lo en la seva responsabilitat global respecte a la conducció del vehicle. Per tant, en aquests casos no podem parlar en propietat de vehicles autònoms. Aquests sistemes automatitzats es limiten a respondre als senyals detectades a través de diferents sensors per, en funció d’aquestes senyals, accionar determinats dispositius. El sistema es limita a

reaccionar als impulsos rebuts des del sensor corresponent, però en cap cas substitueixen la funció del conductor com a responsable de la conducció del vehicle. Per això mateix, els vehicles que porten incorporats alguns d'aquests sistemes, per sofisticats que siguin, no poden considerar-se com vehicles autònoms.

Alguns dels sistemes més estesos actualment són els que a partir de la humitat detectada posen en marxa els eixugaparabrises a diferents velocitats; o els que graduen els llums del vehicle en funció de la il·luminació detectada pels sensors; els que avisen de la no col·locació dels cinturons de seguretat quan el sensor dels seients detecta que un dels passatgers no el porta correctament; el canvi de marxes automàtic; els sistemes de frenada segons el paviment o la marxa del vehicle, incloent els sistemes de frenada d'emergència en detectar obstacles amb els seus sensors; els limitadors de velocitat; els ordinadors de bord; els *airbags* i d'altres mecanismes similars.

Motor, rodes, amortidors, climatitzadors,... pràcticament totes les parts dels vehicles actuals són susceptibles d'estar controlades per sistemes autònoms que actuen d'acord a les senyals detectades a través dels sensors. Però tots aquests sistemes estan concebuts per a vehicles conduïts per un ésser humà. Fins i tot quan algun d'aquests sistemes impedeix físicament la conducció del vehicle per part d'un conductor amb taxes d'alcohol superior a les autoritzades, o quan, com passa en alguns casos, és el propi vehicle el que posa els cinturons de seguretat al conductor i passatgers independentment del seu desig, o quan el vehicle s'atura en detectar somnolència en el conductor, o quan no li permet accedir-hi si no es tracta d'algú prèviament autoritzat o aquest no pot identificar-se com a tal. En tots els casos aquests sistemes

automatitzats es limiten a respostes prèviament programades sense que en cap cas alterin el fet que és sempre l'ésser humà el conductor del vehicle i per tant el que a tots els efectes és el seu responsable. Fins i tot els vehicles dotats actualment de sistemes per a l'aparcament del vehicle de manera autònoma, depenen de la decisió del conductor per ordenar la realització de la maniobra, per la qual cosa pressuposa la seva presència física en el lloc i amb això la seva pròpia responsabilitat. El tema es complica, tanmateix, quan no ens referim a sistemes automatitzats, sinó a vehicles capaços de circular de manera autònoma sense necessitat de la presència física en el vehicle per part del conductor.

## **Els vehicles autònoms**

L'aparició de vehicles plenament autònoms planteja nombrosos interrogants tant legals com jurídics. Així, en cas d'accident per un mal funcionament d'un d'aquests vehicles, qui s'hauria de considerar responsable: el fabricant del vehicle, el programador del sistema, el dissenyador dels sensors, el propietari, el venedor?

En cas d'avaria o de danys produïts per un mal funcionament de la màquina sol estar ben definida la possible responsabilitat de fabricants, dissenyadors, programadors, o qualsevol altre professional involucrat en la seva construcció. En general, la interpretació sobre els nivells de responsabilitat en cas d'un mal funcionament dels sistemes ve definida per les pròpies competències que corresponen a cadascun dels actors involucrats.



Així, els ensenyaments mínims establerts per a exercir les diferents professions es recullen normativament. En aquest sentit, al nostre país els ensenyaments mínims d'estudis com els de tècnic/a superior en programació de la producció en fabricació mecànica, vénen establertes en el Reial Decret 1687/2007, de 14 de desembre; o els del títol de Tècnic Superior en Automatització i Robòtica Industrial, es recullen en el Reial Decret 1581/2011, de 4 de novembre; o les competències professionals, personals i socials del títol de programador de la producció en fabricació mecànica que han d'adquirir els estudiants que cursin la corresponent formació professional de grau superior, vénen establertes en la seva pròpia normativa específica<sup>226</sup>. Així, entre les diferents competències que han d'adquirir aquests estudiants hi ha les de supervisar la programació i posada a punt de les màquines de control numèric, robots i manipuladors per a la mecanització:

"... a) Determinar els processos de mecanitzat, interpretant la informació tècnica inclosa en els plànols, en les normes de fabricació i en els catàlegs.

b) Elaborar els procediments de muntatge de béns d'equip, a partir de la interpretació de la informació tècnica inclosa en els plànols, en les normes de fabricació i en els catàlegs.

c) Supervisar la programació i posada a punt de les màquines de control numèric, robots i manipuladors per a la mecanització

---

<sup>226</sup> El Decret 55/2014, de 22 d'abril, estableix el currículum del cicle formatiu de grau superior de programació de la producció en fabricació mecànica, que si bé no habilita en si mateix per a l'exercici d'una professió concreta, sí que proporciona els continguts necessaris per a adquirir les competències necessàries per al control i posada a punt de, entre altres, els robots i sistemes robotitzats.

assegurant el compliment de les normatives de qualitat, prevenció de riscos laborals i protecció ambiental.

d) Programar la producció utilitzant tècniques i eines de gestió informatitzada, controlant el seu compliment i responent a situacions imprevistes, per assolir els objectius establerts.

e) Determinar l'aprovisionament necessari per a garantir el subministrament en el moment adequat, reaccionant davant les contingències no previstes i resolent els conflictes sorgits en l'aprovisionament.

f) Assegurar que els processos de fabricació s'ajusten als procediments establerts, supervisant i controlant el seu desenvolupament i resolent possibles contingències que es puguin presentar.

g) Gestionar el manteniment dels recursos de la seva àrea, planificant, programant i verificant el seu compliment en funció de les càrregues de treball i la necessitat del manteniment..."<sup>227</sup>.

D'altra banda, en el cas dels vehicles que sense requerir la presència física del conductor en el lloc, siguin conduïts a través de tele conducció, la responsabilitat segueix sent del conductor, perquè fins i tot encara que la seva absència del lloc pugui representar una certa limitació de la seva percepció de l'entorn, ell ha de disposar abans de l'inici de la conducció de tots els elements necessaris per garantir el seu domini en tot moment de la conducció del vehicle. El tema es complica més quan parlem de vehicles totalment autònoms, en què la conducció no és

---

<sup>227</sup> Punt 2.2 de l'annex del Decret 55/2014, de 22 d'abril.

realitzada ni telemàticament ni de manera directa per cap ésser humà, si no pel propi vehicle mitjançant tecnologies d'intel·ligència artificial.

Podem definir un vehicle autònom, també conegut com a vehicle no tripulat, com "un vehicle de motor que utilitza intel·ligència artificial, sensors i sistemes de posicionament global de manera coordinada, per tal de conduir-se a si mateix sense la intervenció activa d'un operador humà"<sup>228</sup>.

Les experiències de vehicles sense conductor van començar fa ja molts anys. De fet, en 1925 es van realitzar proves del linrrican Wonder un vehicle capaç d'imitar mitjançant ones de ràdio el recorregut d'un altre que li precedís, o les realitzades el 1958 per General Motors en unió de RCA en un vehicle guiat per circuits i cables magnètics situats sobre l'asfalt. L'any 1991 el Departament d'Estat Nord-americà, en unió de diferents companyies privades, va desenvolupar el Demo'97, però posteriorment es va centrar exclusivament en el desenvolupament de vehicles autònoms per a ús militar, dels quals es van desenvolupar diversos models.

En l'actualitat Google utilitza un vehicle autònom. El vehicle autònom de Google no és l'únic desenvolupant-se en l'actualitat. Algunes marques com Mercedes, en col·laboració amb Nokia estan desenvolupant altres models. També el EN-V de General Motors, el Volkswagen Temporary

---

<sup>228</sup> Aquesta és la definició recollida pel Comitè de Transport de l'Assemblea Legislativa de l'Estat de Nevada, en la legislació sobre aquest tipus de vehicles. La primera Llei desenvolupada per permetre la circulació de vehicles autònoms per les vies públiques de Nevada (Assembly Bill No. 511-Committee on Transportation, es pot consultar a [http://www.leg.state.nv.us/Session/76th2011/Bills/AB/AB511\\_EN.pdf](http://www.leg.state.nv.us/Session/76th2011/Bills/AB/AB511_EN.pdf)).

Auto Pilot de Volkswagen<sup>229</sup>. Altres companyies automobilístiques com Audi, BMW, Nissan, Cadillac, Tesla, Volvo, Toyota i altres estan estudiant actualment sistemes per desenvolupar vehicles autònoms. No obstant això, l'impuls més gran es produeix quan el 2010 Google aposta per aquests vehicles i posa en marxa el seu propi sistema per a vehicles autònoms.

Google converteix ràpidament el seu sistema en un dels vehicles autònoms més coneguts actualment. En el seu vehicle, entre els diferents sistemes de sensors que interaccionen per a proporcionar una visió integral de l'entorn en què ell mateix es mou, destaca el Laser Imaging Detection and Ranging, (Lidar). Es tracta d'un dispositiu que detecta objectes i mesura la distància fins a ells mitjançant raigs de llum, concretament faigs làser, de manera que construeix una imatge tridimensional al voltant del vehicle, en el que posiciona vianants, vehicles, senyals, mobiliari urbà i qualsevol objecte situat al camp d'acció del vehicle autònom <sup>230</sup>. Les dades subministrades pel Lidar es complementen amb les subministrades de manera integrada per altres sistemes avançats de sensors com radar; GPS; visió computeritzada; detectors làser; i altres similars. Amb totes aquestes dades el vehicle és capaç d'interpretar autònomament la informació, identificar la ruta apropiada, detectar els obstacles i la senyalització rellevant, i conduir-se

---

<sup>229</sup> Aquest model va ser presentat per Volkswagen aprofitant la presentació del projecte HAVEit (Highly Automated Vehicles for Intelligent Transport) un projecte de recerca de transport intel·ligent promogut per la Unió Europea. Podeu consultar el projecte HAVEit a <http://www.haveit-eu.org/displayITM1.asp?ITMID=6&LANG=EN>

<sup>230</sup> El Lidar que empra Google és el VELODYNE HDL-64E S2, d'alta definició. Té 64 raigs làser i gira sobre si mateix 360 ° de manera permanent fins a 900 voltes per minut per monitoritzar tot l'entorn del cotxe amb 1,3 milions de punts per segon.

a si mateix per circular per les vies públiques sense intervenció humana<sup>231</sup>.

## Resposta legal als vehicles autònoms

L'aparició dels vehicles autònoms genera una situació en què el marc legal vigent fins a aquest moment es demostra insuficient per donar resposta a les diferents situacions que aquesta presència pugui generar en el futur. En aquest sentit, l'estat nord-americà de Nevada ha estat el primer a legislar regulant la circulació per les seves vies públiques de vehicles autònoms, capaços de circular sense necessitat de la presència física del conductor gràcies als seus sensors i les seves tecnologies d'intel·ligència artificial<sup>232</sup>.

El Comitè de Transport de l'Assemblea de Nevada va aprovar al juny de 2011 la norma, després desenvolupada reglamentàriament pel Departament de Vehicles de Motor que va entrar en vigor l'1 de març de 2012, en què s'establia aquesta possibilitat de circulació de vehicles autònoms. La normativa de Nevada diferencia clarament els vehicles de conducció autònoma de tots aquells dotats de sistemes automatitzats per facilitar la conducció, els quals en aquest cas no són considerats vehicles autònoms:

---

<sup>231</sup> Es poden consultar les característiques d'aquest vehicle en l'article "What we'RE driving at" a la pàgina oficial de Google: <http://googleblog.blogspot.com.es/2010/10/what-were-driving-at.html>.

<sup>232</sup> La mateixa norma de Nevada (Assembly Bill No 511-Committee on Transportation) defineix com intel·ligència artificial l'ús d'ordinadors i equips relacionats, que permeten habilitar una màquina per tal de reproduir o imitar el comportament dels éssers humans.

"... El Departament interpreta el terme «vehicle autònom» de manera que exclogui els vehicles habilitats amb un sistema de seguretat o sistema d'assistència a la conducció, incloent, sense limitació, els sistemes que proporcionin assistència electrònica d'angle mort, els sistemes per evitar accidents, els de frenada d'emergència, els assistents d'aparcament, el control adaptatiu de la velocitat de creuer, els d'assistència per mantenir-se en el carril, els avisos de sortida de carril i embussos de trànsit i els d'assistència en cues, llevat que el vehicle també estigui habilitat amb intel·ligència artificial i tecnologies que permetin que el vehicle pugui dur a terme totes les operacions mecàniques de conducció sense el control actiu o continu d'una persona física..."<sup>233</sup>.

