IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monogràfic «III Congrés Internet, Dret i Política (IDP). Noves perspectives»

ARTICLE

Vers nous principis de protecció de dades en un nou entorn TIC

Yves Poullet
amb la col·laboració de Jean-Marc Dinant

Data de presentació: maig 2007
Data de acceptació: maig 2007
Data de publicació: setembre 2007

Resum

Davant de les noves transformacions d'Internet, entre les quals podem destacar la tendència a la connexió de xarxes fins ara autònomes i la multifuncionalitat dels equips terminals de telecomunicacions que converteixen els sistemes d'informació en omnipresents, cal establir nous principis per protegir adequadament el ciutadà.

Es proposen cinc nous principis. El d'encriptació i anonimat reversible, el de beneficis recíprocs de manera que la tecnologia també beneficiï els usuaris, el de potenciació de les solucions tecnològiques que afavoreixin o no vagin en contra de la privadesa –tal com estableix el Grup de l'art. 29–, el del complet control per part de l'usuari de l'equip terminal de manera que l'usuari estigui completament informat dels fluxos de dades, i el principi segons el qual els usuaris de determinats sistemes d'informació es beneficiïn de la legislació sobre defensa dels consumidors i usuaris.

És necessari, a més, que l'obligació de compliment de les normes de protecció de dades de caràcter personal es faci extensiva a d'altres subjectes que d'entrada no semblen involucrats en el tractament: els fabricants de programari i de terminals. Aquests tenen el deure d'informar l'usuari dels riscs que corren en utilitzar les xarxes i oferir accés a aplicacions i fabricar productes que garanteixin una major protecció de la privadesa.

Paraules clau

connexió de xarxes, nous principis de protecció de dades, responsabilitat, fabricants de programari, fabricants de terminals de telecomunicacions, informació a l'usuari

Tema

Protecció de dades

Towards new Data Protection Principles in a new ICT environment

Abstract

In view of the new transformations of the Internet, among which we can highlight the trend towards previously autonomous network connections and the multifunctionality of telecommunication terminals, which make information systems omnipotent, new principles must be established in order to provide adequate protection for citizens.

Five new principles are proposed: encryption and reversible anonymity; reciprocal benefits, whereby technology also benefits users; improvement of technological solutions that favour or do not work against privacy – as established by the Group from article 29; complete user control over the terminal, so that he or she is fully informed as to the data flow; and the principle whereby users of certain information systems benefit from legislation in defence of consumers and users.

Furthermore, the obligation to comply with personal data protection regulations must be extended to other subjects that do not initially appear to be involved in processing: namely, software and terminal manufacturers. These are obliged to inform users about any risks that they run when using networks, as well as provide access to applications and manufacture products that ensure greater protection of privacy.

Keywords

networking, new data protection principles, telecommunication terminal manufacturers, information for users

Topic

Data protection

Introducció: un nou entorn TIC

1. Internet i, de manera més àmplia, la propagació de les TIC en la nostra vida quotidiana (GPS, RFID, mòbils) han modificat radicalment l'entorn i han creat nous riscs per a la nostra privadesa considerada en un sentit ampli. En les dues últimes dècades s'ha vist una ràpida i increïble successió d'un gran nombre d'innovacions i tendències tecnològiques que han desembocat en la formació d'una xarxa de telecomunicacions global. Aquest desenvolupament tecnològic s'ha produït a escala internacional sense que cap govern o moviment cívic jugués un paper decisiu i sense que els problemes sobre una reducció en la privadesa que acompanyen aquestes xarxes s'hagin abordat o resolt des del punt de vista tècnic.

2. Les característiques d'aquest entorn es podrien resumir com segueix. També se suggereixen determinats objectius per a garantir una millor protecció dels ciutadans que s'estan tornant més i més *ciutadans de la xarxa*.[1]

La xarxa és **multifuncional** i tendeix a enllaçar totes les xarxes de telecomunicació que fins ara es mantenien autònomes. La capacitat de la infraestructura de comunicació creix i es diu que assolirà 10 kbps.

Respecte a **l'equipament terminal**, hi ha diverses evolucions. En primer lloc, l'equipament terminal, que als anys vuitanta era unifuncional (el terminal de telefonia de veu per a transmissió de senyals d'àudio, la televisió per a la transmissió unidireccional d'imatges, etc.), ara és **multifuncional**. Amb el meu portàtil puc enviar cor-

1. Per una descripció completa, vegeu Y. POULLET; J. M. DINANT (2004, novembre). *Self- determination in an Information Society, Report on the application of Data Protection Principles to the worldwide Telecommunications networks*. Informe para el Comité Asesor de la Convención para la protección de individuos con respecto a procesamiento automático de datos personales (T-PD). Estrasburg. Disponible en la pàgina web del Consell d'Europa. Aquest article és una versió d'aquest informe revisada curosament i resumida.

reus electrònics, veure la televisió, realitzar transaccions i llegir el meu diari. Un altre canvi en l'equipament terminal és que ja no està ancorat en un lloc fix, sinó que ens pot acompanyar en els nostres trasllats. D'altra banda, la seva capacitat s'incrementa de manera notable sota la famosa Llei de Moore. Segons aquesta teoria, cada divuit mesos, la capacitat d'un terminal es pot doblar pel mateix preu. En altres paraules, després de quinze anys, la capacitat de processament i memòria dels ordinadors s'ha multiplicat per mil. En concret, això significa que la compra d'un ordinador en un establiment ha tingut l'evolució següent:

Any	1987	2005	2020 (x1000)
Processador	8 MHz	3 GHz (x 375)	3 terahertz
Memòria	640 KB	512 MB (x 800)	512 GB
Disc dur	20 MB	120 GB (x 6000)	120 terabytes
Connexió telefònica	10 kbps	3 Mbps	10 GBps

Per finalitzar, també es destaca la tendència cap a la **miniaturització** dels terminals gràcies a l'ús de nanotecnologia. Els RFID (dispositius d'identificació per ràdio freqüència) són etiquetes o *tags* anomenades *pols intel· ligent*. Aquests tags es poden incrustar a les nostres robes, als productes que comprem en supermercats i, fins i tot, als nostres cervells, i poden detectar, controlar i, en última instància, influir en el nostre comportament.

Amb l'ús d'aquests diversos terminals, els sistemes informàtics són **omnipresents** ja que han envaït el nostre entorn i tots els segments de la vida quotidiana, tant privada com professional i, amb cada dia que passa, obriran camins cap a nous camps. Els sistemes d'informació multipliquen les empremtes dels usos dels serveis TIC i multipliquen la possibilitat que determinats controladors de dades facin un seguiment de les activitats dels usuaris d'Internet.

