
@XARXA I ÈTICA. REFLEXIONS PER A UN ÚS ETICOCÍVIC DE LES XARXES SOCIALS

JOAN LLUÍS PÉREZ FRANCESCH

Responsable principal del Grup de recerca sobre llibertat, seguretat i transformacions de l'Estat del Departament de Ciència Política i Dret Públic de la Universitat Autònoma de Barcelona

Moltes de les preocupacions que podem tenir en intentar orientar la gestió de les xarxes socials tenen un *contingut jurídic*, atès que es tracta d'aspectes tan importants com la identitat de les persones, l'ús de l'espai i la ponderació entre drets (privadesa, llibertat d'expressió) o limitacions d'acord amb normes i regulacions. Però, més enllà de les regulacions jurídiques, cal desenvolupar un codi de bones pràctiques en l'ús de les xarxes socials, a tall de comportament cívic. Aquestes bones pràctiques no s'han de limitar a no vulnerar la llei (protecció de dades, drets a l'honor, a la intimitat i a la pròpia imatge, etc.) sinó que suposen assumir el civisme, el respecte als altres, la pertinença a una comunitat virtual, una bona educació. La responsabilitat social de la persona s'expressa també a les xarxes socials i a la xarxa.

Many difficulties that we can have on attempting to orientate the management of social networks have some juridical contents, since it deals with aspects as important as personal identity, the use of the space and the balance among rights (privacy, freedom of speech) or even limitations in accordance with rules and regulations. But, beyond the juridical regulations, it's necessary to develop a code of good practices in the use of social networks, such as civic behavior. These good practices do not have to limit themselves to not breaking the law (protection of data, right to honor, to privacy and to self image, etc) but rather assuming the public spirit, with respect to others, to belonging to a virtual community, or to a good education. Social responsibility is also expressed in social networks and in Internet.

1. LA NECESSITAT D'UNES BONES PRACTIQUES O CRITERIS ORIENTADORS PER A UN BON ÚS DE LES XARXES SOCIALS

Potser algunes de les recomanacions que podem fer no tenen res de l'altre món i formen part d'una idea d'autoresponsabilitat pròpia d'una actitud davant la vida, que no ha de diferenciar el món virtual del real. Es tractaria tan sols d'adaptar a les TIC aspectes positius, sense pensar que estem davant d'un àmbit més perillós que un altre, com pot ser el carrer. Les actituds d'autoresponsabilitat i de consciència de les nostres accions són indispensables per a una societat madura, en la qual es vinculen de forma constructiva l'ètica individual com a usuari i la comunitat d'usuaris de la xarxa. Es tractaria, així, de posar en connexió la persona i la comunitat en què s'insereix, una comunitat que es fa amb ell i gràcies a ell.

Vull parlar del concepte de «xarxa social», concepte sociològic antic que fa referència al fet d'enxarxar les persones en un entrellat que els dona sentit i que les comunica. No s'havia inventat Internet i ja es parlava de xarxes socials. Ara bé, les

xarxes socials virtuals ens han tornat a posar en relleu la importància de la comunitat, amb uns lligams interpersonals més sòlids que els merament societaris, amb tots els aspectes positius i negatius que això pugui significar.

També vull destacar la importància del «saber estar» al món, en el cas que analitzem, virtual, dins un rol, un paper, en el marc d'una lògica de les relacions interpersonals, fins i tot de l'amistat i dels llaços d'afectivitat. Aquest «saber estar» comporta llançar missatges, ésser espectador, fins i tot promocionar o expandir idees alienes, la qual cosa com és obvi ni a les xarxes socials ni al món real es pot fer de qualsevol manera. Suposa moure's amb criteri en un espai públic on es desenvolupa una part important de la vida social de la persona.

Com en tot, es pot fer un abús o un mal ús de les xarxes socials, sense responsabilitat, amb frivolitat o fins i tot amb mala fe. Això passa, per exemple, quan hi ha una suplantació de la personalitat, es creen perfils falsos, es promocionen pàgines delictives de signe divers, des de pornografia infantil a estafes... La confiança en les relacions humanes és determinant i en el nostre objecte de reflexió encara més.

Per tant, cal saber què estem fent, restar amatents, no refiar-se, com tampoc es recomanable fer-ho al carrer. Si en el món «real» no ens relacionem amb desconeguts, per què ho hem de fer en el «virtual» i, en especial, a les xarxes socials? Els malfactors saben que la facilitat del contacte virtual es pot aprofitar per al seus interessos. I el desig de compartir o la necessitat de sortir de la soledat poden tenir conseqüències catastròfiques dins les xarxes socials si no es fa amb prudència i, com he dit, amb responsabilitat, sobretot en el cas dels infants i adolescents. *Cal tenir cura de tot el que es fa, perquè l'anonimat no existeix a Internet.* Les coses no són com semblen. Aleshores cal recomanar que no es pugui a Internet —i dins la comunitat virtual d'una xarxa social encara menys— informacions sensibles o privades sobre un mateix, com ara dades personalíssimes, aspectes íntims, ni refiar-se ingènuament d'allò que es veu en una pantalla, perquè pot ser una autèntica trampa. Cal una cura especial de tot allò que fem, fins i tot encara més que al carrer.

Moltes de les preocupacions que podem tenir en intentar orientar la gestió de les xarxes socials tenen un *contingut jurídic*, atès que es tracta de parlar d'aspectes tan importants com la identitat de les persones i les seves conseqüències, l'ús de l'espai i per tant la ponderació entre drets (privadesa, llibertat d'expressió) o limitacions d'acord amb normes i regulacions. Els atemptats a la privadesa o a l'honor, per exemple, són molt similars al món real i les tècniques d'estil *hacker* que es fiquen en els ordinadors dels altres comporten immissions inacceptables de la privacitat i de dades personals i patrimonials, entre d'altres.