La Normativa de Nevada estableix la possible responsabilitat en cas d'accident, especificant clarament que encara que no sigui el conductor, es considera operador del vehicle autònom aquella persona que posi en funcionament el vehicle:

"... A l'efecte d'aquest capítol, llevat que el context indiqui el contrari, una persona es considera que és l'operador d'un vehicle autònom, quan la persona fa que el vehicle autònom es posi en funcionament, independentment de si la persona està físicament present en el vehicle mentre està en marxa..."<sup>234</sup>.

---

<sup>233</sup> Secció 2 del Reglament adoptat pel Departament de Vehicles de Motor de Nevada LCB No R084-11. Vigent a partir de l'1 de març de 2012.

<sup>234</sup> *Ibíd*em Secció 3.

,En definir la consideració d'operador referida a qui posi en marxa el vehicle de manera que aquest pugui circular de manera autònoma, s'estableixen les bases sobre qui és en tot cas el responsable per les possibles infraccions que pugués cometre el vehicle autònom:

"... Als efectes de fer complir les lleis de trànsit i altres lleis aplicables als conductors i als vehicles de motor operats en aquest Estat, l'operador d'un vehicle autònom que funcioni de manera autònoma es considerarà que és el conductor del vehicle autònom amb independència que la persona estigui físicament present en el vehicle autònom mentre aquest estigui en marxa..."<sup>235</sup>.

En reconèixer l'operador a efectes legals com el conductor del vehicle autònom, sembla lògic que l'operador tingui els coneixements i requisits necessaris en l'Estat de Nevada per conduir vehicles per les vies públiques de l'Estat. Això és efectivament el que requereix el legislador en establir que qui vulgui operar un vehicle autònom a Nevada ha d'estar en possessió d'una llicència de conduir vàlida en aquest Estat i obtenir una ampliació de la mateixa en el que denomina de tipus G:

"... Llevat que es disposi el contrari en l'article 10 d'aquest Reglament, una persona que tingui una llicència de conduir en aquest Estat i vulgui operar un vehicle autònom de manera autònoma en aquest Estat, ha d'obtenir un permís G afegit a la seva llicència com a conductor atorgada pel Departament, de conformitat amb la NAC 483.110 abans que l'esmentada persona pugui operar un vehicle autònom en aquest Estat. Es

---

<sup>235</sup> *Ibidem* Secció 4.

pot demanar mitjançant la presentació d'una sol·licitud en un formulari proporcionat pel Departament..."<sup>236</sup>.

Per a què un vehicle autònom pugui ser testat abans de la seva autorització per a què circuli en forma autònoma per les vies públiques de Nevada, ha de reunir unes condicions prèvies establertes en la pròpia norma. Així, es preveu la possibilitat que el vehicle tingui un accident i sigui necessari disposar de les dades generades des del propi vehicle. La norma estableix que tot vehicle autònom ha d'estar dotat d'algun sistema que permeti recollir i emmagatzemar les dades provinents dels sensors del vehicle de manera que quedin gravades aquestes dades des dels 30 segons anteriors a qualsevol accident en que es pugui veure implicat el vehicle autònom. Aquestes dades s'han de conservar almenys durant els tres anys posteriors a aquest accident:

"... cal que disposi d'un mecanisme separat afegit, i separat de, qualsevol altre mecanisme exigít per la llei, per capturar i emmagatzemar les dades dels sensors de tecnologia autònoma durant almenys 30 segons abans que ocorri una col·lisió entre el vehicle autònom i un altre vehicle, objecte o persona física, mentre que el vehicle funciona de manera autònoma. [...] Aquestes dades s'han de conservar durant 3 anys després de la data de la col·lisió..."<sup>237</sup>.

A més a més del sistema de conservació de dades anterior, el vehicle ha de disposar d'un sistema de seguretat preparat perquè en cas de fallada en la tecnologia del vehicle, es comuniqui immediatament a l'operador

---

<sup>236</sup> *Ibíd*em secció 5.1.

<sup>237</sup> *Ibíd*em secció 8.2 (d).



perquè aquest assumeixi el control del vehicle. Cal a més a més demostrar-se que ha circulat almenys 10.000 milles en manera autònoma sense incidents. Per realitzar aquestes milles de prova, el Departament de Vehicles de Motor concedeix una llicència provisional a la que almenys dues persones, inclòs l'operador, han de circular per les vies autoritzades per a això, a bord del vehicle autònom. Entre les condicions que ha de reunir el vehicle, hi ha la demostració de la intel·ligència artificial i la tecnologia utilitzada pel vehicle autònom.

En realitat els sistemes d'intel·ligència artificial són els que a la pràctica han de garantir la viabilitat que el vehicle pugui circular per les vies públiques amb seguretat sense precisar de la presència d'una persona física conduint el vehicle: [booking@caldea.com](mailto:booking@caldea.com)

"... Disposa d'un sistema de seguretat per alertar a l'operador del vehicle autònom perquè prengui el control del vehicle autònom si es detecta un error de la tecnologia..."<sup>238</sup>.

"... b) Trametre al Departament, juntament amb la sol·licitud d'autorització de circulació, una prova satisfactòria que un o més dels vehicles autònoms del sol·licitant han estat circulant per un mínim combinat de no menys de 10.000 milles de manera autònoma. [...] en diverses condicions i de manera que es demostrï la seguretat del vehicle o vehicles en aquestes condicions. Això inclou, sense limitació, el funcionament del vehicle en diverses condicions meteorològiques, en diversos tipus de carreteres i durant diverses hores del dia i de la nit.

---

<sup>238</sup> *Ibíd*em secció 8.2 (b).

c) Demostrar la intel·ligència artificial i la tecnologia utilitzada en els seus vehicles autònoms al Departament per a la seva aprovació...”<sup>239</sup>.

En definitiva, la normativa aprovada per l'Estat de Nevada se centra especialment en establir clarament que la responsabilitat de tot el que succeeixi a causa de la circulació d'un vehicle autònom per les vies públiques de Nevada, correspon sempre a una persona humana. La que es defineix com l'operador, independentment que es trobi o no físicament al lloc, i encara que no estigui realment exercint cap maniobra de conducció. Fins i tot en el cas d'una avaria o mal funcionament del sistema, l'operador s'equipara a tots els efectes al conductor del vehicle i per tant el seu responsable.

---

<sup>239</sup> *Ibíd*em secció 8.3.

## **Capítol dinovè:**

### **Fenomenologia dels sistemes de pagament virtual**

---

#### **Els sistemes de pagament tradicionals**

Els diferents sistemes de pagament utilitzats habitualment a Internet, tenen els mateixos condicionants i exigències que quan s'utilitzen aquests mateixos sistemes en l'espai no virtual. Diners en metàl·lic en qualsevol de les divises reconegudes en els diferents mercats; targetes de crèdit, dèbit i en general qualsevol altre tipus de targeta similar; anotacions en compte bancari; talons i altres documents bancaris de pagament; o qualsevol dels altres sistemes tradicionalment acceptats en les transaccions financeres.

Qualsevol dels sistemes tradicionals de pagament utilitzats en l'àmbit mercantil són tractats legal i jurídicament de la mateixa manera quan s'utilitzen a Internet com quan es fa en el món físic. Les nombroses sentències i normes jurídiques, tant nacionals com internacionals, estableixen un similar tractament sigui quin sigui l'entorn utilitzat. Així per exemple, el delictes d'estafa agreujada recollit en la legislació penal espanyola, estableix les condicions necessàries per a considerar que s'ha produït aquest delictes i també quan s'ha de qualificar de manera agreujada. Entre totes les consideracions i condicionants esmentats en aquesta norma no hi ha cap referència a l'entorn en què es produeix la possible estafa.

La jurisprudència recull aquest criteri de manera que podem esmentar, per exemple, el cas d'una presumpta estafa en encarregar per Internet a una empresa Nord-americana la confecció d'una pàgina web, destinada a la venda de productes als Estats Units per mitjà de comerç electrònic. Donat que pel pagament es va utilitzar un xec sense fons, el tribunal que va veure el recurs de cassació, va decidir que no havia "lloc al recurs de cassació interposat, per l'acusat, contra sentència de 20 de novembre de 2007, dictada per l'Audiència Provincial de Lleó, Secció Primera, que el va condemnar com autor d'un delictes d'estafa agreujada per l'ús de xec per a la defraudació". Subratlla el Tribunal Suprem que:

"... l'ús del xec és ja des d'un principi determinant de l'estafa agreujada sense que es pugui sostenir que sigui objecte de dues sancions, aplicant directament l'art. 250.1.3 CP. que constitueix un subtipus agreujat que engloba tots els mitjans de pagament o crèdit més usuals en el tràfic mercantil (xec, pagaré, lletra de canvi o negoci jurídic fictici) i en què aquests són el mitjà o mecanisme a través del qual es dugui a terme o es produeix l'engany típic de l'estafa, sancionant exclusivament sobre la base del subtipus agreujat..."<sup>240</sup>.

L'ús a internet dels mitjans tradicionals de pagament està per tant sotmès als procediments comercials i bancaris tradicionals. En tots els casos estan ben establerts els procediments per decidir sobre el valor de la moneda, les comissions, el saldo disponible, les garanties assumides i

---

<sup>240</sup> Fonament de dret quart de la sentència 512/2008, de 17 de juliol de 2008, de la Sala Segona del Penal del Tribunal Suprem.

en general prendre les decisions que regiran el tractament econòmic de la transacció.

En tots els casos el paper de "les màquines" és merament el de facilitar les transaccions en un entorn virtual, de manera més ràpida i eficient, però sense que això representi cap variació transcendental en el tractament jurídic del pagament i les seves conseqüències. Això és extensible a tots els sistemes de pagament utilitzats tradicionalment, però l'evolució d'internet fa aparèixer altres sistemes de pagament, exclusivament dissenyats per ser utilitzats en aquest entorn. Un dels més coneguts és el de PayPal.

## **PayPal i d'altres passarel·les de pagament**

PayPal és un sistema que permet l'entrega i l'enviament de diners a qualsevol lloc del món, així com efectuar pagaments de les compres fetes mitjançant comerç electrònic. Aquest sistema està pensat per macropagaments però també es pot obrir una compta per micropagaments amb unes tarifes més reduïdes. D'altra banda, aquest és un sistema de pagament de dèbit, ja que en el moment de fer la transacció es descompten els diners del saldo que cada usuari té al seu compte de PayPal<sup>241</sup>.

Es tracta d'un sistema de pagament electrònic a través d'Internet que segueix un model de prepagament. Un usuari es crea un compte on pot transferir diners des d'un compte bancari, rebre/fer pagaments i retirar-ne els fons. Per efectuar un pagament, l'usuari es connecta al seu

---

<sup>241</sup> <https://micropayments.paypal-labs.com/>

compte, indica el compte del receptor (identificat mitjançant un correu electrònic) i la quantitat que vol transferir. Hi ha diferents tipus de compte, segons el tipus d'usuari que utilitzarà el sistema:

- Personal (per a particulars que efectuen pagaments, amb limitació de la quantitat disponible per als cobraments),
- Premier (pensada específicament per als venedors),
- Business (únicament per a empreses).

Hi ha la possibilitat d'efectuar un pagament a algú que no disposa de compte, si bé en aquest cas haurà de crear un compte en aquell moment, i també permet rebre en un compte PayPal pagaments fets amb una tarja bancària acceptada per PayPal.

L'ús del sistema és força senzill. Un usuari es connecta a la web de PayPal i escull "Crear compte". Després omple el formulari on cal indicar una adreça de correu, la que actuarà com a identificador, i una contrasenya d'accés. L'usuari ha d'afegir informació sobre targetes i comptes bancaris on rebre/ingressar diners. PayPal disposa de mecanismes per comprovar la veracitat d'aquesta informació pel que en la pràctica, l'ús d'aquest sistema segueix plenament els mateixos procediments que per a les transaccions comercials usals. PayPal es mou exclusivament en l'entorn virtual, però això no comporta cap diferència real en els procediments que faríem servir en qualsevol altre entorn en el que es produeixi l'intercanvi comercial.

Per afegir diners al compte PayPal, l'usuari necessita disposar d'un compte bancari confirmat en el món real. Llavors entra al seu compte, selecciona l'opció "Afegir fons" i "Transferir fons des d'un compte bancari". La transferència es fa efectiva en uns 14/16 dies. PayPal no

cobra cap comissió per aquesta acció. Per realitzar un pagament l'usuari inicia una sessió al seu compte, selecciona "Enviar diners", escull el tipus d'enviament personal/comercial i continua. Més endavant caldrà indicar el compte del destinatari i efectuar la transacció.

Per que un comerç virtual pugui integrar pagaments amb aquest sistema a la seva botiga virtual es connecta al seu compte, i selecciona l'opció "Vendre a internet"/"Botons de PayPal" i "Crear botó". Llavors, omple les dades sol·licitades i l'aplicatiu li generarà de forma automàtica el codi HTML que ha d'incrustar a la seva botiga virtual.