En el futur, moltes de les activitats que en el passat es duien a terme sense cap xarxa de telecomunicacions, necessitaran aquestes xarxes. No és absurd pensar que, en uns anys, la majoria de neveres estaran equipades amb components intel·ligents que informaran amb exactitud dels aliments que tenen emmagatzemats i de la seva data de caducitat (gràcies als xips RFID). Aquestes «neveres intel·ligents», fins i tot, podran prendre la iniciativa de mostrar en el televisor familiar anuncis dirigits o de contactar amb els supermercats per obtenir ofertes o realitzar comandes de productes. En general, hi ha una clara tendència que consisteix a crear objectes intel·ligents al nostre entorn equipant-los amb un terminal de telecomunicacions. Els terminals intel·ligents estan operant de manera **opaca i complexa**.

3. En l'actualitat, els ordinadors conformen la immensa majoria de terminals de telecomunicació. En basar-se en ordinadors, aquests terminals generen, de manera completament invisible per als usuaris, moltes empremtes de les telecomunicacions que passen per ells. Aquestes empremtes s'emmagatzemen en el terminal o bé s'envien per la xarxa, habitualment sense informar l'usuari. Els mitjans tècnics posats a disposició dels usuaris són incomplets, massa complexos i configurats per defecte en un mode perjudicial per a la protecció de la privadesa dels navegants d'Internet. El respecte a la privadesa s'ha convertit en una opció accessible a persones que disposen de temps i coneixements. La relació de l'individu amb la protecció de les seves dades s'ha convertit, per si mateixa, en un article d'informació personal que molta gent vol tenir.

Els terminals de telecomunicació incorporen diversos identificadors tècnics que permeten «rastrejar» el comportament de l'individu en la xarxa. La majoria de participants de la indústria no consideren que aquest procés de rastreig sigui una violació de la privadesa de l'individu si aquest no pot ser identificat mitjançant un punt de contacte. La tecnologia de les galetes (*cookies*) permet que una pàgina web, per defecte, insereixi dissimuladament el propi identificador en el terminal de manera permanent per poder rastrejar, així, el comportament de l'individu en Internet.

4. Els protocols de telecomunicacions i el funcionament dels terminals no inclouen la protecció de dades com a requeriment clau, sinó com una opció generalment deixada a la discreció dels fabricants de dispositius i programes que incorporen aquests estàndards. **Determinades opinions expressades recentment pel Grup Article 29 han argumentat que el principi establert pel considerant 2 de la**

Directiva 95/46 UE sobre protecció de dades, que afirma clarament que la tecnologia ha de servir els individus i la societat es pot considerar una justificació per imposar als fabricants d'equipament terminal (incloent-hi elements de programes incorporats als terminals) determinades obligacions adreçades a la transparència del seu funcionament i a la prevenció de l'ús injust o il·lícit de dades personals associades a la connexió i la comunicació amb xarxes. S'ha de tenir en compte que aquests fabricants no estan coberts com a tals per aquesta directiva ja que no són els controladors d'un fitxer. Tanmateix, com el disseny de l'equipament que proveeixen autoritza moltes operacions de processament, se'ls hauria d'imposar determinades responsabilitats sobre seguretat per a prevenir aquestes operacions que podrien realitzar terceres parts de manera injusta o il·lícita, i haurien de ser exigibles per a garantir la transparència, ja que l'usuari del terminal ha de poder exercir un determinat control sobre els fluxos de dades generats pel seu ús.

5. Finalment, ressaltem el caràcter global d'Internet. A causa de la naturalesa global de les xarxes modernes i de l'absència de fronteres respecte a la infraestructura, el processament operat per persones localitzades fora de les fronteres nacionals pot afectar directament la nostra privadesa mitjançant la tramesa de programes espia (*spyware*), que transmeten dades a tercers per mitjà d'hiperenllaços invisibles o envien correu no sol·licitat per mitjà del web, etc. L'abolició de fronteres nacionals fa necessària una aproximació comuna als principis de protecció de dades i la seva possible imposició més enllà de les fronteres. El WSIS (World Summit on the Information Society) s'ha declarat a favor d'un reconeixement internacional de la protecció de la privadesa.

Alguns principis nous per a promoure l'autodeterminació de la informació en el nou entorn tecnològic

6. Tots aquests trets, que són els més característics de l'entorn del servei de comunicacions electròniques –presència creixent i multifuncionalitat de les xarxes i terminals de comunicació electrònica; la seva interactivitat; caràcter internacional de les xarxes, serveis i productors d'equipament; i absència de transparència en el funcionament de terminals i xarxes–, incrementen el risc d'infringir les llibertats individuals i la dignitat humana.

Per a contrarestar aquests riscs i perquè els interessats estiguin més ben protegits i controlin més el seu entorn, s'han d'establir alguns nous principis. El control esmentat és essencial si els usuaris exerceixen una responsabilitat efectiva per a la seva pròpia protecció i han d'estar millor preparats per a exercitar apropiadament l'autodeterminació de la informació.

Aquest és el primer intent d'esbós d'aquests principis. Es basa en una diversitat de documentació i hem intentat estructurar-lo entorn de cinc principis clau, ja que en aquest estadi preferim no parlar de nous «drets» per a l'interessat. El seu contingut i extensió hauria de ser discutit per altres interessats i, llavors, si és apropiat, podrien formar les bases per a recomanacions i altres mesures *ad hoc* per a dotar-los de més força.

a. Primer principi: El principi d'encriptació i anonimat reversible

7. L'encriptació de missatges ofereix protecció contra l'accés al contingut de les comunicacions. La qualitat varia en fer-ho les tècniques d'encriptació i desencriptació. Ara es troben disponibles, a preus raonables, programes d'encriptació per a ser instal·lats als ordinadors dels usuaris d'Internet (protocols S/MIME o Open PG). Mentrestant, atesa la seva ambigüitat, la noció d'*anonimat* potser hauria de ser aclarida i, possiblement, substituïda per altres termes com *pseudoanonimat* o *no-identificable*. El que es busca no sempre és l'anonimat absolut, sinó **la no-identificació funcional de l'autor d'un missatge enviat a altres persones**.[2] Hi ha molts documents no vinculants[3] que defensen el dret a l'anonimat dels ciutadans quan utilitzen serveis de nova tecnologia. La recomanació

2. Vegeu J. GRIJPINK; C. PRIENS (2001). «Digital Anonymity on the Internet, New Rules for Anonymous Electronic Transactions?». *Computer Law & Security Report*. Vol. 17, núm. 6, pàg. 379-389.
3. Vegeu en particular S. RODOTÀ. «Beyond the E.U. Directive: Directions for the Future». A: Y. POULLET; C. DE TERWANGNE; P. TURNER (ed.). «Privacy: New Risks and Opportunities». *Cahier du CRID*. Anvers: Kluwer. Núm. 13, pàg. 211 ff.

núm. R (99) 5[4] del Comitè de Ministres del Consell d'Europa estableix que «l'accés i ús anònim de serveis i mitjans anònims per a realitzar pagaments són les millors proteccions de la privadesa», de la qual cosa deriva la importància de les tècniques de potenciació de la privadesa ja disponibles en el mercat.