Avui ens cal desenvolupar un *codi de bones pràctiques en l'ús de les xarxes socials*, més enllà de les regulacions jurídiques, i de l'aplicació dels termes i condicions d'ús que marquen les empreses que gestionen aquestes xarxes socials, a tall de comportament cívic. Atès que ens movem en un *context comunitari, voluntari i responsable*, caldria tenir clar què es pot fer i què no és recomanable, per raons jurídiques, però també deontològiques, ètiques i cíviques. En definitiva, per salut democràtica. Moltes plataformes tenen uns criteris per a incorporar-se i fer un ús

mínimament cívic, d'acord amb uns principis de funcionament, especialment preocupats per la seva mateixa reputació, més que per la dels usuaris. Hi ha conductes que tenen una sanció jurídica, com l'assetjament o la violació dels drets dels menors. Però el que jo anomeno ús cívic va més enllà. De fet es tractaria de *no molestar* els altres com a principi general i d'aprofitar els aspectes positius de les xarxes socials en termes de creació de comunitat, de responsabilitat comunitària, de respecte, de bona educació. *El civisme hauria de ser el conjunt de bones pràctiques acceptades per la comunitat d'usuaris.*

Aquest civisme hauria d'incloure la prohibició de la «mala administració», intentant evitar així que qui vulneri els drets de les persones siguin els poders públics, autèntic despropòsit democràtic, mitjançant espionatges, prohibicions de drets per raons polítiques, o altres conductes excessives, en termes jurídics. Aquesta «mala administració» també es dona quan no hi ha respostes a les demandes ciutadanes i els poders públics actuen sense sentit de servei públic i de respecte a les persones usuàries.

També és important al·ludir a les implicacions professionals del bon ús de les xarxes socials, tant en el sentit de les conseqüències professionals que pot tenir el mal ús, com les potencialitats que presenten per a promocionar productes, publicar anuncis, etc., sempre amb respecte als drets dels clients. El consentiment previ de les persones referenciades, de fotos o dades personals, és imprescindible en qualsevol cas com un bon element per a gestionar correctament els perfils.

D'altra banda, des de la perspectiva de la seguretat, les persones han d'assumir un paper molt actiu en la gestió de la seva seguretat a les xarxes, ja que els cossos de seguretat no poden fer el monitoratge dels milions d'activitats que es produeixen diàriament per tal de prevenir possibles il·lícits penals, administratius o civils, i menys encara mirar que es compleixin les bones pràctiques. En conseqüència, *l'única manera d'aconseguir una utilització segura de les xarxes socials i dels recursos que ofereix Internet és potenciar l'educació dels ciutadans i això s'ha de portar a terme mitjançant programes de conscienciació dels riscos i de les amenaces que hi ha, per tal d'establir mesures d'autoprotecció i per prevenir qualsevol succés no desitjat.*

Avui es constata un creixement en la *percepció dels riscos* que comporten les xarxes socials o de certes activitats a Internet (p. ex. el comerç electrònic); però ens trobem encara amb una gran falta d'informació. Això és especialment greu en relació amb els menors, ja que moltes vegades hi ha una *escletxa generacional* entre pares i fills, que fa que aquests darrers no tinguin la imprescindible supervisió en la navegació. D'altra banda, la idea genèrica que la seguretat és responsabilitat principalment dels cossos de policia és absolutament errònia i, per tant, molts ciutadans adopten una actitud passiva o poc reactiva a l'hora de prendre les mesures de protecció necessàries, en aquest i altres camps. En definitiva, la ciutadania ha de prendre un *paper actiu* en la seva autoprotecció al món virtual, ha de comprendre que per les característiques del mitjà no pot delegar sense més ni més les tasques *preventives* als cossos de seguretat, com tampoc no té sentit fer-ho en el món físic. Finalment, cal recordar que és imprescindible que les companyies proveïdores dels serveis d'Internet i en concret les que gestionen les xarxes socials s'impliquin al

màxim per tal de fer possible un ús cívic i evidentment respectuós amb la legalitat i els drets de les persones.

Taula 1. Cinc objectius per a millorar l'ús de les xarxes socials i Internet en general.

(Grup de treball sobre Seguretat del Pla Nacional de Valors, Generalitat de Catalunya, juny 2013)

Objectiu 1	Potenciar una navegació segura i responsable dels ciutadans a la xarxa (autoprotecció dels usuaris).
Objectiu 2	Implicació de les companyies privades que són proveïdores de serveis al món virtual per tal d'aconseguir un món virtual segur i evitar així l'incivisme informàtic.
Objectiu 3	Fomentar l'educació dels menors en l'ús segur de les xarxes i conscienciar els pares dels riscos i amenaces que comporta la navegació.
Objectiu 4	Corregir l'esclatxa generacional dins la família.
Objectiu 5	Protegir els drets fonamentals dels ciutadans en l'ús de les noves tecnologies, evitant il·lícits penals o civils.

2. CONTINGUTS IL·LÍCITS I NOCIUS

La Direcció General d'Atenció a la Infància i l'Adolescència (DGAIA), del Departament de Benestar Social i Família, i el CESICAT¹ van signar el 2012 un conveni de col·laboració que té per objecte la producció de materials, la publicació i promoció de continguts i material audiovisual en els mitjans de comunicació o la realització d'estudis sobre la seguretat en l'ús de les noves tecnologies per part dels infants i adolescents.²

Fruit d'aquesta col·laboració, l'abril de 2013 s'ha publicat la Circular sobre xarxes i Internet,³ en la qual com a directriu s'estableix una diferenciació entre els continguts il·legals i els continguts nocius que afecten directament la infància i la joventut però també la societat en general.

1. El Centre de Seguretat de la Informació de Catalunya (CESICAT) és l'organisme executor del Pla nacional d'impuls de la seguretat TIC aprovat pel Govern de la Generalitat de Catalunya el 17 de març de 2009. És una fundació pública creada per la Generalitat de Catalunya. Per a més informació, visiteu el seu web: <https://www.cesicat.cat/>.

2. Fonts: «Benestar Social i Família i el CESICAT organitzen un cicle de jornades sobre seguretat i riscos a Internet i en l'ús de xarxes socials» [en línia]:

<http://premsa.gencat.cat/pres_fsvp/AppJava/notapremsavw/detall.do?id=202287&idioma=0>.

També «Riscos a Internet i en les xarxes socials» [en línia]:

<<http://www10.gencat.cat/gencat/AppJava/cat/actualitat2/2013/30612riscosalInternetienlesxarxessocials.jsp>> (Consulta: 12 juny 2013).

3. Podeu consultar el document complet en línia a:

<http://premsa.gencat.cat/pres_fsvp/docs/2013/06/04/12/45/cdb8cd6d-4594-40b0-9fe0-8f9f00b-de20f.pdf> (Consulta: 12 juny 2013).

Són exemple de *continguts il·lícits*, entre d'altres:⁴

- pornografia infantil,
- propagació de materials que inciten a l'odi, racisme, antisemitisme o altre tipus de discriminació en funció del sexe, religió, origen, orientació sexual,
- propagació de materials i discursos amb violència extrema o sang desmesurada (*gore*),
- incitació al suïcidi,
- apologia de l'anorèxia i la bulímia,
- joc en línia il·legal.