L'usuari diposita tota la seva confiança en l'empresa PayPal que és qui gestiona el compte de cada usuari. La seguretat ve donada per una contrasenya que l'usuari ha d'introduir per accedir al seu compte. L'enviament d'aquesta contrasenya es fa a través d'una connexió xifrada.

La confidencialitat en aquest sistema no està garantida, doncs PayPal coneix el detall de tots els pagaments efectuats per cadascun del seus usuaris. Tanmateix, les comunicacions, en anar xifrades, queden protegides contra l'escolta de tercers. Per les seves pròpies característiques, no és possible l'anonimat en aquest sistema de pagament. L'usuari s'identifica amb la seva credencial i se suposa que PayPal actua de forma honesta no modificant les transaccions efectuades pels seus usuaris.

La integritat i autenticació d'aquest sistema depèn doncs del nivell de confiança que PayPal desperti entre els seus usuaris, doncs si es percep com a poc fiable es produiria el rebuig del sistema de manera immediata. L'empresa PayPal és qui té coneixement de totes les operacions

efectuades. El no rebuig es dona mentre els usuaris confiïn en la honestedat d'aquesta empresa. Obrir un compte, carregar-hi saldo, efectuar un pagament i retirar diners d'un compte és gratuït.

Per rebre el pagament d'una compra, hi ha una comissió de 0.35 euros més un percentatge que oscil·la entre 1.9% i 3.4%. Les transferències personals són gratuïtes si utilitzen saldo d'un compte PayPal o d'un compte bancari. Si s'efectua amb tarja bancària, hi ha una comissió de 0.35 euros més 3,4%. En tots els casos es pot escollir si aquesta comissió la paga l'emissor o el receptor.

Veiem doncs, que PayPal no és més que una passarel·la que utilitza l'espai virtual i permet accedir als sistemes tradicionals de pagament. Encara que PayPal és la passarel·la de pagament més coneguda, no és l'única. De fet hi han d'altres molt similars, que responen als mateixos criteris. Algunes d'aquestes passarel·les de pagament són: Pingit, Zapp, iZettle, Mymoid i moltes altres com aquestes.

## **Bitcoin i d'altres monedes virtuals**

A diferència dels sistemes de pagament anteriors, Bitcoin, i les altres monedes virtuals aparegudes els darrers temps, són monedes generades pel propi sistema. Podríem dir que es tracta del més semblant al desenvolupament d'un sistema de pagament no generat per un estat o un banc central, sinó per les pròpies màquines sense cap control centralitzat. Bitcoin és una moneda electrònica creada específicament per operar en el món virtual. Es tracta d'un sistema de diners digitals que funciona de forma distribuïda directament entre els diferents usuaris



mitjançant tecnologia “peer to peer” (P2P) sense que existeixi una entitat central que reguli les transaccions. Les monedes es transfereixen d’usuari a usuari mitjançant un missatge signat per l’emissor que conté la moneda transferida i la clau pública del receptor. Totes les transaccions s’emmagatzemen en una estructura de dades distribuïda que serveix per consultar si una moneda que rebem ha estat gastada amb anterioritat pel mateix pagador.

Bitcoin va aparèixer el 2009 i va ser acceptada ràpidament per molts usuaris d’Internet, incloent nombroses companyies. El seu tractament a tots els efectes és per a aquests usuaris el mateix que si es tractés de diners en efectiu. El pagament amb aquesta moneda es fa mitjançant un sistema de criptografia asimètrica en el qual el propietari d’una moneda l’envia al destinatari del pagament afegint al final la signatura en el *hash*<sup>242</sup> de la transacció anterior juntament amb la clau pública del destinatari. Un cop es verifica que qui fa l’enviament era el propietari real de la moneda i que aquesta no havia estat utilitzada anteriorment, el receptor de la moneda passa a ser el nou propietari de la mateixa i la podrà transferir un altre cop.

Les principals formes per obtenir Bitcoins són: d’una banda, rebre-la transferida d’un altre usuari que ja tenia monedes; una altra manera es la compra amb una moneda física com el dòlar o l’euro; finalment, també es pot obtenir Bitcoins com a recompensa per la cessió de potència de càlcul utilitzat per proporcionar integritat a l’historial de transaccions mitjançant la comprovació de les funcions *hash*, ja que els usuaris que troben una d’aquestes preimatges d’una funció *hash* reben una moneda Bitcoin com a premi.

---

<sup>242</sup> Un *hash* és un algorisme criptogràfic per a generar claus.

Un usuari que vulgui utilitzar aquest sistema s'ha d'instal·lar l'aplicació Bitcoin. Aquesta aplicació crearà un moneder que queda emmagatzemat al disc de l'usuari. Aquest aplicatiu també descarregarà d'Internet l'historial de transaccions necessari per detectar operacions de sobre despesa. També hi ha la possibilitat de donar-se d'alta en un servidor remot que actua com a moneder de confiança per als seus clients.

La sobre despesa es controla mitjançant un registre de transaccions que es gestiona de forma col·lectiva a través de la xarxa. La seva integritat es garanteix mitjançant un procés computacionalment costós que garanteix que la informació d'aquest registre és íntegra sempre que la majoria dels participants en aquest sistema siguin honestos. A cada operació que es fa, és necessari comprovar el registre de transaccions per assegurar-se que la moneda no ha estat gastada amb anterioritat. En aquest sentit, es tracta d'un sistema online.

Les transaccions venen identificades per la clau pública de l'emissor i del receptor d'un pagament. Si la identitat dels propietaris d'aquestes claus es manté secreta, la seva confidencialitat també. En aquest sentit es tracta d'un sistema anònim, les monedes poden ser guardades en qualsevol ordinador o per un tercer. D'altre banda, la facilitat per obrir diversos comptes ajuda a preservar l'anonimat.

En els pagaments electrònics clàssics, hi ha un actor central (el banc) que s'encarrega de generar monedes i de controlar la sobre despesa. En aquest escenari les monedes es transfereixen als usuaris a canvi de diners reals i en el moment del dipòsit el seu valor és reemborsat.

A Bitcoin no hi ha cap figura central amb capacitat de generar i posar en circulació monedes. Les monedes es generen de forma col·lectiva

(mitjançant un sistema que controla el ritme de generació evitant una implosió de monedes que anul·laria el valor) de tal manera que les monedes noves es distribueixen de forma aleatòria entre els usuaris que col·laboren en el procés de garantir la integritat del registre de transaccions.

Bitcoin utilitza criptografia asimètrica com DigiCash o NetCash però, a diferència d'aquests, no requereix que l'usuari disposi d'un compte bancari associat.

Entre les principals característiques de Bitcoin destaca el fet de no dependre de cap banc central, estat, ni entitat financera concreta. El seu alt nivell de descentralització fa que s'eliminïn la majoria d'intermediaris, ja que les transaccions econòmiques es realitzen directament de persona a persona, alhora que s'evita la intervenció i el control per part dels mercats financers tradicionals. Són els propis usuaris, a través de milers d'ordinadors de tot el món, els que realitzen directament el seguiment i control de les transaccions realitzades amb Bitcoins.

L'usuari és propietari absolut dels Bitcoins de què disposi, pel que els seus comptes no poden ser intervinguts, decomissats, congelats, ni condicionats de cap manera, ja que fins i tot es poden utilitzar sense revelar la identitat i garantint totalment l'anonimat. Les comptes en Bitcoins no estan vinculades a persones concretes, sinó a les claus públic-privades generades a l'atzar. El propietari no ho és perquè tingui els Bitcoins al seu nom, sinó perquè és l'únic que coneix aquestes claus que li permeten utilitzar els seus diners de manera totalment anònima. Els Bitcoins es poden comprar i vendre utilitzant qualsevol altra moneda de curs legal, mentre que el fet que les transaccions siguin irreversibles i

el complex sistema criptogràfic establert, fa molt difícil la falsificació i dota el sistema aparentment d'uns alts nivells de seguretat.

Bitcoin va néixer com una moneda digital segura i fiable orientada a permetre el lliure intercanvi econòmic entre persones de tot el món, sense estar sotmesa als controls i manipulacions dels mercats i sistemes financers tradicionals. No obstant això, aquesta presumpta seguretat fonamental per a la pervivència del sistema basat precisament en la confiança dels usuaris, s'ha vist qüestionada per algunes operacions fraudulentas que teòricament no s'haurien d'haver produït. Així per exemple, va ser suficient amb la notícia apareguda al febrer de 2014 que possiblement diversos pirates haurien robat un total de 744.000 Bitcoins (prop d'un 6% de tots els Bitcoin en circulació) de la major plataforma de cotització de Bitcoin, Mt gox, perquè la seva cotització es desplomés fins als 423 dòlars, lluny dels 1.200 en què havia arribat a cotitzar poc abans<sup>243</sup>.

## **La responsabilitat per l'ús de les monedes virtuals**

Encara que Bitcoin és una moneda virtual generada pel mateix sistema mitjançant una sèrie aleatòria d'algorismes, és a dir, és generada per les màquines d'acord a les coordenades prèviament establertes, té els mateixos efectes que les monedes generades pels bancs centrals.

---

<sup>243</sup> Notícia apareguda a les publicacions econòmiques de tot el món, malgrat la qual cosa el sistema sembla haver resistit bé la pressió dels mercats. Pot consultar més informació sobre el tema a: <http://www.forbes.com/sites/andygreenberg/2014/02/13/silk-road-2-0-hacked-using-bitcoin--bug-all-its-funds-stolen/>

Aquest valor com a moneda d'us legal es reconegut per la mateixa jurisprudència que estableix que Bitcoin és una forma de diners:

“... Bitcoin és una forma electrònica de moneda sense recolzament per cap actiu real ni espècie, com ara monedes o metalls preciosos. Derek A. Dion, *I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-Cash*, 2013 U. Ill. J.L. Tech & Pol'y 165, 167 (2013). «No està regulat per un banc central o cap altra forma d'autoritat governamental; en canvi, l'oferta de Bitcoin es basa en un algorisme que estructura un sistema descentralitzat de transaccions punt a punt». *Id.* Bitcoin va ser dissenyat per reduir els costos de transacció, i permet als usuaris treballar junts per a validar les transaccions mitjançant la creació d'un registre públic de la cadena de custòdia de cada Bitcoin. *Id.* Bitcoin es pot utilitzar per a comprar articles en línia, i alguns establiments comercials han començat a acceptar Bitcoin a canvi de targetes de regal o altres compres. El valor de Bitcoin és volàtil i varia des de menys de \$2 per Bitcoin a més de \$260 per Bitcoin (Dkt. # 3 en 1)...”<sup>244</sup>.

Finalment, el jutge en la mateixa resolució estableix clarament que Bitcoin és una moneda o forma de diners. Naturalment, el propi sistema genera un entorn en el que es faciliten les activitats il·lícites i el rentat de diners procedents d'aquestes. Això fa que les forces de seguretat de tot el món tinguin en aquest sistema de pagament un interès especial. Així, podem seguir els arguments exposats per Preet Bharara, Fiscal

---

<sup>244</sup> Cas número 4:13-CV-416 del Tribunal del Districte de l'Est de Texas.

General del Districte sud de New York, en explicar al gener de 2014 les raons per les que anuncia la presentació de càrrecs contra traficants de drogues que utilitzaven Bitcoins com a moneda per les seves transaccions:

"... va planejar vendre més de \$1 milió en Bitcoins a criminals relacionats amb el tràfic de narcòtics al lloc de la web profunda dedicat al tràfic de drogues anomenat Silk Road. Es tracta de models de negoci veritablement innovadors que no necessiten recórrer a l'antiquada violació de la llei, però quan Bitcoins, com qualsevol moneda tradicional, són blanquejats i s'utilitzen per impulsar l'activitat criminal, la policia no té més remei que actuar. Posarem èmfasi en perseguir aquells que utilitzin les noves formes de moneda amb fins il·lícits..."<sup>245</sup>.

De les reticències que l'ús de Bitcoins genera en les diferents administracions, són un bon exemple intents com el del Govern de Califòrnia que va tractar de prohibir l'ús d'aquest sistema de pagament. Es va denunciar a la Fundació Bitcoin, una organització no lucrativa dedicada a estandarditzar i promoure l'ús d'aquesta moneda virtual, i se li va ordenar el 2013 cessar les seves operacions a Califòrnia, o enfrontar-se a fortes multes, que poden arribar inclús a penes de fins a cinc anys de presó. El Departament d'Institucions Financeres de Califòrnia, que supervisa els bancs, cooperatives de crèdit i altres entitats financeres que operen a l'estat, va acusar la fundació de

---

<sup>245</sup> Declaracions de 27 de gener de 2014 del Fiscal General Preet Bharara. Es pot consultar la demanda presentada a: <http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR/Faiella,%20Robert%20M.%20and%20Charlie%20Shrem%20Complaint.pdf>

"participar en el negoci de transferència de diners sense llicència o sense l'autorització corresponent"<sup>246</sup>. Similar postura van adoptar Illinois i altres estats.