El primer principi referit a la no-identificació funcional es podria expressar de la manera següent: **els que usin tècniques modernes de comunicació han de poder romandre no identificats pels proveïdors de serveis, per unes altres terceres parts que intervinguessin durant la transmissió del missatge i pel receptor o receptors del missatge, i haurien de tenir accés gratuït o a preus raonables als mitjans per a exercir aquesta opció.**[5] **La disponibilitat d'encriptació econòmica, i eines i serveis per a mantenir l'anonimat és una condició necessària per a internautes que exerceixin la seva responsabilitat personal**.

Tanmateix, l'anonimat, o la no-identificació funcional, requerit no és absolut. El dret del ciutadà a l'anonimat ha de ser establert en oposició a interessos majors d'estat, el qual podria imposar restriccions si fossin necessàries «per a protegir la seguretat nacional, defensa, seguretat pública [i per a] la prevenció, investigació, detecció i persecució de delictes». Aconseguir un equilibri entre el monitoratge legítim de delictes i la protecció de dades hauria de ser possible mitjançant l'ús de «pseudoidentitats» que serien assignades a individus per proveïdors de serveis especialitzats, als quals es podria requerir revelar la identitat real d'un usuari però només en determinades circumstàncies i seguint procediments clarament establerts per la llei.

8. Es podrien extreure altres conseqüències d'aquest primer principi: podria incloure la regulació exigida d'equipaments terminals, per prevenir la monitorització de la navegació per permetre la creació d'adreces efímeres i per a la diferenciació de dades d'adreces segons quines terceres parts tinguessin accés a la dada de trànsit o localització, i per a la desaparició dels identificadors únics globals mitjançant la introducció de protocols d'adreces uniformes.

Finalment, l'estatus d'*anonimitzadors,* en què els que els utilitzen dipositen una gran confiança, hauria d'estar regulat per a oferir als afectats determinades barreres respecte a l'estàndard de servei que proporcionen, alhora que haurien de garantir que l'estat tingui els mitjans tècnics per a accedir a les telecomunicacions en circumstàncies legalment definides.[6]

b. Segon principi: El principi de beneficis recíprocs

9. On fos aplicable, aquest principi faria que els que emprin noves tecnologies tinguin l'obligació legal de dur a terme la seva activitat professional a fi d'acceptar determinats requeriments per a restablir l'equilibri tradicional entre les parts implicades. La justificació és simple: si la tecnologia incrementa la capacitat d'acumulació, processament i comunicació d'informació sobre tercers i facilita les transaccions i operacions administratives, és essencial que també es configuri i s'empri per a garantir que els interessats, tant si són ciutadans com consumidors, gaudeixin d'un benefici proporcional d'aquests avenços.

Diverses previsions recents s'han inspirat en el requeriment proporcional per a obligar els que empren tecnologies a posar-les a disposició dels usuaris perquè puguin fer valer els seus drets i interessos.

4. Es troben disponibles diverses recomanacions per a la protecció d'individus respecte a la recaptació i processament de dades personals en les autopistes de la informació en el lloc del Consell d'Europa. Vegeu també la Recomanació 3/97 de l'anomenat Grup de l'Article 29: Anonimat en Internet, i l'opinió de la comissió privada belga sobre comerç electrònic (núm. 34/2000 del 22 de novembre de 2000, disponible en el lloc de la comissió: http://www.privacy.fgov.be), que apunta que hi ha tres maneres d'identificar els remitents de missatges sense que necessàriament se'ls requereixi la identificació.
5. Vegeu la recomanació de la comissió de processament de dades nacionals franceses segons la qual l'accés a pàgines comercials hauria de ser sempre possible sense identificació prèvia: M. GEORGES (2000). «Relevons les défis de la protection des données à caractère personnel: l'Internet et la CNIL». *Commerce électronique- Marketing et vie privée*. París. Pàg.71 i 72.
6. Es podrien establir els requeriments per als serveis proporcionats i pel que fa a la confidencialitat, com es proposa per a les firmes digitals. L'aprovació oficial d'un *anonimitzador* indicaria que es compleixen els requeriments. Aquesta aprovació oficial podria ser més voluntària que obligatòria, com en el cas d'etiquetes de qualitat.

Un exemple és la directiva europea 2001/31/CE (la Directiva d'E-Comerç), que inclou previsions electròniques *antispamming*. De manera similar, l'article 5.3 de la Directiva 2002/58/CE sobre comunicacions privades i electròniques inclou, fins i tot, el requisit segons el qual «(...) l'ús de xarxes de comunicació electròniques a fi d'emmagatzemar informació o obtenir accés a la informació emmagatzemada en l'equipament terminal d'un subscriptor o usuari tan sols està permès sota la condició que al subscriptor o usuari implicat se li hagi proporcionat informació clara i comprensible (...) i se li ofereixi el dret a rebutjar l'esmentat processament (...)». El dret dels subscriptors, sota l'article 8.1 –«per mitjans simples, lliures de cap càrrec, eliminar la presentació d'identificació de línia telefònica en termes de trucada (...) i en termes de línia»–, és una altra aproximació potencialment valuosa si el concepte de *línia telefònica* s'amplia a diverses aplicacions d'Internet, com ara serveis web i correu electrònic.[7] Això implica una obligació relacionada del proveïdor de serveis envers els usuaris consistent a oferir-los les opcions de rebutjar o acceptar trucades no identificades o prevenir-ne la identificació (articles 8.2 i 8.3).

10. Les legislacions anomenades de *llibertat d'informació* introdueixen un dret similar de transparència respecte al govern mitjançant l'addició de més informació que aquest últim té l'obligació de subministrar. Un avenç ben rebut en el Regne Unit és la introducció recent d'una garantia de servei públic en el maneig de dades.[8] Recentment, una comissió sueca[9] ha recomanat una legislació que donaria drets als ciutadans per a monitorar els seus casos electrònicament des del principi fins al final, incloent-hi el seu fitxer, i obligaria les autoritats a adoptar una bona estructura d'accés pública, per facilitar als individus la identificació i localització de documents específics. Fins i tot hi ha un esborrany de legislació que faria possible, d'una manera o una altra, enllaçar qualsevol document oficial en què es basessin les decisions amb altres documents del cas. En altres paraules, un servei públic que s'ha tornat més eficient gràcies a les noves tecnologies ha de ser, també, més transparent i accessible per als ciutadans. El dret d'accés dels ciutadans s'estén més enllà dels documents que els concerneixen directament i inclou les normatives sobre les quals es va basar la decisió.