Pel que fa a *continguts nocius*, és a dir, la informació perjudicial per a la integritat personal, cal destacar que no estan tipificats com a delictes i per tant la seva difusió està permesa. Aquests continguts són diversos, com ara de tipus pornogràfic o violent. Els riscos estan associats a les conductes tant dels infants i adolescents com d'altres persones que es comuniquen amb ells a través del correu electrònic, les xarxes socials i altres eines (fòrums, xats, jocs en xarxa...). Els més comuns són:

- la difusió de dades d'identitat personal: nom, número de telèfon, adreça, correu electrònic... molt important de limitar quan es fa ús de xarxes socials;
- el contacte continuat amb desconeguts i la posterior invitació a intercanviar informació delicada o sensible, o a trobar-se físicament en algun lloc;
- l'escalada de missatges desagradables amb vexacions, amenaces i injúries;
- l'abús escolar i el ciberassetjament escolar (*cyberbullying*);
- el temps incontrolat en l'ús de jocs o dispositius, que pot comportar problemes d'addició al mòbil o caure en el *gambling* (joc amb apostes).

Cal dir que és necessari denunciar tots els continguts i accions de caràcter il·lícit a les xarxes socials i posar els fets en coneixement de la policia mitjançant la denúncia corresponent. Però, un cop més, reiterem la importància de l'educació, de la responsabilitat en l'ús de les xarxes, de la prevenció i, en cas de menors, del control parental presencial —acompanyant els menors en la navegació— o mitjançant filtres.⁵ Els pares, mares o tutors són responsables de les actuacions dels seus fills i aquesta és una responsabilitat que no poden defugir dins l'exercici de la pàtria potestat.

A la mateixa circular, la DGAIA i el CESICAT també estableixen uns consells en l'ús d'Internet per a infants i adolescents, i també per a pares, mares i educadors/ores.

4. D'altres molt greus són el *grooming*, assetjament de caràcter sexual d'un menor; les accions del *grooming* tenen l'objectiu d'establir una relació i un control emocional sobre un nen/a per a després abusar-ne sexualment. A diferència del ciberassetjament, aquest tipus d'assetjament té un objectiu explícitament sexual. També el *phishing*, forma d'enganyar els usuaris perquè revelin informació personal o financera mitjançant un missatge de correu electrònic o lloc web fraudulent.

5. El web del Safer Internet Programme, www.sipbench.eu, s'actualitza trimestralment i compara l'efectivitat i la robustesa dels filtres a diferents edats, dispositius i sistemes operatius.

En l'apartat d'infants i adolescents concreten els consells distingint per franges d'edat: infants de vuit a deu anys, infants d'onze a tretze anys i infants de catorze a quinze anys.

Entre d'altres, un consell adreçat a totes les franges d'edat és que a la xarxa hi ha moltíssimes coses bones, però també n'hi ha alguna de dolenta. S'avisava que si en una web l'infant troba alguna paraula o foto que el fa sentir malament, surti de la pàgina i no deixi que el molesti. També es recomana que ho expliqui als pares o mestres i, en el cas dels adolescents, a algun amic o amiga.

També es recomana a totes les edats no enviar fotografies, ni donar el nom, l'adreça o el telèfon; ser curosos amb les llistes de contactes i les contrasenyes; avisar els pares sobre les noves coneixences que fan a la xarxa, i marxar dels xats que facin sentir l'infant o adolescent incòmode o molestat.

Així mateix es recorda que *l'accés autoritzat* a la majoria de xarxes socials és als *catorze anys*. És important no avançar-se ja que els adolescents es poden trobar amb problemes pel sol fet de no controlar prou bé qui pot veure la informació que hi publiquen. Per això se'ls recomana que es deixin assessorar per un adult en la configuració de la privadesa quan hi accedeixin per primera vegada.

Precisament és a partir d'aquesta edat que es donen consells més específics sobre comprar o fer alguna cosa per Internet que pugui costar diners, haver de donar números de targeta de crèdit o dades bancàries; també s'avisava sobre determinats programes que es puguin descarregar de la xarxa, ja que poden comportar algun virus o programes espies. També s'alerta sobre la informació fiable o dubtosa.

Finalment s'aconsella al jove que, si es vol estalviar possibles problemes i ser un bon ciutadà en línia, actuï correctament i eviti fer res que pugui perjudicar altra gent perquè pot cometre algun delictes com per exemple amenaçar, difamar, atacar el dret a la intimitat enviant fotografies de companys...

En l'apartat adreçat a pares, mares i educadors/ores, s'explica que la millor manera de prevenir situacions de risc i ajudar els fills o l'alumnat a navegar amb seguretat és:

- fer-los conscients dels beneficis i riscos d'Internet,
- educar-los perquè sàpiguen navegar de manera responsable,
- donar-los estratègies que els ajudin a autoprotegir-se mentre naveguen.

També és destacable que es recomani als adults de parlar obertament amb els infants i adolescents sobre l'ús d'Internet, d'interessar-se per allò que els infants i adolescents fan amb l'ordinador i mantenir una bona comunicació amb fills o alumnes. També és important que s'acostumin a presentar-nos les amistats que mantenen per la xarxa.

La millor estratègia és treballar amb ells de manera que puguin aprendre del que ha passat, adquirir uns hàbits de seguretat i saber com protegir-se per si mateixos. Establir una atmosfera de confiança pel que fa a l'ús de la xarxa ens ajudarà a prevenir situacions de risc.

Un altre mètode per prevenir contra els riscos és procurar navegar junts amb els infants i fer d'Internet una activitat lúdica i familiar. En compartir aquesta activi-

tat es pot comentar amb ells, per exemple, la diferència entre publicitat i contingut educatiu o d'entreteniment i mostrar-los exemples de cada cosa.

A la circular també s'aconsella als adults que s'informin sobre les eines de control, com ara els filtres que limiten l'accés a continguts nocius, o que estableixin regles bàsiques de seguretat a la llar: col·locar l'ordinador en una sala comuna a la vista de tothom, establir els llocs web visitables, horaris de connexió, ensenyar-los a navegar amb seguretat (tenir cura amb les dades personals i les contrasenyes, avisar sobre casos que els resultin desagradables, mirar de conèixer els cibermics, compres...).

Un punt important és també que s'aconselli sobre els primers passos en l'ús del mòbil i les xarxes socials.