Com diu Kashmir Hill, Bitcoin es coneix fonamentalment per ser una moneda virtual que dóna l'opció de jugar en línia, comprar medicaments i organitzar viatges, però no és per això que es va crear originalment. El seu misteriós creador, Satoshi Nakamoto, es va entusiasmar amb la possibilitat d'enviar diners a tot el món amb facilitat i sense comissions per operació, i per això ara, cinc anys després de la seva creació, s'ha demostrat un sistema capaç de fer operacions des d'una fracció d'un cèntim i fins a imports de milers de dòlars. (Kashmir Hill, 2014).

Bitcoin no és l'únic sistema de pagament virtual existent actualment, encara que si és el més conegut i el que més ràpidament s'ha estès per tot l'entorn virtual. DigiCash, NetCash i d'altres similars es basen en els mateixos principis. Però en tots els casos es va generant una jurisprudència basada en el fet de que la responsabilitat per l'ús d'aquestes monedes és independent de quin sigui l'origen o les característiques del sistema de pagament utilitzat.

No es definitori de la responsabilitat que hi hagi una entitat centralitzada que generi i controli el sistema monetari de que es tracti, o que aquest sigui generat per uns algorismes sense participació directa de les persones, la responsabilitat pel seu ús és sempre de les persones. Així

---

<sup>246</sup> Steven Musil en el seu article: "Bitcoin Foundation Ordered to Cease Operations in California" es refereix a l'escrit en el que el Departament d'Institucions Financeres de Califòrnia exigeix a la Fundació Bitcoin que deixi d'operar a tot l'Estat. Es pot consultar aquest escrit a <http://www.cnet.com/news/bitcoin-foundation-ordered-to-cess-operations-in-california/>

doncs, l'important no és qui genera, garanteix, o controla el mitjà de pagament utilitzat, sinó qui l'utilitza.



## Capítol vintè: Del núvol virtual a la web profunda

---

### Computació en núvol (*Cloud Computing*)

Es coneix com a computació en núvol, o *Cloud Computing*, una manera de compartir recursos que estan situats en diferents plataformes d'Internet. Es tracta d'un sistema que permet que un proveïdor de serveis pugui oferir els seus productes a través d'Internet, comptant amb una mínima infraestructura pròpia, mitjançant la contractació de diferents proveïdors externs per configurar el producte final que s'ofereix al client. La computació en núvol representa una major eficiència, especialment econòmica. Així, la mateixa Comissió Europea, en definir a la web de l'agenda digital per a Europa el terme computació en núvol, fa al·lusió directa a l'economia d'escala que la mateixa permet:

"... La computació en núvol és on les infraestructures de Tecnologies de la Informació, plataformes i programari són proporcionats de manera centralitzada i es distribueixen als usuaris finals a través d'una xarxa. La centralització en l'emmagatzematge i processament de dades ofereix economies d'escala que fins i tot les organitzacions més grans no poden aconseguir per si mateixes. [...] Empreses del sector privat que utilitzen la computació en núvol afirmen tenir entre un 10 i un

20% menys de costos de Tecnologies de la Informació..."<sup>247</sup>.

Aquestes plataformes diferents poden formar part de la pròpia infraestructura del proveïdor de serveis, el qual per tal de fer més ràpid i eficient el seu servei, pot optar per dividir els seus recursos en un núvol particular. No obstant això, el més usual és que s'utilitzi per proveïdors de serveis que subcontracten part dels recursos necessaris a d'altres proveïdors externs que ofereixen els seus serveis en núvol. També els particulars utilitzen serveis en núvol, per exemple per estalviar espai en el seu propi ordinador guardant els seus fitxers en bases de dades externes, utilitzar programes externalitzats sense tenir la necessitat de carregar-los en el seu propi sistema, o evitar l'adquisició de costoses infraestructures per realitzar determinades tasques.

El principal risc de la computació en núvol consisteix en el possible desconeixement per part de l'usuari de la procedència del material utilitzat. Els programes i altres elements que es poden trobar en núvol poden ser transparents o opacs. En el primer cas el servei prestat està identificat i és conegut el lloc en el qual està ubicat l'ordinador que conté les dades o el programa. En el segon cas aquesta informació no està accessible, cosa que el situa totalment fora del control de l'usuari.

Aquest desconeixement, en el cas del comerç electrònic, impedeix garantir el ple respecte als drets del client. Encara que en cas de conflicte que comporti acudir als tribunals la legislació aplicable és la del país en què resideix el consumidor, en la pràctica en desconèixer la ubicació del servei se li dificulta enormement l'exercici dels seus drets.

---

<sup>247</sup> About Cloud Computing. En Digital Agenda for Europe (European Commission) Pot consultar-se a: <https://ec.europa.eu/digital-agenda/node/1322>

Tot i que, tal com explica la mateixa Agència Espanyola de Protecció de Dades:

"... El proveïdor del servei pot trobar-se en, pràcticament, qualsevol lloc del món i el seu objectiu últim serà proporcionar els serveis esmentats optimitzant els seus propis recursos a través de, per exemple, pràctiques de deslocalització, compartició de recursos i mobilitat o realitzant subcontractacions addicionals..."<sup>248</sup>.

Els serveis de *Cloud Computing* que solen contractar són aquells relacionats amb la utilització de Programari dipositat en núvol, utilització d'infraestructures alienes, o utilització de plataformes, eines de gestió i bases de dades alienes.

## La responsabilitat en la computació en núvol

El caràcter internacional i diversificat dels serveis oferts en núvol, fa complexa la definició de responsabilitats. De fet, en emmagatzemar les pròpies dades en bases de dades externes, es cedeix a la pràctica la responsabilitat pel manteniment, guarda i control d'aquestes dades en mans del proveïdor del servei. Aquesta és una de les principals crítiques al *Cloud Computing*, doncs l'usuari en la pràctica queda captiu del proveïdor del servei responsable de la gestió de les seves informacions.

---

<sup>248</sup> Pàgina 5 de la "Guia per a clients que contractin serveis de *Cloud Computing*" editada per l'Agència Espanyola de Protecció de Dades. Madrid (2013) Es pot consultar aquest document a: [http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Orientaciones\\_Cloud\\_Computing.epub](http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Orientaciones_Cloud_Computing.epub)

El responsable del tractament de les dades personals, però, és sempre el client que contracta serveis de *cloud computing*.

Acudint al *Cloud Computing*, una empresa de comerç electrònic podria oferir els seus serveis gairebé sense disposar d'infraestructura pròpia. De fet, el *Cloud Computing* permet una gran disponibilitat d'informació, programes, i serveis gairebé sense suports físics per part de l'usuari, el qual utilitza recursos externs situats en núvol. Donada l'accessibilitat i la flexibilitat del sistema, s'utilitzen només aquells recursos que es requereixen, el que agilitza els processos i permet economitjar costos. Però encara que contracti externalitzadament la pràctica totalitat dels seus serveis en núvol, des de la publicitat, la cistella de la compra, la logística, o la gestió financera, la responsabilitat pel tractament de les dades personals dels seus clients, seguirà sent seva. Tal com recorda l'Agència Espanyola de Protecció de Dades:

"... El client que contracta serveis de *cloud computing* continua sent responsable del tractament de les dades personals. Encara que els contracti amb una gran companyia multinacional la responsabilitat no es desplaça al prestador del servei, ni tan sols incorporant una clàusula en el contracte amb aquesta finalitat..."<sup>249</sup>.

D'altra banda, la Unió Europea també s'ha referit a les qüestions jurídiques que la computació en núvol presenta. El Grup de Treball de

---

<sup>249</sup> Agència Espanyola de Protecció de Dades. "Guia per a clients que contractin serveis de Cloud Computing" Agpd.es, Madrid (2013) Es pot consultar aquest document en el lloc de l'AEPD: [http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Orientaciones\\_Cloud\\_Computing.epub](http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Orientaciones_Cloud_Computing.epub)

protecció de dades de l'article 29<sup>250</sup> va elaborar un Dictamen, sobre la computació en núvol, adoptat l'1 de juliol de 2012. En aquest Dictamen s'analitzen els aspectes que afecten els proveïdors de serveis de computació en núvol que operen a l'Espai Econòmic Europeu i els seus clients, especialment en tot el que fa referència a la protecció de dades.

En aquest Dictamen, després de reconèixer les múltiples avantatges que la computació en núvol presenta per als usuaris, s'adverteix sobre els riscos que aquesta comporta. El Dictamen comença recordant que en utilitzar els serveis presents en núvol, s'acudeix a múltiples proveïdors de les diferents operacions, el que multiplica el nombre d'encarregats del tractament de les dades i amb això els riscos.

En el cas que es tracti d'una administració pública la que utilitzi els serveis de computació en núvol per externalitzar part de la seva gestió, les responsabilitats s'han d'atribuir, en tot cas, a la pròpia administració, tal com defensen Alamillo i Urios:

"... cal tenir present que, per molt ben definida que estigui l'estructura de resposta davant de les incidències, errors o negligències del prestador del servei, les administracions públiques tenen assumida una responsabilitat de caràcter objectiu, davant dels perjudicis que puguin patir els ciutadans quan es relacionen amb aquelles. Per aquesta raó, per molt ben desenvolupats o regulats que estiguin aquests extrems, la responsabilitat primera davant del ciutadà serà sempre la de la

---

<sup>250</sup> Aquest Grup de treball va ser creat per l'article 29 de la Directiva 95/46/CE. Es tracta d'un òrgan europeu consultiu en matèria de protecció de dades i privacitat. Les seves funcions es descriuen en l'article 30 de la Directiva 95/46/CE i en l'article 15 de la Directiva 2002/58/CE.

corresponent administració pública, la qual no pot al·legar qüestions de caire organitzatiu o intern per exonerar-se de les responsabilitats del que, en última instància, ha estat una actuació administrativa..." (Alamillo i Urios 2012).

## **De l'anonimat a la web profunda**

La permanent tensió entre els qui defensen la necessitat de potenciar l'anonimat a la xarxa i aquells que el consideren un risc excessiu, fa que sorgeixin intents d'avançar en un i l'altre sentit. Casos com els de WikiLeaks, o el de May First/People Link no són els únics intents de permetre un cert anonimat dels seus usuaris. En realitat l'evolució i complexitat de l'entorn virtual, fa que a la pràctica s'estan qüestionant constantment conceptes com privacitat o anonimat. És cada vegada més difícil delimitar clarament els responsables directes o indirectes de les diferents accions que amenacen d'alguna manera la privacitat en l'entorn virtual, així com els seus col·laboradors necessaris.

De fet existeixen eines de comunicació dissenyades expressament per facilitar l'anonimat de qui les utilitza. Algunes, com Riseup Networks, es defineix en la seva presentació com una manera de crear alternatives democràtiques:

"... Riseup Networks ofereix eines de comunicació en línia per a les persones i grups que treballen en el canvi social alliberador. Som un projecte per crear alternatives democràtiques i practicar l'autodeterminació mitjançant el control dels nostres propis

mitjans segurs de comunicació..."<sup>251</sup>.

Altres, com European Counter Network, ofereixen un espai on publicar anònimament textos i articles alternatius, comunicacions anònimes, o entre altres coses, publicar vídeos anònimament mitjançant la plataforma New Global Visió (NGV)<sup>252</sup>.

Altres iniciatives no estructurades en organitzacions concretes, també tenen com a finalitat la protecció de l'anonimat en les seves activitats. Un exemple d'això podria ser Anonymous, que s'organitza de manera difusa a la xarxa, el que facilita l'anonimat des del qual s'organitzen operacions individuals o concertades a través de diferents canals online.

Podem veure també com es multipliquen els repetidors anònims (*remailers* anònims) com Mixmaster, o Cypherpunk, utilitzats per enviar correus electrònics de forma anònima. Hi ha per descomptat portals, o fins i tot xarxes dissenyades expressament per garantir l'anonimat de la navegació per internet. L'anonimat en principi no és il·lícit, sinó que en tot cas ho són les possibles activitats il·lícites que des d'aquest anonimat es poguessin realitzar. Fins i tot el Tribunal Suprem dels Estats Units ha dictaminat que l'anonimat està protegit per la Primera Esmena a la Constitució Nord-americana:

"... La protecció del discurs anònim és vital en el discurs democràtic. Permetre als dissidents blindar les seves identitats permet l'expressió d'opinions crítiques per part de les minories. [...] L'anonimat és un escut enfront de la tirania de la majoria.

---

<sup>251</sup> Es poden veure els serveis ofertats per Riseup a: <https://www.riseup.net/>

<sup>252</sup> Poden consultar-se les activitats d'European Counter Network a: <http://www.ecn.org/> i les de New Global Visión a: <http://www.ngvision.org/>

[...] Per tant, exemplifica el propòsit que persegueix la Declaració de Drets i la Primera Esmena en particular: per protegir els individus impopulars de represàlies -i la supressió de les seves idees- a mans d'una societat intolerant..."<sup>253</sup>.