11. **Fins i tot és possible imaginar que determinats drets associats a la protecció de dades, com el dret a la informació, els drets d'accés i rectificació, i el dret a la reclamació, podrien ser de compliment obligat electrònicament. Es podrien proposar moltes aplicacions**:

- Hauria de ser possible aplicar el dret a la informació dels interessats en qualsevol moment amb un simple clic (o de manera més generalitzada mitjançant una acció electrònica i immediata) i oferir l'accés a la política de privadesa, que hauria de ser tan detallada i completa com permeti el menor cost de la propagació electrònica. El pas esmentat ha de ser anònim respecte al servidor de la pàgina, per a evitar així qualsevol risc de creació de fitxers sobre usuaris «preocupats per la privadesa». A més, en el cas de pàgines a què s'han atorgat etiquetes de qualitat, hauria de ser obligatori que proporcionessin un hiperenllaç des del símbol de l'etiqueta cap a l'organisme que li ha atorgat l'etiqueta. El mateix seria aplicable a la declaració del controlador del fitxer cap a l'autoritat supervisora. S'instal·laria un hiperenllaç entre una pàgina ineludible de qualsevol lloc web amb processament de dades personals i l'autoritat supervisora rellevant. Finalment, es podria fer atenció a la senyalització automàtica de qualsevol pàgina localitzada en un país que oferís una protecció inadequada.
- En el futur, els interessats haurien de poder exercir el dret d'accés emprant una signatura electrònica. Seria obligatori estructurar els fitxers perquè el dret d'accés fos d'aplicació fàcil. La informació addicional hauria d'estar sistemàticament disponible, com l'origen dels documents i una llista dels interessats a qui s'haurien subministrat determinades dades. Com s'ha esmentat

7. Fixeu-vos en la connexió entre aquestes previsions i el principi d'anonimat.
8. Garantia de servei públic en el maneig de dades: disponible ara per a la seva implementació a entitats públiques. D'aquesta manera, s'estableixen els drets de les persones sobre com es manipulen les seves dades personals i els estàndards que poden esperar que les organitzacions públiques subscriguin. http://www.dca.gov.uk/foi/sharing/psguarantees/data.htm#2
9. P. SEIPEL (2004). «Information System Quality as a Legal Concern». A: U. GASSER (ed.). *Information Quality Regulation: Foundations, Perspectives and Applications*. Nomos Verlagsgesellschaft. Pàg. 248. Vegeu també l'informe de la comissió sueca de P. SEIPEL (2002). *Law and Information Technology: Swedish Views*. Swedish Government Official Reports, SOU. Pàg. 112.

anteriorment,[10] de manera incremental, les dades personals acumulades per un gran nombre de públic i de xarxes privades no es guarden amb un o més propòsits clarament definits, sinó que s'emmagatzemen en la xarxa per a usos posteriors que només emergeixen segons sorgeixen noves oportunitats de processament o necessitats no identificades prèviament. En aquestes circumstàncies, els interessats han de poder tenir accés a la documentació que descriuen els corrents de dades en la xarxa, les dades concernents i els diversos usuaris –un tipus de registre de dades.[11]

- Hauria de ser possible exercir en línia els drets de rectificació i impugnació davant d'una autoritat amb un estatus clarament definit responsable de mantenir o considerar una llista de queixes.
- El dret a la reclamació s'hauria de beneficiar també de la possibilitat de derivació en línia, intercanvi de sol·licituds de les parts i altres documentacions, decisions i proposicions de mediació.
- Finalment, quan els individus interessats vulguin apel·lar les decisions preses automàticament o realitzar una notificació mitjançant una xarxa (com el rebuig d'atorgar un permís de construcció després d'un anomenat *procediment e-governamental*), haurien de tenir dret a la informació, pel mateix canal, sobre la lògica subjacent en la decisió. Per exemple, en el sector públic[12] els ciutadans haurien de tenir el dret a provar anònimament qualsevol paquet de presa de decisions o sistemes experts que poguessin utilitzar. Això es podria aplicar als programes per al càlcul automàtic d'impostos o drets a subsidis per a la rehabilitació d'habitatges.

c. Tercer principi: El principi del foment d'aproximacions tecnològiques compatibles amb la situació de persones protegides legalment o la seva millora

12. Recomanació 1/99 de l'anomenat Grup de l'Article 29 (grup de treball sobre protecció de dades de la UE),[13] que es preocupa de l'amenaça a la privadesa que representen els programes i maquinària de comunicacions en Internet, estableix el principi segons el qual la indústria de productes de programes i maquinària hauria de proporcionar les eines necessàries per a acatar les normes europees de protecció de dades. Segons aquest tercer principi, s'haurien d'atorgar diversos privilegis als reguladors. Aquesta conclusió s'ha deduït del considerant 2 de la Directiva 95/46 sobre protecció de dades que preveu que els sistemes d'informació i els productes han d'estar al servei de la societat i dels individus.

Per exemple, els reguladors haurien de poder intervenir en resposta a desenvolupaments tecnològics que presentin riscs importants. L'anomenat ***principi de precaució***, que es troba ben establert en les lleis ambientals, també es podria aplicar a la protecció de dades. El principi de precaució podria requerir que l'equipament terminal de telecomunicacions (incloent-hi els programes) adoptés els paràmetres més protectors com a opció per defecte per a garantir que els afectats no estiguin, per defecte, exposats als diversos riscs dels quals no tenen coneixement i que no poden avaluar.

De manera similar, segons el principi de beneficis recíprocs, és apropiat i gens irracional equipar els terminals de telecomunicacions amb *weblogs* (*blogs*), com és el cas de programes tipus servidor usats per compromisos en línia i per departaments governamentals. Això permetria que els usuaris controlessin quines persones han accedit al seu equip i, quan fos apropiat, identificar les característiques principals de la informació transferida.