Finalment s'exposen alternatives davant d'un possible problema o si hi ha indicis de risc per als fills o l'alumnat, i així poder reaccionar a temps.⁶

Taula 2. Consells a les xarxes socials. CESICAT⁷

Les xarxes socials et permeten conèixer gent i tenir amics arreu del món. Pots compartir informació alhora amb tots els teus companys i pots conèixer altres cultures i costums. L'ús de les xarxes socials s'ha estès de forma molt ràpida, però també és un mitjà que utilitzen els delinqüents (sobretot assetjadors sexuals) per captar les seves víctimes. Per això cal estar alerta:

- **No acceptis «amistats» de desconeguts.** A Internet és molt fàcil dir mentides i fer veure que ets una altra persona.
 - **Publicar informació a les xarxes socials és molt fàcil i ràpid, però un cop publicada no saps quin ús en poden fer.** Abans de penjar una notícia o publicar una fotografia pensa-t'ho bé. No facilitis o publiquis dades, informació, fotografies o vídeos d'altres persones sense que t'hagin donat el seu permís.
 - **Inventa contrasenyes llargues i complexes.** Fes servir un àlies (*nick*) que només coneguin els teus amics.
 - **Si algú et molesta o t'assetja en algun xat o grup, surt del grup i avisa els teus pares o tutors.** Sigues respectuós tu també amb totes les persones del grup.
 - **No comparteixis dades** com el telèfon, l'adreça o el teu nom i cognoms. No enviïs mai les teves fotos ni donis les teves dades personals a cap desconegut.
-

6. Si hi ha indicis de risc per als fills o l'alumnat, primerament es pot parlar amb ells, però també notificar-ho a l'adreça electrònica internetsegura@gencat.cat o trucar al 112. En cas de trobar pornografia infantil, material presumptament il·legal o qualsevol altre que es consideri que pot ferir la sensibilitat d'infants o adolescents, es pot contactar amb la policia per denunciar-ho. També es pot denunciar al CESICAT a través de l'adreça info@cesicat.cat o del telèfon 977 010 893.

7. Vegeu notícies al web del CESICAT: «Benestar i Família i CESICAT organitzen un cicle de jornades sobre seguretat i riscos a Internet i en l'ús de xarxes socials» [en línia] <<https://www.cesicat.cat/ca/article/bsf-cesicat-seguretat-xarxes-socials>> (Consulta: 4 juny 2013). També podeu consultar la pàgina web per la navegació segura per la Xarxa del mateix CESICAT: <<http://www.Internetsegura.cat/>>.

-
- **A Internet no tothom és amic.** No quedis amb les persones que coneguis a través de la xarxa. I si quedes amb algú, avisa els teus pares o algun amic que t'acompanyin i queda en un lloc públic.
-
- **No acceptis arxius de persones que coneguis al xat,** perquè podrien incloure algun virus. Fins i tot les cançons o les fotos que t'envien poden ser perilloses.
-

3. UN DISCURS POSITIU PER A LES XARXES SOCIALS

De tot el que estem comentant deriva la necessitat de fer un ús ètic i responsable de les xarxes socials, a banda d'atendre a les conseqüències legals dels propis actes.⁸ No podem oblidar l'important paper que fan per a la construcció d'una societat democràtica, amb més transparència i capacitat de debat dels afers col·lectius.⁹ Les xarxes socials han de promocionar el coneixement del dret que també les regula i afecta els usuaris i administradors. De fet, es discuteix si els gestors de comunitats (*community managers*), de grups o blocs són responsables dels continguts dels membres o seguidors actius. Avui tothom pot ser considerat periodista, en un sentit impropï,¹⁰ com a creador d'una opinió pública lliure, a partir del debat racional de la informació que es posa a la xarxa, per la qual cosa hom ha de vetllar per la veracitat i pel respecte dels drets a l'honor, a la intimitat, a la pròpia imatge, sense oblidar la protecció de les dades personals. Una piulada al Twitter es veu sotmesa a aquests condicionaments, en la mesura que esdevenim partícips de

8. Sobre el dret a la protecció de dades personals: Llei orgànica 5/1999, de 13 de desembre, de protecció de dades de caràcter personal i STC 292/2000, de 30 de novembre, sobre aquesta Llei; Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions; Llei 34/2002, d'11 de juliol, de serveis de la informació i del comerç electrònic, modificada per la Llei 32/2993, de 3 de novembre; Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic (modificada per la Llei 32/2003, de 3 de novembre, general de telecomunicacions, per Llei 59/2003, de 19 de desembre, de signatura electrònica, per Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions, i per la Llei 56/2007, de mesures d'impuls a la societat de la informació); STC 94/1998, de 4 de maig (dades d'afiliació sindical, com a dades sensibles).

D'altra banda, cal tenir en compte els límits i la ponderació entre els drets fonamentals dels art. 20 i 18 CE. La jurisprudència del Tribunal Constitucional sobre la limitació de drets fonamentals, com ara la STC 57/1994, estableix que tot acte o resolució que limiti drets fonamentals ha de garantir que les mesures restrictives siguin adequades, és a dir eficaces per obtenir el que es vol, necessàries, que no hi hagi una mesura igualment eficaç que sigui en canvi menys limitadora de drets fonamentals, i proporcionada, que el sacrifici final del dret no sigui massa gran en relació amb l'objectiu assolit. En general és cabdal atendre el principi *favor libertatis* com a criteri interpretatiu. Finalment no podem deixar passar la relació que s'estableix entre la llibertat d'expressió, el secret professional i la seguretat nacional (com ho posen de manifest el cas Roldán o el cas Wikileaks).

9. Vegeu, en aquest sentit, Castells (2012). Entre altres aspectes cal ressenyar l'ús ja imprescindible de les xarxes socials per part de polítics, personatges famosos, professionals, empresaris, etc. El president Obama va fer una intensa campanya a Facebook a les eleccions de 2008. També s'ha de recordar la lluita per a un ús lliure i no sotmès a censures a diverses parts del món, i la capacitat cada dia més gran de convocatòria per a trobades, en general i per a manifestacions, vagues, etc. de manera especial.

10. Ens trobem amb el fet que cada usuari esdevé un creador d'opinió pública, sense proposar-s'ho.

l'àgora de la xarxa social. La capacitat d'incidir en la *construcció de l'espai públic deliberatiu* i d'afectar així la reputació dels altres (i d'un mateix) fa que la presència dins la xarxa social no es pugui utilitzar impunement per a injuriar, difamar o lesionar drets dels altres. Dret i ètica van del bracet.