## La web profunda i els seus riscos

El que avui es coneix com la web profunda (*The Deep Web*), no és més que el conjunt de llocs web que per una o altra raó no apareixen indexades en els cercadors tradicionals. Alguns autors com Michael Bergman, sostenen que la web profunda representa de 400 a 500 vegades més llocs que el total de la web usualment consultada pels usuaris de la web tradicional o oberta (Bergman, 2001).

A la web profunda<sup>254</sup> podem trobar les més variades informacions, unes perfectament legals, però moltes d'altres qüestionables o directament il·legals i delictives. Així per exemple, la Hidden Wiki, és una enciclopèdia encriptada que no resulta accessible als navegadors tradicionals, però que conté tot tipus d'informació amagada al públic: arxius secrets, terrorisme, pedofília, manuals per fabricar artefactes explosius, delinqüència organitzada, sicaris, drogues, *hackers* i multitud d'informacions similars els continguts de les quals són considerats il·legals en la majoria de països.

---

<sup>253</sup> Resolució en el cas *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995) del Tribunal Suprem dels Estats Units.

<sup>254</sup> Utilitzem en aquest treball el terme web profunda com a sinònim de web fosca, encara que per a alguns autors els dos termes es refereixen a aspectes diferents d'una mateixa realitat.



Els defensors de la web profunda, com Ian Clarke, creador de Freenet<sup>255</sup>, addueixen que l'anonimat que proporciona és necessari per garantir la llibertat d'expressió, especialment en països amb alts nivells de cibercensura.

Alguns navegadors, com Torch Browser, estan dissenyats per permetre navegar per la web profunda, però un dels més coneguts sistemes de navegació, dissenyat específicament per a la web profunda, és la xarxa Tor<sup>256</sup>. Aquesta xarxa dificulta que es pugui descobrir la destinació o l'origen d'una connexió d'internet. Tor consisteix en una sèrie de retransmissors administrats per voluntaris, que mantenen connexions permanentment entre si per formar una xarxa. Els clients Tor retransmeten els seus fluxos d'informació cap a o des d'Internet a través d'aquesta xarxa i així aconseguen l'anonimat de la seva navegació. Es tracta d'una xarxa virtual que té com a objectiu la privacitat i la seguretat de l'anonimat a internet. Funciona enviant les seves dades a través de tres servidors aleatoris dins de la xarxa Tor, abans que aquestes dades siguin enviades cap a internet.

Atès que en tots aquests casos, l'objectiu últim és el de resistir la censura i donar suport a la privacitat i l'anonimat, la delimitació d'un nivell de responsabilitat a les diferents persones que d'alguna manera faciliten un fet punible, o fins i tot la simple identificació d'aquells que hi participen, es fa difús i complex.

---

<sup>255</sup> Pot consultar-se a: <https://freenetproject.org/fairshare.html?language=en>

<sup>256</sup> La xarxa TOR (*The Onion Router*) resol adreces de la web a les quals no es pot accedir normalment des dels navegadors usals. Pot consultar el seu funcionament a: <https://www.torproject.org/>

Així, la detenció el 2013 del creador de la pàgina de la web profunda Silk Road i tres dels seus col·laboradors, així com del vicepresident de la Fundació Bitcoin, acusats de mantenir una xarxa il·legal de venda de drogues i de blanqueig de diners, són un bon exemple de la complexitat de l'entramat presumptament delictiu que facilita la web profunda. Després de ser detingut el creador del lloc Silk Road, van ocupar el seu espai altres webs com Pandora, o Agora. A més a més, va sorgir immediatament un nou lloc anomenat DarkList que el va substituir, tractant de convertir-se en un directori per a tots els venedors clandestins de droga al creixent mercat de la web profunda<sup>257</sup>.

Un altre cas sobre les activitats delictives a la web profunda, és el de Freedom Hosting Network, una plataforma que l'FBI nord-americà vincula amb la distribució de pornografia infantil. Mentre es decideix l'extradició o no als Estats Units de l'acusat, resident a Irlanda, la Xarxa TOR va publicar un avís desmarcant-se del cas i insistint en la legitimitat de l'anonimat, que no té perquè estar vinculat necessàriament a activitats delictives. "Qualsevol pot executar serveis ocults, i molts ho fan. Les organitzacions poden utilitzar els serveis ocults per protegir els dissidents, i activistes, i per protegir l'anonimat dels usuaris que tracten de trobar ajuda per a la prevenció del suïcidi, la violència domèstica , i els abusos". En el mateix comunicat TOR es refereix a la necessitat de l'anonimat per part de periodistes i altres professionals per intercanviar informació i protegir a les seves fonts.

---

<sup>257</sup> Greenberg, Andy. "Winklevoss-Funded Bitcoin Startup's CEO Arrested In Silk Road Investigation" Forbes. (24 de gener de 2014) Interessant article sobre el cas publicat a la revista Forbes, en el que es plantejant les contradiccions d'aquest cas. Pot consultar-se a: <http://www.forbes.com/sites/andygreenberg/2014/01/24/darklist-aims-to-be-the-yelp-of-silk-road-style-drug-dealers/>

## **Com a conclusió: La responsabilitat no és delegable**

---

### **Tecnologia, valors i procediments**

L'evolució de la tecnologia permet albirar canvis socials encara més importants que els produïts fins ara. Això comporta que la concepció de valors com el dret a la intimitat, la protecció de dades personals, o la llibertat d'informació, es vegi fortament condicionada per avanços tecnològics que generen una nova realitat. Es tracta de béns jurídics protegits enfrontats a noves realitats que qüestionen la pròpia eficàcia dels sistemes tradicionals de protecció. No obstant això, la progressió de la intel·ligència artificial comportarà nombrosos canvis específics, que de fet ja s'estan produint.

A l'aprofundir en els avenços tecnològics sorgeixen preguntes a les que cal anar donant resposta a mida que es vagin fent realitat. Així per exemple, és plausible que en el futur sigui factible adquirir una nevera dotada d'intel·ligència artificial i capaç d'avaluar, mitjançant codis de barres i altres tipus de sensors, l'absència de productes d'acord a les pautes alimentàries detectades i transmetre la demanda d'aquests productes al sistema automatitzat del comerç més pròxim. Aquest senzill tràmit, ja possible tecnològicament en l'actualitat, implica la transmissió habitual al comerç de dades que permeten conèixer informacions considerades d'indole privada, com pautes d'alimentació de

la família, nombre de membres, presència de convidats, dates assenyalades, solvència econòmica, influència de la publicitat, al·lèrgies i altres situacions sanitàries ...

Un altre exemple encara més gràfic podria ser el dels sistemes informàtics infectats per un troià situat no ja en el Sistema, si no en el propi nucli operatiu de la màquina. Programes que permeten el control remot de l'ordinador per qui tingui les claus apropiades, capaços de mantenir encesa la *WebCam* sense que l'usuari ho noti. Programes com LogMeIn o com MioControlPc Espia permeten el control remot d'ordinadors per qui tingui les claus apropiades.

## **Intel·ligència Artificial i comerç electrònic**

Les tecnologies basades en intel·ligència artificial s'utilitzen en els més variats aparells d'ús quotidià. Aplicades al comerç electrònic podem trobar-les en pràcticament totes les seves fases, des de l'anàlisi de mercat, fins al lliurament final del producte i el seu abonament corresponent. Els algorismes més sofisticats permeten una automatització creixent de les diferents activitats relacionades amb aquest comerç electrònic. Així, per exemple, els servidors actuals són capaços d'aprendre sobre els gustos i necessitats de l'usuari i en base a això recomanar els productes de la botiga virtual més adequats al seu perfil o a les seves demandes, així com personalitzar la publicitat que se li presenti al visitar un lloc web determinat.

Per intuir com influiran aquests canvis en el futur des d'una perspectiva legal i jurisprudencial en el concepte de responsabilitat en les diferents

facetes d'aquest comerç, el principal repte consisteix a conèixer el tipus de canvis que es produiran i el seu abast. El dubte és saber si aquests canvis produiran profundes modificacions en els valors i els paradigmes socials actuals i, per tant en el comerç electrònic tal com avui es concep, i en el seu marc de protecció legal i jurisprudencial, o només implicaran la necessitat d'adaptació de procediments i garanties.

D'aquesta creixent utilització de dispositius dotats de programes d'intel·ligència artificial, es desprèn la necessitat de definir clarament qui és el responsable en cas d'un mal funcionament del sistema o de danys causats pel mateix durant la seva execució. El concepte de responsabilitat està relacionat amb pautes religioses, culturals i socials, pel que és variable en funció de l'entorn concret en què s'apliqui.

En totes les sentències consultades es repeteix una i altra vegada la consideració que el responsable pels danys causats per algun animal o per algun objecte inanimat o alguna cosa inimputable, correspon sempre a qui tingui el deure de custòdia, control o supervisió. Ni tan sols és possible adduir l'absència personal de culpa per no estar present al lloc dels fets, tal com ha expressat el mateix Tribunal Suprem. Per al legislador, i per la jurisprudència actual, el desistiment en el deure de custòdia, control o supervisió per part de qui tingui aquesta obligació és un comportament típicament antijurídic.

Però en un tema tan complex i canviant com és la intel·ligència artificial aplicada cada vegada més als diferents sistemes utilitzats en el comerç electrònic, la pròpia definició de qui és l'encarregat de la seva custòdia, control, o supervisió ha d'estar ben definida. En el cas dels vehicles autònoms, capaços de circular per les vies públiques sense conductor, el

legislador atribueix la responsabilitat a la persona que posa en marxa el vehicle. Quan es tracta de vehicles aeris, els coneguts com drones, actualment només es comercialitzen per a ús civil els teledirigits, és a dir amb un pilot responsable capaç d'assumir el control del vehicle en qualsevol moment. Però en el cas dels drones militars, que plantegen la possibilitat de posar en l'aire màquines capaces de prendre decisions per si mateixes, fins i tot letals, tots els treballs i recomanacions oficials consultades insten al desenvolupament normatiu de la definició que l'ésser humà s'ha de considerar responsable.

## **La responsabilitat de les màquines intel·ligents**

En cap cas s'apunta la possibilitat que una màquina pugui tenir algun tipus de responsabilitat. Tampoc apareixen indicis d'una possible responsabilitat compartida amb la màquina, o que aquesta signifiqui algun tipus d'atenuant de la responsabilitat de les persones. Per als legisladors actuals, i per jutges i tribunals, a les màquines no se'ls pot atribuir responsabilitat ja que aquesta només és atribuïble a les persones.

Les màquines tampoc tenen drets que es consideren específics de les persones, com ara els drets d'autor per les obres que realitzen, ni són reus de difamació, invasió de la privacitat, o tractament inadequat de la informació personal. És evident que les màquines poden robar, lesionar, o fins i tot matar, però la responsabilitat, tant penal com de qualsevol altre tipus, només és atribuïble a les persones.

La hipòtesi des de la què es partia en aquest treball, és a dir, que "el desenvolupament de sistemes dotats d'intel·ligència artificial, o el que

podríem definir com a màquines intel·ligents, no modifica el paradigma de la responsabilitat com una cosa aplicable en exclusiva als éssers humans, en una activitat tan complexa com és en la pràctica el comerç electrònic" queda ratificada.

El que diferencia un ésser humà d'una màquina no és la memòria, la capacitat de càlcul, la presa de decisions, la manipulació d'objectes, la capacitat d'aprendre, o la interacció amb l'entorn, tot això realitzat avui mateix, o en un futur pròxim, de manera molt més eficient per les màquines que pels éssers humans. El que, al meu entendre, caracteritza la responsabilitat en l'ésser humà és l'existència d'un sistema de valors, la presa de decisions en funció d'aquests valors, la capacitat de preveure les conseqüències de les nostres accions, i la consciència de la nostra pròpia responsabilitat. És a dir la consciència del jo.

La consciència del jo, la pròpia autopercepció, la capacitat de valorar èticament les conseqüències de les accions, o de penedir-nos d'elles, és una cosa que ara com ara resulta difícilment reproduïble en les màquines i en general en els diferents sistemes dotats d'intel·ligència artificial existents en l'actualitat o que puguin existir en pròxim futur. Mentre les màquines no disposin d'aquests atributs, difícilment se'ls pot assignar cap responsabilitat.

De fet, perquè es pugui atribuir algun tipus de responsabilitat a les màquines per les accions que realitzen, primer cal que deixin de ser màquines. Si en el futur l'avanç de la ciència i de la biotecnologia ho aconsegueixen llavors haurem de canviar els nostres paradigmes sobre la responsabilitat.