13. Aquest principi es pot il·lustrar amb una provisió de la Directiva de la UE sobre privadesa i comunicacions electròniques. L'article 14 estableix que on es requereixi, la Comissió pot adoptar mesures que garanteixin que l'equip terminal és compatible amb les normes de protecció de dades. En altres paraules, l'estandardització d'equipament terminal és una altra manera, certa-

10. Vegeu el paràgraf 3.
11. Aquesta idea és l'origen de dues lleis belgues recents que requereixen l'establiment de comitès sectorials per a les xarxes enllaçades amb el Registre Nacional (Acta del 8 d'agost de 1983, que estableix un registre nacional de persones, segons les esmenes de l'Acta del 35 de març de 2003, MB. 28 de març de 2003, article 12§1) i amb l'autoritat de registre comercial (Banque Carrefour des Entreprises) (Acta de 16 de gener de 2003 que estableix l'autoritat, MB. 5 de febrer 2003, article 19 §4).
12. S'aplica el mateix principi als prenedors privats de decisions, subjectes als interessos legítims dels controladors de fitxer (especialment relacionat amb la confidencialitat d'empreses, que podria limitar l'obligació d'aclarir la lògica subjacent).
13. Grup de l'Art. 29. Recomanació sobre el processament invisible i automàtic de dades personals per Internet portat a terme mitjançant programes o maquinària.

ment subsidiària, de protecció de dades personals dels riscs de processament il·legal –riscs que han estat creats per totes aquestes opcions de nova tecnologia. Anant més lluny, és necessari prohibir les anomenades *tecnologies per a acabar amb la privadesa*,[14] segons el principi de seguretat consagrat en l'article 7 del Conveni 108 del Consell d'Europa. L'obligació d'introduir mesures tècniques i organitzatives apropiades per contrarestar les amenaces a la privadesa de dades requerirà que els administradors de llocs s'assegurin que l'intercanvi de missatges romangui confidencial, i que també s'indiqui clarament quines dades s'estan transmetent, bé de manera automàtica o per hiperenllaç, com és el cas de companyies de cibermercadotècnia.

Aquesta obligació de seguretat també requerirà que els que processen dades personals optin per la tecnologia més apropiada per a minimitzar o reduir l'amenaça a la privadesa. Aquest requisit té una clara influència sobre el disseny de targetes intel·ligents, en particular sobre targetes multifuncionals,[15] com les targetes d'identificació. Un altre exemple de l'aplicació d'aquest principi afecta l'estructura de fitxers mèdics a diversos nivells, com recomana el Consell d'Europa.

14. **Es podria anar més lluny recomanant, tal com ha fet recentment el Comitè de la UE (2 de maig de 2007), el desenvolupament de tecnologies que potenciïn la privadesa, referint-se a eines o a sistemes que posin més èmfasi en els drets dels interessats**. Per descomptat, el desenvolupament d'aquestes tecnologies dependrà del lliure comportament del mercat, però l'estat ha d'adoptar una actitud activa per potenciar productes que siguin compatibles amb la privadesa i que la compleixin, oferint subsidis d'investigació i desenvolupament, establint certificacions voluntàries i sistemes d'acreditació equivalents, fent publicitat de les seves etiquetes de qualitat i garantint que els productes que es considerin necessaris per a la protecció de dades estiguin disponibles a preus raonables.

d. Quart principi: El principi segons el qual l'usuari ha de mantenir un control ple sobre l' equipament terminal

15. La justificació per a aquest principi és òbvia. Atès que aquests terminals poden permetre que d'altres monitorin les nostres accions i comportament, o simplement ens localitzin, han de funcionar de manera transparent i sota el nostre control. L'article 5.3 de la Directiva 2002/58/EC, esmentat anteriorment, ofereix una primera il·lustració sobre aquest punt. Els interessats han de ser informats sobre qualsevol accés remot als seus terminals mitjançant galetes (*cookies*), programes espia (*spyware*) o altres mitjans, i han de tenir la possibilitat de prendre mesures fàcils, efectives i lliures de qualsevol càrrec. La Directiva 2002/58/EC també estableix la norma segons la qual els usuaris de línies connectades i emissores de trucades puguin prevenir la presentació de la identificació de línia emissora de trucades.

Més enllà dels exemples anteriors, podríem argumentar que **tot equip terminal s'hauria de configurar de manera que garanteixi que els propietaris i usuaris tenen informació completa sobre qualsevol corrent de dades entrants o sortints perquè puguin realitzar les accions que considerin apropiades**. De manera similar, com ja és el cas sota determinada legislació, la possessió d'una targeta intel·ligent hauria d'incloure la possibilitat d'accedir a la lectura de les dades emmagatzemades en la targeta.

16. El control exercit per l'usuari també significa que els individus poden decidir desactivar els seus terminals definitivament i en qualsevol moment. Això adquireix importància respecte als identificadors per radiofreqüència (RFID). Els interessats han de tenir la possibilitat de confiar en tercers[16] que garanteixin que els mitjans tècnics d'identificació remota esmentats han estat completament desactivats.

14. Expressió utilitzada per J. M. DINANT en «Law and Technology Convergence in the Data Protection Field?». A: I. WALDEN; J. HORNE (2002). *E-commerce Law and Practice in Europe*. Cambridge: Woodhead Publishers. Cap. 8.2.
15. Sobre dissenys de targetes multiaplicació que satisfan la privadesa, vegeu E. KEULEERS; J.M. DINANT (2004). «Data protection: multi-application smart cards. The use of global unique identifiers for cross-profiling purposes». Part 2: «Towards a privacy enhancing smart card engineering». A: Computer Law and Security Report. Oxford: Elsevier. Vol. 20, núm 1, pàg. 22-28.
16. Certament, es refereix a acords d'acreditació com els ja descrits en el paràgraf 15 (regulació conjunta) o l'emissió, per part de les autoritats, d'autoritzacions per a realitzar determinades accions (regulació pública).

Els usuaris bé podrien aplicar aquest principi a empreses que no es troben necessàriament cobertes per les normes de protecció de dades, ja que no són responsables del processament de dades. Alguns exemples inclouen subministradors d'equip terminal i moltes formes de programes de navegació que es poden incorporar als terminals per facilitar la recepció, el processament i la transmissió de comunicacions electròniques.

Aquest principi també s'aplica a organismes d'ordenació estàndard públics i privats preocupats per la configuració del material i equipament esmentats.

17. El punt clau rau en el fet que els productes subministrats als usuaris no haurien d'estar configurats de tal manera que terceres parts o els fabricants els poguessin utilitzar per a propòsits il·lícits. Es pot il·lustrar amb diversos exemples:

- Una comparació dels navegadors disponibles en el mercat mostra que el diàleg que intercanvien ultrapassa en gran manera el que seria estrictament necessari per a establir la comunicació.[17]
- Entre els navegadors hi ha una gran diversitat en la manera de rebre, eliminar i prevenir la tramesa de galetes, la qual cosa implica que les oportunitats de processament inapropiat també variaran d'un navegador a l'altre. Tanmateix, sembla ser impossible, almenys de manera simple, que, en el navegador instal·lat per defecte en la majoria dels cents de milions d'ordinadors personals, bloquegi les finestres emergents o la comunicació sistemàtica de referències a articles llegits en línia o a paraules clau introduïdes en els motors de cerca.
- També s'ha de parar atenció a l'ús que fan els subministradors d'eines de navegació i programes de comunicació sobre identificadors únics i programes espia.