Ara bé, cal diferenciar entre *fets i opinions*. Els primers han de ser verídics i les segones, respectuoses amb els drets de les persones. A banda, hi ha la qualitat dels missatges i la vulgaritat d'allò què es diu, encara que sigui veritat. En aquesta línia, caldria plantejar-se què fer quan un usuari penja, per exemple, una piulada errònia al Twitter o que conté una informació falsa. Quina és la millor solució? Esborrar-lo, rectificar la informació o penjar-ne un altre? Deixem la pregunta oberta, però la resposta té un fort contingut educatiu, ètic i cívic.

Han augmentat les fotos que es penjen a les xarxes socials, que són així compartides. Cal respectar els drets d'autor i, per què no, evitar la compartició sense que es formalitzi l'autorització. En un altre cas, l'usuari esdevé un personatge «sol davant el perill» i haurà d'assumir les conseqüències. La identitat i la reputació digital es configuren avui en gran part mitjançant el que posem de nosaltres mateixos i d'allò que els altres ens posen a les xarxes socials. És per això que cal ser curiosos i diligents amb les coses que diem, les fotos o vídeos que pengem, etc. De fet, la privadesa, en sentit clàssic, era concebuda com un santuari que protegia la persona, cosa encara molt important. Però avui hi ha una cosa diferent, perquè consentim fàcilment a mostrar aspectes de tot tipus de la nostra vida, també els més privats i fins i tot íntims. Hem de ser conscients que el límit que posem és molt baix massa vegades, tant a les xarxes socials com a Internet en general. Diego Guerrero Fuertes (2010, 2011) ha posat de manifest com la navegació pot ser una cosa segura i plaent, sempre que es faci amb cura i responsabilitat.¹¹ Donar dades financeres, acceptar galetes (*cookies*) sense pensar, navegar per llocs insegurs, respondre a la geolocalització, no vigilar les vulnerabilitats del maquinari, tallafocs i antivirus per tal d'evitar cavalls de Troia, contactar amb estranys, en especial en el cas de menors, té els seus perills i no ens ajuda a fer de la vida digital un món segur i habitable.

Les xarxes socials són un important producte de la nostre societat de masses i, per tant, un àmbit adient per a exercir determinats lideratges (comercials, polítics, ideològics, etc). Són també un perillós camp d'experimentació on la persona *massa* es pot endinsar i ser manipulada, demanant-li informació de tot tipus, i ser objecte de malifetes o actuacions denigrants. Les relacions humanes a la xarxa no passen només en un sentit horitzontal —entre els membres— sinó en relació amb els creadors o propietaris del servei, els quals aproven unes condicions d'ús que suposen un autèntic *contracte d'adhesió*. Aquest contracte és important atès que, entre altres coses, es determina la propietat compartida de les fotos, la informació i el mateix perfil de cada usuari, en termes de privadesa (tot i que s'ofereixen diversos nivells). Tanmateix, el foment de la feina cooperativa en la construcció de grups és

11. «Diez consejos para despistar al "Gran Hermano" de Internet». *La Vanguardia.com*, 16 juny 2013 [en línia] <<http://www.lavanguardia.com/Internet/20130616/54375645613/diez-consejos-evitar-ser-controlados-Internet.html>>.

una dada molt rellevant i formativa, que no podem obviar. Els administradors de la xarxa normalment adverteixen dels controls de privadesa que procuren i articulen mecanismes per tal de denunciar comportaments o continguts il·lícits o perillosos. Un aspecte a destacar és el «dret a l'oblit», actualment molt en boga, atès que les dades marxen ràpidament per la xarxa i acabem perdent-ne el control, fins i tot encara que ens donem de baixa.

Si prenem com a exemple Facebook, cal recordar que té una *declaració de drets i responsabilitats*, basada en la llibertat per a compartir i connectar-se, en la propietat i el control de la informació de les persones que s'hi adhereixen, la igualtat de tracte entre tots els membres, la gratuïtat, la transparència i la universalitat. A més, cal saber que les dades poden ser cedides a tercers (com a mínim als EUA), tot i el consentiment exprés exigible per la protecció de la propietat intel·lectual; que els menors reben una protecció especial (no s'accepten menors de catorze anys a Espanya); que s'ha de donar una informació autèntica del nom (malgrat els pseudònims)¹² i de la fotografia, aspectes que *no es consideren dades privades*. A més, Facebook *emmagatzema* informació de tot el que posem a la xarxa, fins i tot obtenint-la de tercers, tot i que l'usuari pot modular el seu grau de privadesa. Quan es cancel·la un compte s'elimina el perfil, però no el «rastre» que hem deixat en la interconnexió amb els «amics». D'això també penso que n'hauríem de ser més conscients. Facebook fonamenta el negoci en el màrqueting segons el nostre perfil.

En el cas de Twitter, per citar una altra gran xarxa social, és important llegir les condicions d'ús i la política de privacitat. Les piulades comporten sol·licitud de publicitat del missatge dins la xarxa i per tant llicència per a gestionar-la. El límit d'edat d'accés és de tretze anys a tots els països. En funció dels perfils dels usuaris s'ofereix informació comercial.

En tot cas, cal que recordem que els propietaris de les xarxes socials són *empreses privades*, que es guien pels principis del mercat i que com tants àmbits d'Internet és difícil de controlar, atesa la no-territorialitat de les actuacions. Tot i així, les condicions d'ús estableixen sempre les clàusules contractuals de submissió jurisdiccional als tribunals competents, normalment de la nacionalitat de la societat gestora. El problema, però, és com solucionar els conflictes sense anar als tribunals. I sovint també superar una certa desconfiança sobre l'ús real que fan de les dades personals que tenen, per la via de la cessió d'arxius.

Cal tenir sempre en compte els paràmetres que fa servir l'Organització per a la Cooperació i el Desenvolupament Econòmic (OCDE):¹³ conscienciació, responsabilitat, resposta dels participants per a poder fer front als reptes de la seguretat, ètica —respecte als interessos de tercers—, respecte als principis democràtics, ava-

12. Normalment s'exigeix a les condicions d'ús una identificació real, però es poden utilitzar pseudònims per a ésser menys localitzable, o per a compartir només amb els amics que et coneguin la informació que es puja a la xarxa. Un pot posar el que vulgui, però en sentit estricte això no estaria recollit per les normes generals d'ús de la xarxa, perquè facilitaria la creació de perfils falsos.