Sentiments com l'amor, la ràbia, o la por són producte de processos químics que potser algun dia puguin ser generats en bioorganismes creats artificialment, però si aquests organismes arriben a resultar tan evolucionats com per tenir la seva pròpia consciència del jo, llavors sí que haurem de variar la nostra concepció de la responsabilitat, però en la pràctica, llavors també haurem de canviar la nostra concepció de les diferències entre les màquines i els éssers humans.

## **A tall de conclusió**

L'evolució dels sistemes intel·ligents està progressant de manera exponencial en els últims anys, i presumiblement aquesta tendència s'accelerará encara més en el futur. Aquest treball s'ha centrat especialment en l'anàlisi de les aplicacions de la intel·ligència artificial als més variats mecanismes automatitzats, i tot això en l'àmbit de les diferents fases que comporta el comerç electrònic. No obstant això, aquests processos s'estan produint en els camps més diversos i afecten, o afectaran en un pròxim futur, el nostre entorn més immediat i les nostres mateixes pautes de comportament, tant personal com social.

Així, no només veurem desenvolupar-se nous i més sofisticats robots d'aspecte humanoide; sistemes informàtics de velocitat i capacitat de processament inimaginables fa uns anys; o aplicacions capaços de realitzar les més variades tasques de manera més eficient que els propis éssers humans. També veurem electrodomèstics capaços d'interactuar amb l'entorn i realitzar accions de comunicació entre sistemes, màquina a màquina, directament i sense la intervenció directa de cap ésser humà.



Molts d'aquests dispositius ja estan avui mateix al mercat. Així, podem trobar peces de roba amb sensors incorporats capaços de detectar les nostres dades biològiques i enviar-les directament als centres d'anàlisi que de manera automàtica donen l'alarma quan aquests superen els límits establerts. Teixits que canvien de color segons el nostre estat d'ànim i que envien senyals a altres dispositius segons les necessitats detectades. Jaquetes d'autodefensa capaces de reaccionar automàticament i enviar fortes descàrregues elèctriques a qui estableixi contactes no desitjats. Sabates capaces de dirigir-nos mitjançant GPS a l'adreça desitjada, i infinitat d'altres dispositius capaços d'interactuar amb les persones, amb l'entorn, o amb altres dispositius.

Tanmateix, aplicant per analogia a aquests nous dispositius els criteris sobre responsabilitat que es desprenen de la jurisprudència i la legislació analitzada en aquest treball, podem avançar que, excepte canvis radicals impensables per ara, els dispositius intel·ligents seguiran sent per molt temps, a efectes de la seva responsabilitat, mers dispositius.

Les màquines, ara per ara, són doncs només màquines i, si alguna vegada prenem un camí equivocat, no podem esperar donar la culpa a les nostres sabates intel·ligents, per intel·ligents que aquestes siguin. La responsabilitat serà sempre nostra. La responsabilitat no és delegable, ni tan sols en unes sabates intel·ligents.

Barcelona, setembre de 2014



## Bibliografia

---

- Alamillo Domingo, Nacho i Urios Aparisi, Xavier (2012). “Aspectes Jurídics de la Prestació de Serveis Públics Emprant Computació al Cloud” Barcelona: Treballs de recerca 2011-2012. Escola d’Administració Pública de Catalunya i GRIS.
- Alcover, Guillermo i Alonso, Alberto (2000). “La firma electrónica” Pamplona: Ed. Aranzadi.
- Alvarado, L., Clavero, M., Illescas, R., Madrid, A. et al. (1998). “Comentario a los Principios de Unidroit para los Contratos del Comercio Internacional” Pamplona: Ed. Aranzadi.
- Aramayo, Roberto R. (2012). “Responsabilidad ética” Madrid: Eunomía. Revista en Cultura de la Legalidad. Nº 1 Septiembre 2011- Febrero 2012 Universidad Carlos III.
- Asaro, Peter (2013) “On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanisation of Lethal Decision-making”, Geneve: International Review of the Red Cross Nº 886. Extret de: <http://www.icrc.org/eng/resources/documents/article/review-2012/irrc-886-asaro.htm>
- Ballbé, Manuel (2009). “La importancia de los organismos reguladores nacionales ante la competencia global.” en La regulación de los

mercados telecomunicaciones, energía y valores. Madrid: Ministerio de Justicia.

Ballbé, Manuel (2007). “El futuro del derecho administrativo en la globalización: entre la americanización y la europeización.” Madrid: Revista de Administración Pública núm. 174

Bergman, Michael K. (2001). “White Paper: The Deep Web: Surfacing Hidden Value.” Michigan: The Journal of Electronic Publishing. Volume 7, Issue 1 Michigan University, (Aug./01)

Bok, Hilary (1998). “Freedom and Responsibility” Princeton NJ: Princeton University Press.

Burrieza, Alfredo (2013). “Decidability of a Logic Order of Magnitude Qualitative Reasoning with Comparability and Negligibility Relations” en Concha Bielza et al. (ed.) Advances in Artificial Intelligence. Lectures Notes in Computer Science. Madrid: Association for Artificial Intelligence.

Cañabate Pérez, Josep i Ramos Romeu, Francisco (2011). “Los datos digitales en el proceso civil: prevención, producción y autenticación” Barcelona: La Revista Jurídica de Catalunya núm. 1

Collobert, Ronan et al. (2011). “Natural Language Processing (Almost) from Scratch” en “Journal of Machine Learning Research” núm. 12 pp. 2493-2537 NEC Laboratories America. Princeton.

Coulouris, George; Dollimore, J.; Kindberg, T. i Blair, G., (2012). “Distributed Systems: Concepts and Design” Essex: Pearson Education Limited.

- 
- Deibert, Ronald J., Palfrey, John G., Rohozinski, Rafal i Zittrain, Jonathan (ed.) (2008). "Access Denied: The Practice and Policy of Global Internet Filtering" The MIT Press
- Descartes, R. "Discurso del método". Traducción de Arnau Gras, H.; ed. Alhambra, Madrid, 1987
- Díaz Bemejo, Guillermo (2012) "La resolución internacional de controversias en el comercio electrónico" E-Gov, 2012. Extret de <http://www.egov.ufsc.br/portal/conteudo/la-resolución-internacional-de-controversias-en-el-comercio-electrónico>
- Díaz Bermejo, Guillermo (2008). "La firma electrónica y los servicios de certificación" Altea: Portico Legal S.L. Extret de [http://www.porticolegal.com/pa\\_articulo.php?ref=311](http://www.porticolegal.com/pa_articulo.php?ref=311)
- Diéguez, Antonio (2001). "Milenarismo Tecnológico: La Competencia Entre Seres Humanos y Robots Inteligentes" Sevilla: Argumentos de Razón Técnica, Nº 4. Publicacions de la Universidad de Sevilla.
- Figueroa J.L. (2001). "Comercio Electrónico: Revolución o e-Volución." Monterrey: ITESM-Campus.
- Filangieri, Caetano (1836). "Ciencia de la Legislación". (Ilustrada con comentarios por Benjamin Constant) Paris: Tomo VI de la Tercera edició. Librería Española de Lecointe.
- Flores, María de la Sierra (2010). "Impacto del comercio electrónico en el Derecho de la contratación" Madrid: Cuadernos Mercantiles.
- Giménez-Salinas i Colomer, Eshter; García Solé, Marc i Román Maestre, Begoña (2003). "Sociedad abierta y delitos de odio en la era de la

globalización” Eguzkilore: Cuaderno del Instituto Vasco de Criminología, Núm. 17.

Gómez Ligüerre, Carlos (2005). “Solidaridad y responsabilidad: La responsabilidad conjunta en el derecho español de daños” Programa de Doctorat en Dret Patrimonial. Universitat Pompeu Fabra. Barcelona

Gonzales de Alaiza Cardona, Jose Javier (2004). “La lucha de los titulares de derechos de autor contra las redes “Peer to Peer” (2004) Revista de propiedad intelectual núm. 18 sep-dic

Hernández Orallo J; Ramirez Quintana, M. J; i Ferri Ramirez C. (2004). “Introducción a la minería de datos” Madrid: ed. Pearson.

Heyns, Christof (2013). “Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias” Informe A/HRC/23/47 presentat en el 23è període de sessions del Consell de Drets Humans de l’Assamblea General de les Nacions Unides.

Hill, Kashmir (2014). “Secret money: Living on Bitcoin in the real world” New York: ed. Forbes.

IBM Institute for Business Value i Said Business School de la Universidad de Oxford (2012). “Analytics Study: The RealWorld use of big data”

Kurose, James, F. i Ross, Keith W., (2013). “Computer Networking: A Top-Down Approach” Essex: Pearson Educational Limited.

Kurzweil, Ray (2005). “The singularity is near: When humans transcend biology” Berlin: Lola books.

- Lacruz Mantecón, Miguel L. (2006). "Copias privadas y calamidades públicas" en Carlos Rogel Vide, Abel Martín Villarejo en Anuario de Propiedad Intelectual 2005. Madrid: Editorial Reus
- Lastiri Santiago, Mónica (2013). "El tratamiento jurídico de las Keywords Advertising en la jurisprudencia del Tribunal de Justicia de la Unión Europea." Puebla: Rev. IUS vol. 7 núm. 31 (Enero/Junio)
- López Barja de Quiroga, Jacobo (1998). "Delitos contra la propiedad intelectual" Cuadernos de derecho judicial, Núm. 10.
- López Díaz, Elvira (2006). "Iniciación al derecho" Madrid: ed. Delta Publicaciones.
- Loredo, Alejandro (2006). "Derecho Comparado: Derecho de Autor y Copyright. Dos caminos que se encuentran" Mexico: Alfa-redi. Derecho y Nuevas Tecnologías. (Ag./06) Extret de <http://www.alfa-redi.org/node/9065>
- Marchant, Gary et al., (2011). "International governance of autonomous military robots" New York: Columbia Science and Technology Law Review, vol. XII
- Marquez Lobillo, P., (2007) "Prestadores de servicios de intermediación: Algunas especialidades de su estatuto jurídico" Revista de Contratación Electrónica. Núm. 88, Diciembre
- Martín Fernández, Manuel (1992) "Policía, profesión y organización: Hacia un modelo integral de Policía en España" Reis: Revista española de investigaciones sociológicas. Núm. 59

McCarthy, John et al., (1955). “A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence” Hanover, New Hampshire: Report of the Dartmouth Summer Project on Artificial Intelligence. Extret de <http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html>

Melchor y Lamanette, Federico (1877). “La penalidad en los pueblos antiguos y modernos” Madrid: Imprenta de la Revista de Legislación.

Mendoza Buergo, Blanca (2001). “El Derecho Penal en la Sociedad del Riesgo” Madrid: ed. Civitas.

Miguel Asensio, Pedro A. de (2011). “Derecho Privado de Internet (Estudios y Comentarios de Legislación)” Madrid: ed. Civitas/Thomson Reuters.

Miguel L. Lacruz Mantecón, (2006). “Copias privadas y calamidades públicas” en Carlos Rogel Vide, Abel Martín Villarejo en Anuario de Propiedad Intelectual 2005. Madrid: Editorial Reus, (pp. 449- 477)

Moles Plaza, Ramón J. (2004). “Derecho y control en Internet: la regulabilidad de Internet” Barcelona: Ariel Derecho

Moncada Flórez, Juan Pablo. (2009). “La responsabilidad de los prestadores de Servicios de Intermediación en la Sociedad de la Información” Tesis doctoral. Granada: Editorial de la Universidad de Granada.

Montesinos García, Ana (2008). “Mediación on line” Barcelona: Vlex. Revista de Contratación Electrónica Nº 94, Junio



- 
- Morales Plaza, Antonio; Pardo Gonzalez, Miguel i Rodrigo Lavilla, Jesus (2010). "Tratado del sector publico estatal" Madrid: Ed. La Ley-Actualidad S.L.
- Morales Plaza, Antonio (2009). "La regulacion nuclear globalizada" Madrid: Ed. Wolters Kluwer.
- Moratalla Escudero, José Ramón (2013). "Las diez sentencias más reveladoras de 2013" Extret de [http://www.elderecho.com/actualidad/sentencias-reveladores\\_0\\_623625032.html](http://www.elderecho.com/actualidad/sentencias-reveladores_0_623625032.html).
- Moravec, H. (1988). "Mind Children, The future of robots and human intelligence" Cambridge, Mass.: Harvard University Press.
- Moravec, H. (2000). "El apogeo de los Robots" Barcelona: Investigación y Ciencia (edició espanyola de Scientific American). Nº 280. Gener.
- Mundó Blanch, Jordi (2003). "Fundamentos psicológicos de la socialidad y la cultura humanas, y la importancia para su caracterización en otras especies" México: Ludus vitalis: revista de filosofía de las ciencias de la vida. Núm. 19
- Mundó Blanch, Jordi (2000). "Ética, identitat i ciència social normativa" Barcelona: Publicacions i Edicions de la Universitat de Barcelona
- Nichols, Shaun (2008). "Free Will versus the Programmed Brain" New York: Scientific American. Mind Matters. Agosto/2008. Extret de <http://www.scientificamerican.com/article/free-will-vs-programmed-brain/>
- Paniagua Aris, E; Sanchez Gonzalez, J.L; Martin Rubio, F. (2003). "Lógica Computacional" Madrid: Ed. Paraninfo.