18. **En general, l'equipament terminal hauria de funcionar de manera transparent perquè els usuaris mantinguessin un control complet sobre les dades enviades i rebudes. Per exemple, hauria de ser possible establir, sense complicacions, l'extensió precisa del diàleg en els seus ordinadors, quins fitxers s'han rebut, els seus propòsits i qui els ha enviat o rebut. Des d'aquest punt de vista, els blogs semblem ser una eina apropiada que és relativament fàcil d'introduir**.

19. A més del dret de l'usuari a ser informat sobre els corrents de dades entrants, hi ha la qüestió de si les persones tenen el dret de requerir a tercers l'obtenció d'autorització per penetrar en la seva «llar virtual». En aquest punt és rellevant el Conveni del Consell d'Europa sobre cibercrim, en particular els articles 2 (accés il·legal)[18] i 3 (intercepció il·legal).[19] En aquest cas, la identificació de les persones que tenen part activa en les comunicacions no és una precondició per a l'aplicació del Conveni. De manera similar, l'accés no autoritzat a un sistema informàtic no està limitat a la pirateria de grans sistemes operats per bancs o departaments governamentals, sinó també a accessos no autoritzats a terminals de telecomunicacions, els quals estan representats en la situació tecnològica actual pels ordinadors.[20]

En altres paraules, mantenim que situar un número d'identificació en un terminal de telecomunicacions, o

17. Vegeu Jean-Marc DINANT (hivern 2001). «Le visiteur visité». *Lex Electronica*. Vol. 6, núm. 2.
18. Article 2 – Accés il·legal:
Cada part adoptarà les mesures necessàries, bé legals o d'una altra naturalesa, perquè en la llei local quedi establert com a ofensa criminal l'accés a qualsevol part o a la totalitat del sistema informàtic sense tenir-hi dret, quan s'hagués comès intencionalment. Una part podria requerir que l'ofensa es cometés mitjançant la infracció de mesures de seguretat, amb la intenció d'obtenir dades informàtiques o una altra intenció deshonesta, o en relació amb un sistema informàtic connectat a un altre sistema informàtic.
19. Article 3 – Intercepció il·legal: Cada part adoptarà les mesures necessàries, bé legals o d'una altra naturalesa, perquè en la llei local quedin establertes com a ofenses criminals, quan havent estat comeses de manera intencional, la intercepció sense dret, realitzada amb mitjans tècnics, de transmissions privades de dades informàtiques, des d'un sistema informàtic o en ell, que incloguin emissions electromagnètiques des d'un sistema informàtic transmissor de les esmentades dades informàtiques. Una part podria requerir que l'ofensa fos comesa amb intenció deshonesta, o en relació amb un sistema informàtic que estigués connectat a un altre sistema informàtic.
20. En aquest context, vegeu l'excel·lent article de Thierry LÉONARD. «E-commerce et protection des données à caractère personnel : Quelques considérations sur la licéité des pratiques nouvelles de marketing sur internet». A: http://www.droit.fundp.ac.be/Textes/Leonard1.pdf

accedir simplement a aquest número o un altre identificador de terminal, constitueix un accés no autoritzat. En aquest context legal, no hi pot haver cap dubte en l'avaluació de proporcionalitat de les accions esmentades. L'autorització és un acte positiu, bastant diferent de qualsevol acceptació que es pogués inferir del silenci o de no expressar objecció.

Per tant no es pot donar per assumit, com va fer DoubleClick,[21] que, pel mer fet de no activar el supressor de galetes, els usuaris hagin atorgat la seva autorització plena a la instal·lació d'aquest tipus d'informació en els seus terminals.

e. El principi segons el qual els usuaris de determinats sistemes d'informació s'haurien de beneficiar de la legislació de protecció al consumidor

20. **L'ús rutinari de tecnologies de la informació i comunicació, anteriorment confinat a activitats transcendentals, i el ràpid desenvolupament del comerç electrònic que ha multiplicat el nombre de serveis en línia han conduït a una aproximació més consumista de la privadesa**. Els navegants d'Internet veuen incrementades les transgressions a la seva privadesa –*spamming*, creació de perfils, polítiques de càrrecs diferenciats, rebuig d'accés a determinats serveis, etc.– com a consumidors d'aquests nous serveis.

D'aquesta manera, als Estats Units, els primers passos indecisos cap a la legislació de la protecció de dades en el sector privat es va enfocar cap a la protecció del consumidor en línia. Ja s'ha fet referència a la legislació californiana[22] però també hauríem de tenir en compte la Llei de privadesa del consumidor de 1995 i, més recentment, la declaració de 2000 de la Comissió de Comerç Federal,[23] que emfatitza la necessitat de legislació de privadesa per a la protecció dels consumidors en línia. A Europa i a Amèrica, les mesures per a combatre l'*spamming* es preocupen tant dels interessos econòmics dels consumidors com de les dades de privadesa dels subjectes.

21. **Aquesta convergència entre els interessos econòmics dels consumidors i les llibertats dels ciutadans obre perspectives interessants**. Suggereix que el dret a recórrer a determinades formes d'acció col·lectiva, que ja estan reconegudes en el camp de protecció al consumidor, s'hauria d'estendre a assumptes de privadesa. L'esmentat dret a «demandes col·lectives» és particularment rellevant en una àrea en la qual sovint és difícil avaluar el perjudici sofert pels interessats i en el qual el baix nivell de danys que es concedeix és un desànim per a les accions individuals.

A més, hi ha molts aspectes de la Llei del consumidor que es podrien aplicar eficaçment a la protecció de dades. Un exemple serien les obligacions de proporcionar informació i assessorament, que es podrien imposar als operadors que ofereixen serveis que impliquen essencialment la gestió i subministrament de dades personals, com ara els proveïdors d'accés a Internet i servidors de bases de dades personals (bases de dades de jurisprudència, motors de cerca i similars). Altres exemples serien la llei aplicable a les condicions generals de la contractació (aplicable a la política de privadesa), i mesures per a combatre pràctiques comercials i competència deslleial.