13. Recomanacions de l'OCDE dins el document «Directrius per a la seguretat de sistemes i xarxes d'informació: cap a una cultura de seguretat» adoptades pel Consell de l'OCDE en la sessió número 1.037, de 25 de juliol de 2002.

luació del risc, adopció de protocols de seguretat, o reavaluació de la seguretat dels sistemes que es fan servir.

Ara bé, en termes de *civisme*, no podem caure en el vessant negatiu, atès que les xarxes socials permeten una nova forma de comunicar-se i de relacionar-se molt interessant, i avui en dia ja ineludible, en especial de cara al jovent. No hi ha dubte que provoquen una integració de les persones en una comunitat (encara que sigui per a compartir fotos, per exemple) i, a més, de forma molt senzilla i assequible per a qualsevol. El fet de la gratuïtat encara fa més ràpid i simple la incorporació a la xarxa, la qual cosa no hauria de fer suposar que tenim un control absolut dels continguts, sinó més aviat al contrari, atès que la informació que proporcionem és precisament la matèria primera del «negoci» de les xarxes socials. I també hauríem de ser conscients que en principi qualsevol persona, fins i tot la més anònima, ens podria observar.

De la idea anterior derivaria un principi general d'*autoresponsabilitat* no tan sols en l'ús de la xarxa sinó en el mateix maquinari que es fa servir. La seguretat és una preocupació general que contextualitza activitats d'intercanvi d'informació i fins i tot de comerç. L'accés a pàgines xifrades, o des d'un port segur, tenir cura de la protecció de dades personals, el respecte als drets de les persones (no tan sols els de la personalitat sinó els connectats a ella com la propietat industrial i intel·lectual) ha de ser la divisa màxima d'una bona actuació a les xarxes socials.

És clar que cal lluitar per a evitar que es vulneri el dret a l'honor dels altres i, per tant, que no es calumniï (acusació d'haver comès un delictes) ni injuriï (lesionar la reputació i l'honor dels altres). És fàcil atemptar contra l'honor de les persones a les xarxes socials, si tenim en compte que el mateix instrument ens facilita una actitud proactiva i per tant una predisposició per a dir coses. Caldria ser conscients que de vegades és millor callar? La identificació dels usuaris, obligats legalment a donar-se d'alta mitjançant dades reals, ens hauria de fer reflexionar sobre la *capacitat potencialment lesionadora d'allò que podem dir dels altres*. També el dret a la intimitat pot ser fàcilment vulnerable, si posem informacions sobre persones que després poden ser reenviades a tercers, i de forma especial caldria que fóssim respectuosos amb la imatge dels altres, com pot passar si pengem fotos amb amics al Facebook o Twitter. El cas encara pot ser més greu si hi surten menors. Cal que cerquem, arribat el moment, el consentiment des seus representants legals. Tots aquests drets són objecte de protecció per la via penal o per la via civil. També s'han d'evitar i perseguir tot tipus d'amenaques i coaccions a tercers, que, com és obvi, constitueixen delictes. Ara bé, les xarxes socials ofereixen la possibilitat de denunciar conductes abusives, il·legals i contràries a les condicions d'ús. La llibertat d'expressió ha de ser modulada i ponderada amb l'exercici dels drets que estem comentant, d'acord amb l'art. 20 CE.¹⁴

Igualment cal protegir la propietat intel·lectual, els drets d'autor, perquè no podem acceptar que el món d'Internet i menys el que funciona en àmbits «tancats»

14. «Difundir por redes sociales información privada puede ser delito» [en línia]. *La Vanguardia.com*, 30 de novembre de 2012. <<http://www.lavanguardia.com/Internet/20121130/54355958465/difundir-redes-sociales-informacion-privada-delito.html>>.

com les xarxes socials siguin «lliures», com la selva. Les plataformes posen a l'abast dels usuaris mecanismes de denúncia. Tot i així, la capacitat per a «copiar» continguts, imatges o vídeos, és altíssima i difícilment controlable en la seva totalitat, i encara menys quan es fan trucatges o modificacions sense permís dels autors. És fàcil ser «creatiu» i agafar idees d'altres per a reenviar-les reelaborades. El mateix passa amb el respecte a la propietat industrial, de marques o logos. En tots els casos, si la via preventiva no funciona, caldrà atendre a la responsabilitat penal o civil de les persones que produeixin accions lesives.

Un altre punt de col·lisió amb l'ordenament jurídic i que comporta una conducció d'un desvalor important en termes també de civisme en l'ús de les xarxes socials és la vulneració de la privadesa i de les dades personals, com anem insistint en aquestes línies, en casos en què *no es respecta el consentiment previ necessari dels afectats* o, el més greu, de recopilar dades de forma enganyosa —conductes considerades per la Llei orgànica 5/1999 de protecció de dades de caràcter personal de tipus greu i molt greu. També tenim el robatori de dades personals, la suplantació de la identitat digital i en general conductes il·lícites que comporten una gran molèstia i perjudici a terceres persones. D'altra banda, els *hackers* fan servir coneixements tècnics per a robar contrasenyes, crear perfils falsos, segrestar el compte d'usuari en definitiva, tot amb l'objectiu de fer malifetes. Fins i tot, la consulta d'un enllaç en una piulada, com que es mostra de forma curta i diferent de l'original, pot provocar un engany.

Les xarxes socials permeten cada vegada més allò que s'ha anomenat l'*extimitat*.¹⁵ Avui sembla que no hi ha gens ni mica de pudor a l'hora d'explicar qualsevol aspecte de la vida privada, com una mena de *reality show*, amb el perill d'un excés de confiança en relació amb els «amics», que potser no sempre ho són. La vida és desenvolupa, així, en una mena de «casa de vidre» on és fàcil rastrejar i conèixer mitjançant les nostres petjades molts aspectes de la vida més íntima (vida amorosa, lleure personal i potser excessos que es poden cometre, fins i tot actuacions delictives en potència, com penjar fotos o vídeos compromesos).¹⁶ El concepte de «vida privada» s'ha transformat en part, si més no, per les pròpies conductes dels usuaris a les xarxes socials, tant en relació amb ells mateixos com davant terceres persones.¹⁷

Darrerament hem tingut casos que han fet saltar les alarmes per una actuació «viral».¹⁸ El cas del robatori i la difusió de telèfons de l'agenda del periodista Pipi Estrada. El fet de repiular unes dades privades pot ser un delictes de revelació de

15. Vegeu, M. Garmendia: «Internet impulsa l'exhibicionisme». *La Vanguardia.com*, 23 de juny de 2013, p. 34. Aquest és un concepte creat pel psicoanalista Lacan i que avui s'ha posat en relleu per P. Sibina, *La intimidad como espectáculo*, FCE, Mèxic, 2008.