Perez Bes, Francisco (2008). "El Derecho de autor y las nuevas tecnologías" Barcelona: Editorial La Ley.

Pifarré, Maria Jose (2013). "Internet y redes sociales: Un nuevo contexto para el delito". Revista d'Internet, Dret i Política N° 16 (Universitat Oberta de Catalunya) Barcelona

Posada Prieto, Fernando et al., (2012). "Multimedia y web 2.0" Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (Febrer)

Puget, Jean François (2013). "Big Data For Dummies" New York: IBM corporation/developerWorks. (IT Best Kept Secret Is Optimization) Extret de: [https://www.ibm.com/developerworks/community/blogs/jfp/entry/big\\_data\\_for\\_dummies23?lang=en](https://www.ibm.com/developerworks/community/blogs/jfp/entry/big_data_for_dummies23?lang=en)

Ramos, Andy. (2014). "Caso Svensson: Un Enlace de Internet constituye un acto de comunicación pública (cuando se dirige a un público nuevo)" Interiuris.com

Reporters Without Borders (2014). "Enemies of the Internet" Extret de: [http://12mars.rsf.org/wp-content/uploads/EN\\_RAPPORT\\_INTERNET\\_BD.pdf](http://12mars.rsf.org/wp-content/uploads/EN_RAPPORT_INTERNET_BD.pdf)

Resing, W. i Drenth, P. (2007). "Intelligence: knowing and measuring" Amsterdam: Ed. Nieuwezijds.

Ribes, Xavier (2007). "La Web 2.0. El valor de los metadatos y de la inteligencia colectiva" Telos. Cuadernos de Comunicación, Tecnología y Sociedad. N° 73, (Fundación Telefónica, Diciembre)

- 
- Richard, C. (2014). "Internet Censorship Around the Globe" London: WholsHostingThis? (Febrer) Extret de: <http://www.whoishostingthis.com/blog/2014/02/20/internet-censorship/>
- Richards, Neil M. i Smart, William D. (2013). "How should the law think about robots?" New York: Social Science Research Network. Extret de: <http://ssrn.com/abstract=2263363>
- Roca Trias, Encarna (2009). "El riesgo como criterio de imputación subjetiva del daño en la jurisprudencia del Tribunal Supremo español" Barcelona: InDret, Revista para el análisis del Derecho Núm. 4/09 (Octubre)
- Rodríguez Ardura, Inma (2002). "Marketing.com y comercio electrónico en la sociedad de la información" Madrid: Ed. Piramide SA.
- Rodríguez, Rodolfo J. (1996). "Modelos cognoscitivos para la filosofía contemporánea de la mente" Revista de Filosofía de la Universidad de Costa Rica, Vol. XXXIV (83-84), pag. 423-432. Extret de: [http://inif.ucr.ac.cr/recursos/docs/Revista de Filosofía UCR/Vol. XXXIV/No. 83-84/modelos cognoscitivos para la filosofia contemporanea de la mente.pdf](http://inif.ucr.ac.cr/recursos/docs/Revista%20de%20Filosofia%20UCR/Vol.%20XXXIV/No.%2083-84/modelos%20cognoscitivos%20para%20la%20filosofia%20contemporanea%20de%20la%20mente.pdf)
- Roselló Mallol, Víctor (2009). "Marketing y Protección de Datos" Cap. III Noticias Jurídicas Setembre.
- Russell, Stuart i Norvig, Peter (2009). "Artificial Intelligence: A Modern Approach" Edinburgh: Pearson Education Limited. (3a. ed.)

Saunders, K. M., (2002). "Confusion is the Key: a Trademark Law Analysis of Keyword Banner Advertising" New York: Fordham Law Review núm. 71. Ed. Fordham University School of Law.

Simon, Herbert A. (1995). "Explaining the ineffable: AI on the topics of intuition, insight and inspiration". Montreal: Actes de la decimocuarta conferència internacional conjunta en Intel·ligència Artificial, Vol. 1, 939-948.

Simon, Herbert A. (1995). "Artificial intelligence: an empirical science". Amsterdam: Elsevier Science B.V. Extret de: <http://www.ic.unicamp.br/~wainer/cursos/2s2006/epistemico/simon-ia.pdf>

Soler Jiménez, Joan (2013) "Big Data, l'anarxiu i l'evolució dels arxius històrics" Diplomàtica.cat. Extret de: <http://diplomaticapuntcat.blogspot.com.es/2013/04/big-data-lanarxiu-i-levelucio-dels.html>

Steven Musil en article: "Bitcoin Foundation ordenado tono Cease Operations in California"

Teran Perez, D. M., (2012). "Introducción a la computación cuantica para ingenieros" Barcelona: ed. Alfaomega Grupo editorial.

Touriño, Alejandro (2010). "Régimen de responsabilidad de los prestadores de servicios de la sociedad de la información" Barcelona: Diario Jurídico.com [www.diariojuridico.com/regimen-de-responsabilidad-de-los-prestadores-de-servicios-de-la-sociedad-de-la-informacion](http://www.diariojuridico.com/regimen-de-responsabilidad-de-los-prestadores-de-servicios-de-la-sociedad-de-la-informacion)

- Turing, Alan (1950). "Computing Machinery and intelligence" Oxford: Mind núm. 49, pp. 433-460 Oxford University Press.
- Velasco Núñez, Eloy (2010). "Delitos cometidos a través de Internet. Cuestiones procesales" Madrid: ed "La Ley" grupo Wolters Kluwer.
- Velasco Núñez, Eloy (2006). "Aspectos procesales de la investigación i de la defensa en los delitos informáticos" Diario La Ley núm. 6506 del divendres 16 de juny.
- Wunsch-Vincent, Sacha (2013). "The economics of copyright and the internet: Moving to an empirical assessment relevant in the digital era" WIPO Economic Research Working Papers n° 09. Cambridge University Press.
- Wunsch-Vincent, Sacha (2006). "The WTO, the Internet and Trade in Digital Products: EC-US Perspectives" Portland: Hart Publishing, Oxford and Portland, Oregon.
- Xalabarder, Raquel (2006). "La responsabilidad de los prestadores de servicios en Internet (ISP) por infracciones de propiedad intelectual cometidas por sus usuarios" IDP. Revista de Internet, Derecho y Política. N.º 2. UOC



## Legislació

---

Compendi dels Estats Units, de 19 d'agost de 2014, de pràctiques de l'oficina de drets d'autor.

Ordre IET/1090/2014, de 16 de juny, per la qual es regulen les condicions relatives a la qualitat de servei en la prestació dels serveis de comunicacions electròniques.

Llei 9/2014, de 9 de maig, general de telecomunicacions.

Decret 55/2014, de 22 d'abril, pel qual s'estableix el currículum del cicle formatiu de grau superior de programació de la producció en fabricació mecànica.

Resolució 2014/2567 (RSP) del Parlament Europeu, de 27 de febrer de 2014, sobre l'ús de drones armats.

Directiva 2014/26/UE del Parlament Europeu i del Consell, de 26 de febrer de 2014, relativa a la gestió col·lectiva dels drets d'autor i drets afins i a la concessió de llicències multiterritorials de drets sobre obres musicals per a la seva utilització en línia a el mercat interior.

Informe A/HRC/23/47, de 9 d'abril de 2013, del Relator Especial sobre les execucions extrajudicials, sumaris o arbitràries.

Codi dels Estats Units, de 2012.

Codi Administratiu de Nevada (NAC).

Dictamen 05/2012 del Grup de Protecció de Dades de l'Article 29, d'1 de juliol de 2012, sobre la computació en núvol.

Dictamen 04/2012 del Grup de Protecció de Dades de l'Article 29, de 7 de juny de 2012, sobre l'exempció del consentiment per a l'ús de cookies.

Reial decret llei 13/2012, de 30 de març, pel qual es transposen directives en matèria de mercats interiors d'electricitat i gas i en matèria de comunicacions electròniques, i pel qual s'adopten mesures per a la correcció de les desviacions per desajustaments entre els costos i ingressos dels sectors elèctric i gasista.

Reglament LCB Núm R084-1 del Departament de Vehicles de Motor de Nevada, d'1 de març de 2012, relatiu als vehicles autònoms.

Llei de reforma i modernització de la FAA dels Estats Units, d'1 de febrer de 2012.

Dictamen 16/2011 del Grup de Protecció de Dades de l'Article 29, de 8 de desembre de 2011, sobre la recomanació de millors pràctiques de EASA/IAB sobre publicitat compartamental en línia.

Reial Decret 1581/2011, de 4 de novembre, pel qual s'estableix el Títol de Tècnic Superior en Automatització i Robòtica Industrial i es fixen els seus ensenyaments mínims.

Projecte de Llei 511 de la Comissió de Transport de Nevada, de 6 de juny de 2011, sobre el transport; proporcionant certs privilegis al propietari o l'arrendatari a llarg termini d'un vehicle de combustible



alternatiu qualificat; autoritzant en aquest Estat el funcionament de, i anotació en la llicència de conduir per als operadors de, vehicles autònoms; proporcionant una sanció; i altres assumptes relacionats.

Reial Decret 726/2011, de 20 de maig, pel qual es modifica el Reglament sobre les condicions per a la prestació de serveis de comunicacions electròniques, el servei universal i la protecció dels usuaris, aprovat pel Reial Decret 424/2005, de 15 d'abril.

Le Llei 22/2010, de 20 de juliol, del Codi de consum de Catalunya.

Dictamen 2/2010 del Grup de Protecció de Dades de l'Article 29, de 22 de juny de 2010, sobre publicitat comportamental en línia.

Llei Orgànica 5/2010, de 22 de juny, per la qual es modifica la Llei Orgànica 10/1995, de 23 de novembre, del Codi Penal.

Llei 29/2009, de 30 de desembre, per la qual es modifica el règim legal de la competència deslleial i de la publicitat per a la millora de la protecció dels consumidors i usuaris.

Directiva 2009/140/CE del Parlament Europeu i del Consell, de 25 de novembre de 2009, per la qual es modifiquen la Directiva 2002/21/CE relativa a un marc regulador comú de les xarxes i els serveis de comunicacions electròniques, la Directiva 2002/19/CE relativa a l'accés a les xarxes de comunicacions electròniques i recursos associats, i a la seva interconnexió, i la Directiva 2002/20/CE, relativa a l'autorització de xarxes i serveis de comunicacions electròniques.

Directiva 2009/136/CE del Parlament Europeu i del Consell, de 25 de novembre de 2009, per la qual es modifiquen la Directiva 2002/22/CE relativa al servei universal i els drets dels usuaris en relació amb les xarxes i els serveis de comunicacions electròniques, 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 i el Reglament (CE) núm 2006/2004 sobre la cooperació en matèria de protecció dels consumidors.

Reial Decret 899/2009, de 22 de maig, pel qual s'aprova la carta de drets de l'usuari dels serveis de comunicacions electròniques.

Directiva 2009/24/CE del Parlament Europeu i del Consell, de 23 d'abril de 2009, sobre la protecció jurídica de programes d'ordinador.

Reglament (CE) núm 207/2009 del Consell, de 26 de febrer de 2009, sobre la marca comunitària.

Directiva 2008/95/CE del Parlament Europeu i del Consell, de 22 d'octubre de 2008, relativa a l'aproximació de les legislacions dels Estats membres en matèria de marques.

Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

Reial Decret 1687/2007, de 14 de desembre, pel qual s'estableix el títol de Tècnic Superior en Programació de la Producció en Fabricació Mecànica i es fixen els seus ensenyaments mínims.

Reial Decret Legislatiu 1/2007, de 16 de novembre, pel qual s'aprova el text refós de la Llei General per a la Defensa dels Consumidors i Usuaris i altres lleis complementàries.

Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.

Llei 44/2006, de 29 de desembre, de millora de la protecció dels consumidors i usuaris.

Directiva 2006/116/CE del Parlament Europeu i del Consell, de 12 de desembre de 2006, relativa al termini de protecció del dret d'autor i de determinats drets afins.

Directiva 2006/115/CE del Parlament Europeu i del Consell, de 12 de desembre de 2006, sobre drets de lloguer i préstec i altres drets afins als drets d'autor en l'àmbit de la propietat intel·lectual.

Directiva 2006/24/CE del Parlament Europeu i del Consell, de 15 de març de 2006, sobre la conservació de dades generades o tractats en relació amb la prestació de serveis de comunicacions electròniques d'accés públic o de xarxes públiques de comunicacions i per la qual es modifica la Directiva 2002/58/CE.

Reial Decret 225/2006, de 24 de febrer, pel qual es regula determinats aspectes de les vendes a distància i la inscripció en el registre d'empreses de vendes a distància.