Per finalitzar, proporcionar dades personals com a condició d'accés a un lloc web o a un servei en línia es podria interpretar no solament des del punt de vista de la legislació de protecció de dades –el consentiment de l'usuari compleix els requisits necessaris? i, és suficient per a legalitzar el processament en qüestió?– sinó també de la legislació sobre defensa del consumidor, encara que només fos en termes de pràctiques injustes en l'obtenció de consentiment o d'obstacles importants sorgits del des-

21. A conseqüència de la demanda col·lectiva iniciada contra ells fa diversos anys als Estats Units, la pràctica actual de DoubleClick és enviar a tots els terminals no identificats una galeta inicial no residual i no identificadora anomenada *acceptar cookies*. Si la galeta és retornada, DoubleClick assumeix que el terminal accepta les galetes i envia una galeta identificadora que es manté durant uns deu anys (abans, trenta). Si no es retorna la galeta, DoubleClick enviarà indefinidament la galeta, que requerirà autorització. Hi ha disponible una opció d'exclusió que permet als usuaris informats emmagatzemar una galeta que té el significat de *no les accepta*.
22. Vegeu paràgraf 12.
23. Vegeu l'informe per al Congrés «privadesa en línia: pràctiques d'informació justes», del maig de 2000, disponible en el lloc FTC: http://www.ftc.gov/os/2000/05/index.htm. Als Estats Units, l'FTC, que és molt actiu en el camp de la protecció al consumidor, ha jugat un paper clau en la protecció de la privadesa dels ciutadans.

equilibri entre el valor de la seguretat de dades i el dels serveis subministrats.

Un altre camí a explorar és si la responsabilitat pel producte de terminals i programari pot fer-se extensiva més enllà de la causació d'un dany físic o econòmic per tal d'incloure la vulneració dels requeriments de protecció de dades. Fins a quin punt un subministrador d'un navegador l'ús del qual condueix a vulnerar la intimitat és responsable objectiu per la violació de la normativa sobre protecció de dades causada per un tercer?

Conclusions

22. La irrupció d'Internet ha creat la necessitat d'una tercera generació de regulacions sobre protecció de dades. No es tracta de girar l'esquena a les dues primeres generacions, sinó de proporcionar un nivell addicional de protecció, mantenint inalterades les mesures ja introduïdes. La primera generació es basava principalment en la naturalesa de les dades, en essència, en si eren sensibles i si afectaven el domini privat dels individus. L'autodeterminació informativa es va equiparar, llavors, amb la prohibició de processament d'aquestes dades, i es va englobar en l'article 8 de la Convenció Europea de Drets Humans. La segona generació s'ocupava no solament de la protecció de dades personals, sinó també de la manera en què el seu processament podria modificar l'equilibri de poder entre els processadors d'informació i els subjectes d'aquest processament. L'autodeterminació informativa es va estendre així per ajustar aquest equilibri mitjançant la garantia que l'esmentat processament romandria transparent i es restringiria el dret a processar dades sobre tercers. Aquest va ser l'origen de la Convenció núm. 108. Té molts emuladors i ha justificat la seva presència àmpliament.

23. **La tercera generació emergent, que esperem que s'adopti ben aviat, es caracteritza pel reconeixement de la tecnologia per si mateixa.** L'ús de les noves tecnologies multiplica la quantitat de dades i dels individus capaços d'accedir-hi, incrementa el poder dels que les recopilen i processen, i trenca fronteres. Un altre factor a tenir en compte és la complexitat i opacitat d'aquesta tecnologia. Un tercer implicat –el terminal o la xarxa– intervé ara entre l'individu i el controlador de dades. L'autodeterminació informativa reclama una mesura de control sobre aquest tercer implicat.

Com s'hauria d'exercir aquest control? Els suggeriments següents no són exhaustius en el tema:

- Segons Clarke,[24] «la resposta a la màquina rau en la màquina» amb relació als problemes que la societat de la informació planteja a la propietat intel·lectual. També podria suggerir vies per afrontar les amenaces que la mateixa societat presenta a la privadesa. Com ja s'ha vist, el principi de beneficis recíprocs i la promoció d'aproximacions tecnològiques amb «mentalitat privada» poden ajudar els interessats a exercir més control sobre la circulació i ús de la seva informació personal.
- Aquest optimisme té els seus límits. Encara que aquestes tecnologies podrien contribuir a allò que alguns anomenen apoderament o donar poder a l'usuari, hi ha el risc que, als individus afectats, se'ls deixi fer front sense suport als controladors de dades. En realitat, la tecnologia no és neutral: encara que s'ofereix àmpliament als ciutadans, continua estant indirectament finançada per les empreses, i les agències i departaments oficials, que paguen els servidors. Inevitablement, aquests últims estan probablement més atents als interessos dels controladors de dades que als dels interessats. L'anomenada tecnologia de protecció de la privadesa transforma o podria transformar la relació entre els individus i les seves pròpies dades personals, i convertir-la en una relació de propietat negociable gràcies a les noves tecnologies. Per tant és necessari destacar que l'autodeterminació informativa és una llibertat personal que no és susceptible de negociació, i que la societat té l'obligació de fixar certs límits al dret d'usar aquestes dades.
- Aquest enfocament sobre les eines tecnològiques s'ha d'estendre també a nous jugadors aliens a l'àmbit de la legislació de la segona generació, principalment als serveis de comunicació i subministradors d'equips terminals. El seu paper és crític en qualsevol intent de

24. C. CLARKE (1996). «The answer to the machine is in the machine». A: B. HUGENHOLTZ (ed.). *The Future of Copyright in a Digital Environment*. Kluwer. Pàg. 139 f.

permetre que els usuaris dels nous serveis de la societat de la informació monitoritzin les dades entrants i sortints del sistema, a més de les empremtes de dades que ofereixen a les xarxes i els seus possibles usos. S'ha de prestar atenció per establir responsabilitats estrictes en el subministrament d'equipament i serveis que compleixin amb la privadesa.

24. **Què vol dir exactament aquesta responsabilitat dels productors d'equips terminals i de subministraments de serveis de comunicació?** En la nostra opinió, els proveïdors d'accés a Internet, mòbils i altres operadors telefònics són els responsables d'informar el públic sobre els riscs associats a l'ús de les seves xarxes, informant sobre tecnologies amenaçadores de la privadesa, i han d'oferir accés a aplicacions apropiades per a protegir la privadesa. Aquests proveïdors d'accés tenen un paper central, ja que actuen de guardabarreres entre els usuaris i la xarxa. Per tant, se'ls demana[25] «informar els usuaris sobre mitjans tècnics que puguin usar legítimament per reduir el risc per a la seguretat de dades i comunicacions», «emprar procediments apropiats i tecnologies disponibles, preferentment els que han estat certificats, per protegir la privadesa de les persones afectades (...), especialment mitjançant la garantia de la integritat i confidencialitat de les dades, a més de la seguretat física i lògica de la xarxa», i informar els usuaris d'Internet sobre les maneres d'usar els seus serveis i pagar per ells de manera anònima». Els subscriptors haurien de tenir accés a una línia directa que els permetés informar sobre violacions de la privadesa, i els proveïdors s'haurien de subscriure a un codi de conducta que els obligués a bloquejar l'accés a llocs web que no compleixin els requisits de protecció de dades, sense que importi on estigui localitzada la pàgina web.