16. El cas d'Olvido Hormigos és el més clar. Es tractava de la difusió sense consentiment d'un vídeo íntim. La persona afectada va guanyar notorietat. Podeu consultar *El Huffington Post* [en línia] de 6 de setembre de 2012: <http://www.huffingtonpost.es/2012/09/06/video-concejal-psoe-alcaldia_n_1860262.html>, o del 11 d'octubre de 2012: <http://www.huffingtonpost.es/2012/10/11/olvido-hormigos-dice-que-_n_1957742.html>.

17. M. Wieviorka, «Secret, seguretat i vida privada», *La Vanguardia*, 21 juny de 2013, p. 21.

18. «Difundir por redes sociales información privada puede ser delito» [en línia]. *La Vanguardia.com*, 30 de novembre de 2012. <<http://www.lavanguardia.com/Internet/20121130/54355958465/difundir-redes-sociales-informacion-privada-delito.html>>.

secrets de l'art. 197 CP en condició de cooperador necessari o còmplice. I les víctimes han estat no tan sols el periodista sinó les persones afectades per la revelació del seu número de telèfon. Un altre cas conegut ha estat el de la presentadora de televisió Paula Vázquez,¹⁹ en difondre pel Twitter el seu telèfon, i després en no poder parar les trucades distribuir els telèfons dels «assetjadors», en una mena d'espiral sense fi. D'altra banda, al Regne Unit milers de tuitaires han estat acusats de difamadors per repiular missatges²⁰ que acusaven d'abús de menors un polític retirat. En tot cas, en termes jurídics, s'ha començat a reconèixer que una xarxa social és un mitjà adient per a rectificar una informació falsa, per ordre judicial,²¹ i Facebook es considera un mitjà de prova vàlid a judicis.²²

Però, com estem dient, no tot són perills i actes il·lícits, que cal integrar dins la cultura del ciberespai. Hi ha xarxes socials, com ara la plataforma LinkedIn, especialitzades en les relacions professionals i empresarials. Es pot propiciar una feina cooperativa, promocionar les pròpies activitats a tall d'un màrqueting en línia, entrar en contacte amb nous empleats potencials, generar dades reputacionals en definitiva. Com a element destacable, en l'àmbit empresarial, em sembla interessant la capacitat per a posar en comú la responsabilitat social corporativa.

La censura és un dels grans perills del món de les xarxes socials. La censura és incompatible amb la societat democràtica que les xarxes socials han de poder desenvolupar, de cara a construir una democràcia més deliberativa. Alguns governs han censurat xarxes —per no dir gran quantitat de pàgines web— com en el cas de la Xina, per exemple. Però cal tenir en compte també la impropedència de la presència organitzada de grups (neonazis, gihadistes, màfies, etc.) que pretenen captar adeptes i fins i tot fer apologia d'activitats criminals terroristes.

Les xarxes socials s'han situat en l'escenari de l'exercici dels drets socials, com és el dret a l'educació, el dret al treball (teletreball), i són una via sostenible del manteniment dels estàndards de drets, quan falla la presencialitat pel seu cost elevat. El treball cooperatiu, en grups, és una gran aportació de les xarxes socials al món de la cultura, que no es pot oblidar. El futur, cada vegada més, es desenvoluparà mitjançant plataformes, campus virtuals, xarxes socials i per tant escenaris virtuals, on es tindrà molt en compte l'esperit emprenedor, la motivació i la construcció d'una ciutadania activa (basada en competències i habilitats transversals). A l'altra banda de la balança, s'han donat casos en què, per a donar una feina, l'empresari consulta abans el perfil de Facebook d'una persona, i s'ha rescindit el contracte de treballadors que consulten xarxes socials a l'empresa.

19. «Paula Vázquez desencadena una crisis en su perfil de Twitter tras publicar su número de teléfono» [en línia]. *La Vanguardia.com*, 22 d'octubre de 2012. <<http://www.lavanguardia.com/Internet/20121022/54353796828/twitter-crisis-paula-vazquez.html>>.

20. «Miles de tuiteros, acusados de difamación por rebotar rumores en la red» [en línia]. *El País*, 22 de novembre de 2012. <http://sociedad.elpais.com/sociedad/2012/11/22/actualidad/1353599720_847000.html>.

21. «El derecho de rectificación se extiende a las redes sociales» [en línia]. *Expansión.com*, 18 de juny de 2013. <<http://www.expansion.com/2012/11/23/juridico/1353693916.html>>. El jutjat de primera instància de Pamplona obliga a publicar la decisió al Twitter, en exercici del dret de rectificació.

22. «El derecho a la intimidad se redefine en Internet» [en línia]. *Expansión.com*, 12 d'abril de 2012. <<http://www.expansion.com/2009/04/12/juridico/1239560180.html>>.

Les xarxes socials han de garantir al màxim no tan sols la seguretat sinó el ple desenvolupament dels drets de les persones i ajudar a augmentar la confiança en les TIC. Cal fer pedagogia en positiu, sense por, i reconèixer que com en tots els àmbits de la vida se'n pot fer un mal ús i que aleshores cal que s'apliqui amb contundència la llei. Però avui hem de reconèixer que les xarxes socials són un bon instrument d'ajuda a les persones i així ho ha entès la policia, els bombers, protecció civil, els serveis socials dels ajuntaments, etc. que les fan servir. També és un gran basar d'informació: el seguiment de les xarxes et permet estar informat de l'actualitat, en un procés de retroalimentació entre actors públics i privats de gran transcendència social. D'altra banda, permet un retrobament amb persones i una socialització massiva si així es desitja, fins i tot localitzant persones en temps real segons les darreres aplicacions. L'ús en els àmbits educatiu, comercial, polític, etc. conforma un dels fenòmens sociològics més transcendents dels nostres dies.