Reial Decret 1553/2005, de 23 de desembre, pel qual es regula l'expedició del document nacional d'identitat i els seus certificats de signatura electrònica.

Reial Decret 424/2005, de 15 d'abril, pel qual s'aprova el Reglament sobre les condicions per a la prestació de serveis de comunicacions electròniques, el servei universal i la protecció dels usuaris.

Directiva 2004/48/CE del Parlament Europeu i del Consell, de 29 d'abril de 2004, relativa al respecte dels drets de propietat intel·lectual.

Llei 59/2003, de 19 de desembre, de signatura electrònica.

Llei 21/2003, de 3 de novembre, general de telecomunicacions.

Llei 39/2002, de 28 d'octubre, de transposició a l'ordenament jurídic espanyol de diverses directives comunitàries en matèria de protecció dels interessos dels consumidors i usuaris.

Directiva 2002/77/CE de la Comissió, de 16 de setembre de 2002, relativa a la competència en els mercats de xarxes i serveis de comunicacions electròniques.

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 (Directiva sobre la privacitat i les comunicacions electròniques).

Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

Decisió Núm 676/2002/CE del Parlament Europeu i del Consell, de 7 de març de 2002, sobre un marc regulador de la política de l'espectre radioelèctric a la Comunitat Europea (Decisió espectre radioelèctric).

Directiva 2002/22/CE del Parlament Europeu i del Consell, de 7 de març de 2002, relativa al servei universal i els drets dels usuaris en relació amb les xarxes i els serveis de comunicacions electròniques (Directiva servei universal).

Directiva 2002/21/CE del Parlament Europeu i del Consell, de 7 de març de 2002, relativa a un marc regulador comú de les xarxes i els serveis de comunicacions electròniques (Directiva marc).

Directiva 2002/20/CE del Parlament Europeu i del Consell, de 7 de març de 2002, relativa a l'autorització de xarxes i serveis de comunicacions electròniques (Directiva autorització).

Directiva 2002/19/CE del Parlament Europeu i del Consell, de 7 de març de 2002, relativa a l'accés a les xarxes de comunicacions electròniques i recursos associats, i a la seva interconnexió (Directiva accés).

Directiva 2001/84/CE del Parlament Europeu i del Consell, de 27 de setembre de 2001, relativa al dret de participació en benefici de l'autor d'una obra d'art original.

Directiva 2001/29/CE del Parlament Europeu i del Consell, de 22 de maig de 2001, relativa a l'harmonització de determinats aspectes dels drets d'autor i drets afins als drets d'autor en la societat de la informació.

Directiva 2000/31/CE del Parlament Europeu i del Consell, de 8 de juny de 2000, relativa a determinats aspectes jurídics dels serveis de la societat de la informació, en particular el comerç electrònic en el mercat interior (Directiva sobre el comerç electrònic).

Directiva 1999/93/CE del Parlament Europeu i del Consell, de 13 de desembre de 1999, per la qual s'estableix un marc comunitari per a la signatura electrònica.

Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

Directiva 98/84/CE del Parlament Europeu i del Consell, de 20 de novembre de 1998, relativa a la protecció jurídica dels serveis d'accés condicional o basats en aquest accés.

Directiva 97/55/CE del Parlament Europeu i del Consell, de 6 d'octubre de 1997, per la qual es modifica la

Directiva 84/450/CEE sobre publicitat enganyosa, a fi d'incloure-hi la publicitat comparativa.

Reial Decret Legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de Propietat Intel·lectual, regularitzant, aclarint i harmonitzant les disposicions legals vigents sobre la matèria.

Directiva 96/9/CE del Parlament Europeu i del Consell, d'11 de març de 1996, sobre la protecció jurídica de les bases de dades.

Llei 7/1996, de 15 de gener, d'ordenació del comerç minorista.

Llei de Decència en les Telecomunicacions d'Estats Units, de 1996.

Llei Orgànica 10/1995, de 23 de novembre, del Codi Penal.

Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades.

Reglament (CE) núm 40/94 del Consell, de 20 de desembre de 1993, sobre la marca comunitària.

Acord de l'Organització Mundial del Comerç, de 15 d'abril de 1994, sobre els Aspectes dels Drets de Propietat Intel·lectual relacionats amb el Comerç (Acord ADPIC).

Directiva 93/83/CEE del Consell, de 27 de setembre de 1993, sobre coordinació de determinades disposicions relatives als drets d'autor i drets afins als drets d'autor en l'àmbit de la radiodifusió via satèl·lit i de la distribució per cable.

Directiva 93/13/CEE del Consell, de 5 d'abril de 1993, sobre les clàusules abusives en els contractes celebrats amb consumidors.

Llei Orgànica 5/1992, de 29 d'octubre, de regulació del tractament automatitzat de les Dades de Caràcter Personal.

Primera Directiva 89/104/CEE del Consell, de 21 de desembre de 1988, relativa a l'aproximació de les legislacions dels estats membres en matèria de marques.

Llei 34/1988, d'11 de novembre, general de publicitat.

Conveni Núm 108 del Consell d'Europa, de 28 de gener de 1981, per a la protecció de les persones respecte al tractament automatitzat de dades de caràcter personal.

Constitució Espanyola, de 1978.

Llei de Drets d'Autor 17 USC §§ 101 i següents, de 19 d'octubre de 1976.

Pacte Internacional de Drets Econòmics, Socials i Culturals, adoptat i obert a la signatura, ratificació i adhesió per l'Assemblea General en la seva resolució 2200 A (XXI), de 16 desembre 1966.

Reglament Federal d'Aviació dels Estats Units, de 30 setembre de 1963.

Declaració Universal dels Drets Humans (DUDH) adoptat per l'Assemblea General de les Nacions Unides en la seva Resolució 217 A (III), el 10 de desembre de 1948.

Reial Decret, de 24 de juliol de 1889, text de l'edició del Codi Civil manada publicar en compliment de la Llei de 26 de maig últim.

Conveni de Berna per a la Protecció de les Obres Literàries i Artístiques, de 9 de setembre de 1886.

Codi Civil dels francesos, aprovat per la Llei del 21 març 1804.

Carta de Drets dels Estats Units, de 15 desembre 1791.

Constitució dels Estats Units d'Amèrica, de 1787.



## Jurisprudència i altres resolucions

---

Sentència del Tribunal de Justícia de la Unió Europea (Gran Sala), de 8 d'abril de 2014, en els assumptes acumulats C-293/12 i C-594/12.

Sentència 103/2014, de l'Audiència Provincial de Madrid, de 31 març 2014.

Cas Michael P. Horta, administrador de l'Administració Federal d'Aviació dels Estats Units, v. Raphael Pirker, de 6 març de 2014.

Sentència del Tribunal de Justícia de la Unió Europea (Sala Quarta), de 13 de febrer de 2014, en l'assumpte C-466/12.

Resolució R/00936/2014 de l'Agència Espanyola de Protecció de Dades.

Resolució R/02892/2013 de l'Agència Espanyola de Protecció de Dades.

Cas Securites and Exchange Commission v. Trendon T. Shavers and Bitcoin Saving and Trust, núm. 4: 13-CV-416 del Tribunal del Districte de l'Est de Texas, de 6 agost 2013.

Sentència 3644/2013, de la Sala del Contenciós-Administratiu de l'Audiència Nacional, de 23 juliol 2013.

Sentència del Tribunal Constitucional 17/2013, de 31 gener 2013.

Solució de diferències de l'Organització Mundial del Comerç: diferència DS285, Estats Units - Mesures que afecten el subministrament

transfronterer de serveis de jocs d'atzar i apostes, de 28 de gener de 2013.

Acte CIV-2012-404-1928 [2012] NZHC 1494, l'Alt Tribunal de Nova Zelanda, de 6 de desembre del 2012.

Sentència Núm 832, de 12 de juliol de 2012, de la Cort Suprema de França.

Casos K-Beech, Inc, CV 11-3995 (DRH) (GRB); Malibu Media, LLC, CV 12-1147 (JS) (GRB); Malibu Mitjana LLC, CV 12-1150 (LDW) (GRB) i Patrick Collins, Inc, CV 12-1154 (ADS) (GRB) del Tribunal del Districte Est de Nova York, d'1 de maig del 2012.

Sentència del Tribunal Constitucional 173/2011, de 7 de novembre del 2011.

Sentència del Tribunal de Justícia de la Unió Europea (Sala Primera), de 22 de setembre de 2011, en l'assumpte C-323/09.

Sentència del Tribunal de Justícia de la Unió Europea (Gran Sala), de 12 de juliol de 2011, en l'assumpte C-324/09.

Acte 6623/2011, de la Sala Civil del Tribunal Suprem, de 31 de maig de 2011.

Sentència 72/2011, de la Sala Civil del Tribunal Suprem, de 10 de febrer del 2011.

Sentència del Tribunal de Justícia de la Unió Europea (Gran Sala), de 7 de desembre de 2010, en els assumptes acumulats C-585/08 i C-144/09.

Sentència 630/2010, de l'Audiència Provincial de València, de 26 d'octubre del 2010.

Sentència del Tribunal de Justícia de la Unió Europea (Sala Primera), de 8 de juliol de 2010, en l'assumpte C-558/08.

Cas Arista Records LLC v. Lime Group LLC, 715 F. Supp. 2d 481 del Tribunal del Districte del Sud de Nova York, de 25 de maig del 2010.

Sentència 316/2010, de la Sala Civil del Tribunal Suprem, de 18 de maig del 2010.

Sentència del Tribunal de Justícia de la Unió Europea (Gran Sala), de 23 de març de 2010, en els assumptes acumulats C-236/08 a C-238/08.

Solució de diferències de l'Organització Mundial del Comerç: diferència DS362, Xina - Mesures que afecten a la protecció i observança dels drets de propietat intel·lectual, de 19 de març de 2010.

Sentència 558/2010, de la Sala del Social del Tribunal Suprem, de 20 de gener del 2010.

Sentència 773/2009, de la Sala Civil del Tribunal Suprem, de 9 de desembre del 2009.

Sentència 3338/2008, de la Sala del Contenciós-Administratiu de l'Audiència Nacional, de 17 de setembre del 2008.

Sentència 512/2008, de la Sala Penal del Tribunal Suprem, de 17 de juliol de 2008.

Sentència 156/2008, de la Sala Penal del Tribunal Suprem, de 8 d'abril de 2008.

Sentència del Tribunal de Justícia de la Unió Europea (Gran Sala), de 29 de gener de 2008, en l'assumpte C-275/06.

Sentència 416/2007, de la Sala Penal del Tribunal Suprem, de 23 de maig del 2007.

Sentència 61/2007, de la Sala del Contenciós-Administratiu de l'Audiència Nacional, de 12 de gener del 2007.

Sentència 403/2007, de l'Audiència Provincial de València, de 29 de juny del 2007.

Sentència del Tribunal de Justícia de la Unió Europea (Sala Tercera), de 7 de desembre de 2006, en l'assumpte C-306/05.

Sentència 2/2006, de la Sala del Contenciós-Administratiu de l'Audiència Nacional, de 18 de maig del 2006.

Sentència 517/2005, de l'Audiència Provincial de Madrid, de 21 de novembre del 2005.

Cas Metro-Goldwyn-Mayer Studios, Inc, et al. v. Grokster, Ltd, et al. 545 US 913 de la Cort Suprema dels Estats Units, de 27 de juny del 2005.

Sentència 4362/2005, de la Sala del Contenciós-Administratiu de l'Audiència Nacional, de 12 de gener del 2007.

Sentència 876/2001, de la Sala Penal del Tribunal Suprem, de 19 de maig del 2001.

Cas A & M Records, Inc v. Napster, Inc 239 F. 3d 1004 de la Cort d'Apel·lació dels Estats Units, de 12 de febrer del 2001.

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

Sentència 162/2000, de la Sala del Social del Tribunal Superior de Justícia de Burgos, de 21 de març del 2000.

Sentència del Tribunal Constitucional 94/1998, de 4 maig 1998.

Sentència del Tribunal Constitucional 11/1998, de gener 13, 1998.

Cas Reno v. American Civil Liberties Union 521 US 844 de la Cort Suprema dels Estats Units, de 26 juny 1997.

Cas McIntyre v. Ohio Elections Commission 514 US 334 de la Cort Suprema dels Estats Units, d'abril 19, 1995.

Sentència del Tribunal Constitucional 254/1993, de 20 juliol 1993.

Cas Gershwin Publishing Corp v. Columbia Artists Management, Inc 443 F. 2d 1159 del Segon Circuit de Corts d'Apel·lació dels Estats Units, de maig 24, 1971.

Cas Shapiro P, Bernstein and Co v. H.L. Green Co 316 F. 2d 304 del Segon Circuit de Corts d'Apel·lació dels Estats Units, de 1963.

Sentència, de 13 de febrer de 1930, de la Cort Suprema de França.

Sentència, de 18 de juny de 1896, de la Cort Suprema de França.