El segon objectiu inclou els fabricants i desenvolupadors d'equipaments i programes, i els responsables del traçat d'estàndards tècnics i protocols usats en la transmissió d'informació de la xarxa. Respecte als seus productes o estàndards,[26] haurien de garantir el següent:

- Que compleixen la llei, per exemple garantint que els navegadors d'Internet transmeten la informació mínima necessària per a connectar-se i adoptar mesures de seguretat apropiades.
- Que faciliten l'aplicació dels principis subratllats en la part II, per exemple, permetent als usuaris l'accés directe a les seves dades personals i l'exercici del dret d'objecció automàtic, en particular mitjançant blogs.
- Que eleven el nivell de protecció de dades personals.

25. Potser, en la mateixa línia, hem d'ampliar l'abast de la protecció respecte a les dades cobertes per les legislacions de privadesa. Les noves tecnologies fan possible progressivament el processament de dades sobre individus no –com en el cas tradicional– mitjançant dades relacionades amb la seva identitat legal com el nom o adreça, sinó mitjançant un punt d'ancoratge o, fins i tot, un objecte (anomenat *intel· ligència ambient*) associat. Les dades generades per galetes –com les generades per les etiquetes RFID incrustades en la roba o en productes– no fan necessàriament referència a un individu sinó que, com permeten contactar i fins i tot prendre decisions respecte a una persona –la persona que hi ha darrere del terminal en el cas de les galetes, la persona posseïdora de la roba o els productes en el cas de RFID–, han d'estar subjectes a una determinada protecció.

26. Els terminals, en sentit ampli, s'han de convertir en eines tecnològiques totalment transparents per als que les tenen i les usen. Encara més, en realitat, sovint pertanyen als individus interessats i es podrien veure com a part de la seva llar. Qualsevol intrusió en la seva privadesa s'ha de tractar com qualsevol altra intrusió.

L'opacitat i complexitat dels sofisticats sistemes d'informació a què les persones sotmeten dades requereixen informació addicional que ja no se centra estrictament en el processament per si mateix o en característiques individuals, sinó en el funcionament general del sistema d'informació i la seva habilitat per a generar una gran quantitat d'informació, present i futura. D'allà la necessitat de documentar les dades (origen, usuaris, justificació lògica), descriure els diversos fluxos d'informació i establir normes que controlin com es prenen les decisions, qui té accés i com es controla.

25. Recomanació del Consell d'Europa R (99) 5, III, 1, 2 i 4.
26. Vegeu l'Opinió de la Comissió Belga núm. 34/2000 sobre comerç electrònic i protecció de dades.

Tradicionalment i fins ara, les autoritats de protecció de dades no han parat atenció a les eines tecnològiques. Rarament recorren a especialistes informàtics o penetren en el *sancta sanctorum* dels que decideixen quins desenvolupaments tecnològics es realitzaran i com es configuraran els productes. Tal com els estats europeus han demanat l'establiment d'un comitè assessor governamental (GCA) a l'ICANN –un organisme privat responsable de la gestió de noms i adreces de dominis d'Internet–, podria ser igualment necessari proposar o, fins i tot, insistir en la presència d'un comitè assessor de protecció de dades en l'ICANN, W3C (Consorci World Wide Web) i l'IETF (Grup de Treball en Enginyeria d'Internet). És necessari fer que el sector de comunicacions electròniques sigui plenament conscient de la importància de la protecció de dades.

27. Per resumir, m'agradaria destacar les dues necessitats principals següents:

- La necessitat de subministrar als individus tot el que necessitin per a comprendre i controlar el seu entorn informàtic; en particular, el mitjà per a penetrar en les seves llars. Se'ls ha d'atorgar control sobre qualsevol eina l'ús del la qual faci que es mostrin a d'altres.
- La necessitat de dotar la societat d'eines per a controlar els desenvolupaments tecnològics que, d'una altra manera, podrien amenaçar la supervivència de les nostres llibertats col·lectives i individuals.

La legislació viària imposa als usuaris determinades normes no solament per a reduir els accidents, sinó també per a assolir un equilibri satisfactori entre drets i obligacions dels diversos usuaris de la carretera, ja que les lleis tendeixen a oferir protecció específica als més vulnerables. Això no solament requereix un codi viari, sinó una legislació específica sobre la xarxa de carreteres en concret i els vehicles que les poden usar, que estan subjectes a determinats estàndards obligatoris.

En l'autopista de la informació, no hi ha una legislació que regeixi les normes de funcionament de les telecomunicacions per a la protecció de la privadesa dels usuaris, o requisits per a garantir que els terminals de telecomunicacions que permeten als usuaris navegar en aquestes autopistes funcionen amb justícia i transparència.

Tan sols aplicant els principis de protecció de dades tradicionals a aquestes noves tecnologies, que són implícits però components inevitables de tota telecomunicació, la computació ens pot dirigir vers una societat de la informació democràtica, i proporcionar progrés general per a tothom.

Citació recomanada

POULLET, Yves; DINANT, Jean-Marc (2007). «Vers nous principis de protecció de dades en un nou entorn TIC». A: «III Congrés Internet, Dret i Política (IDP). Noves perspectives» [monogràfic en línia]. *IDP. Revista d'Internet, Dret i Política*. Núm. 5. UOC. [Data de consulta: dd/mm/aa].

<http://www.uoc.edu/idp/5/dt/cat/poullet_dinant.pdf>

ISSN 1699-8154

Sobre els autors

Yves Poullet
Yves.poullet@fundp.ac.be

Professor de la Facultat de Dret de Namur i Lieja (Bèlgica). Llicenciat en Filosofia i doctor en Dret. Director del Centre de Recherche Informatique et Droit de les Facultés Universitaires Notre-Dame de la Paix de Namur (Bèlgica). Professor de Dret, especialment dels ensenyaments sobre «llibertats i societat de la informació», i degà de la Facultat de Dret de les FUNDP. Així mateix, és professor a la Universitat de Lieja.

Jean-Marc Dinant
Jean-marc.dinant@fundp.ac.be

Professor en el Computer Science Institute i CRID (Universitat de Namur)