En el marc del *discurs positiu i constructiu*,²³ sempre acompanyat de la reflexió jurídica, destaquen les bones pràctiques, perquè cal donar un pas endavant en l'argumentació i no deixar-nos endur pel discurs de la por i els perills. És clar que n'hi ha i molts, de perills. Però per progressar cal establir mesures efectives per a lluitar contra els malfactors de tota mena. També cal millorar el control sobre unes empreses privades que si bé desenvolupen una funció social, el seu principal objectiu es econòmic o mercantil.²⁴ I especialment el gran problema és el caràcter globalitzat d'unes actuacions que caldria ordenar també des d'una política global —s'intenta en l'àmbit europeu, amb la nova proposta de reglament de protecció de dades de la Unió Europea,²⁵ però els Estats encara no accepten uns estàndards de conducta únics; i de vegades són ells mateixos els primers interessats en aquesta diversitat.

En el context de l'argumentació positiva, cal recomanar que els usuaris llegeixin les *condicions d'ús* de les xarxes i, en especial, la política de privadesa, i que un cop a dins en facin un ús segur i responsable, sense exposar-se a actuacions abusives ni lesives dels drets de tercers. El problema és la interpretació de casos concrets, com podem veure en el cas de les *Directrius de la comunitat YouTube*,²⁶ tot i que adoptar les bones pràctiques ajuda molt. A grans trets, destaco algunes de les directrius que estableix l'equip de YouTube:

23. Touriño, A. «Escribir en Internet: Guía jurídica para los nuevos medios y las redes sociales». Actualidad. Abogacía Española, 2 d'octubre de 2012 [en línia] <<http://www.abogacia.es/2012/10/02/escribir-en-internet-guia-juridica-para-los-nuevos-medios-y-las-redes-sociales/>>.

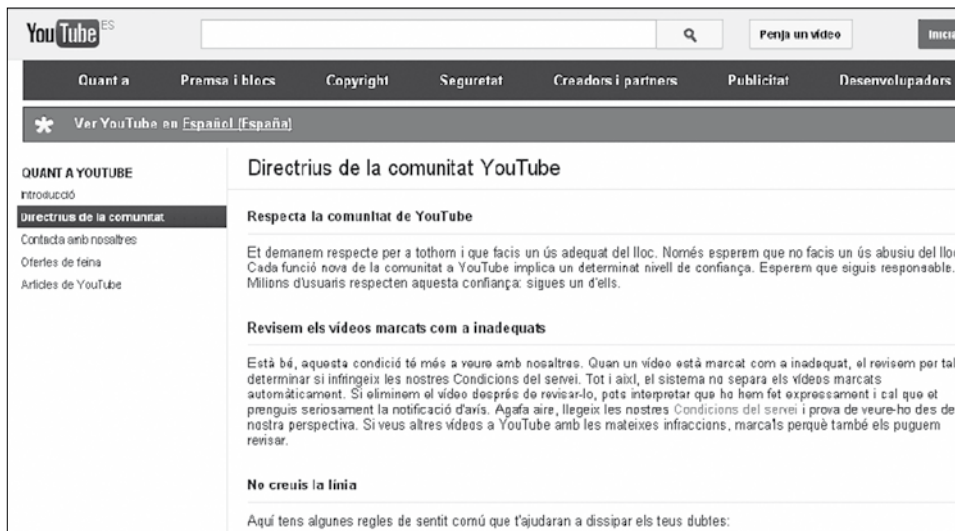
24. «El peligro del SaaS para la libertad de expresión». La Pastilla Roja, 30 de setembre de 2012 [en línia] <<http://lapastillaroja.net/2012/09/peligro-saas-para-libertad-expresion/>>.

25. Vegeu per exemple: «España apoya el Reglamento europeo de protección de datos ante el rechazo de algunos Estados miembros» [en línia]. DiarioJurídico.com, 7 de juny de 2013. <<http://www.diarijuridico.com/actualidad/noticias/espana-apoya-el-reglamento-europeo-de-proteccion-de-datos-ante-el-rechazo-de-algunos-estados-miembros.html>>. I també: «¿Qué novedades y requerimientos establece el nuevo Reglamento Europeo de Protección de Datos?» [en línia]. *Expansión.com*, 20 de juny de 2013. <<http://www.expansion.com/2013/06/20/empresas/tmt/1371710142.html>>. Es preveu una regulació uniforme d'àmbit europeu del dret de la privadesa.

26. Podeu consultar les Directrius de la comunitat YouTube, completes, a <http://www.youtube.com/community_guidelines?gl=ES&hl=es>.

- respecte per a tothom i ús adequat;
- nivell de confiança;
- revisió dels vídeos marcats com a inadequats;
- les infraccions de les condicions d'ús poden provocar una notificació d'advertiment o la cancel·lació del compte;
- no creuar la línia de les regles de sentit comú: YT no està pensat per mostrar pornografia ni contingut sexualment explícit, ni per mostrar coses cruels com ara maltractament d'animals, consum de drogues o fabricació de bombes; no és permesa la violència gràfica o gratuïta; no és un lloc de commocions; cal respectar els drets d'autor; no s'admet la incitació a l'odi; tolerància zero amb els comportaments depredadors, assetjaments, amenaces, hostilitats, invasió de la privadesa o revelació de dades personals d'altres membres; no fer accions que confonguin i comportin correu brossa;
- es recorda a l'usuari que YT és la seva comunitat i que cadascun fa que aquest lloc sigui el que és.

Figura 1. Imatge de la pàgina web de Directrius de la comunitat YouTube.



4. REFLEXIÓ FINAL

En aquest treball he volgut destacar que les xarxes socials hi són ja per a quedar-s'hi i, per tant, necessitem unes regles clares de bon ús. Aquest bon ús no s'ha de limitar a no vulnerar la llei (protecció de dades, privadesa, drets a l'honor, a la intimitat i a la pròpia imatge, etc.) sinó que ha d'anar més enllà. Les bones practiques suposen assumir el civisme com a concepte que comporta el respecte als altres, la pertinença a una comunitat virtual, una bona educació. La responsabilitat

social de la persona s'expressa també a les xarxes socials i a la xarxa, en el món entès com una totalitat.

Davant del discurs de la por, els perills i les incerteses, necessitem seguretats, visions constructives de les accions humanes. La qualitat de l'ús de les xarxes socials és una mostra de la qualitat humana i, per extensió, de la qualitat del país. Un país educat, amb persones que saben allò que fan és un país admirable, al qual aspirem. No renunciem a posar el llistó al més amunt possible. Aquesta hauria de ser la nostra esperança.

REFERÈNCIES

CASTELLS, M. *Redes de indignación y esperanza*. Madrid: Alianza, 2012.

GUERRERO FUERTES, Diego. *Fraude en la red*. Madrid: Ra-Ma, 2010.

— *Facebook. Guía rápida*. Madrid: Star Book, 2011.