Arquitectures de comerç electrònic

Josep Lluís Ferrer Gomila
Llorenç Huguet Rotger
M. Magdalena Payeras Capellà

PID_00199768

UOC
Universitat Oberta de Catalunya

Índex

Introducció

La generalització del comerç electrònic ha suposat una revolució en la forma de dur a terme les transaccions comercials, sobretot des del moment en què totes les etapes de determinades operacions es poden efectuar a distància. La compra, la contractació i el pagament són algunes de les operacions que es poden realitzar electrònicament gràcies a l'aparició de protocols que implementen la versió electrònica dels serveis comercials tradicionals. Les primeres relacions dels usuaris consumidors amb el comerç electrònic es limitaven a l'obtenció d'informació i a la selecció de productes, úniques etapes de la cadena comercial que un usuari estava disposat a realitzar electrònicament, potser perquè aquestes etapes es caracteritzen per l'anonimat de l'usuari i l'absència de dades personals o bancàries. De manera general, els usuaris no es mostren disposats a continuar el procés si el servei no ofereix garanties de seguretat i de protecció del consumidor. Actualment, totes les etapes comercials es poden realitzar electrònicament, fins i tot la contractació i el pagament, utilitzant protocols que satisfan conjunts importants de propietats desitjables. Algunes d'aquestes propietats deriven de les propietats dels serveis anàlegs del món físic, mentre que altres provenen de les característiques pròpies del món electrònic. Algunes propostes es descarten per la seva mancança de seguretat, privacitat o viabilitat.

En aquest primer capítol de l'assignatura de comerç electrònic s'enumeraran els models de negoci habituals en les arquitectures de comerç electrònic. Aquests models de negoci seran el punt de partida de les aplicacions que requereixen protocols segurs i que s'aniran descrivint en els diferents mòduls de l'assignatura. En la segona secció es descriuran les bases de seguretat utilitzades en el comerç electrònic i en la tercera secció es farà un repàs de la situació actual, partint de dades i xifres relatives al comerç electrònic.

1. Arquitectures, actors i models de negoci

En aquest primer capítol de l'assignatura de comerç electrònic definirem el terme comerç electrònic basant-nos en la descripció dels actors i els models de negoci.

La definició de comerç electrònic engloba la compartició d'informació comercial, el manteniment de relacions comercials i l'execució de transaccions comercials a través d'ordinadors o altres dispositius connectats a xarxes de telecomunicacions.

Dins de les relacions comercials englobades en el comerç electrònic es poden identificar diferents tipus d'actors, els consumidors, als que anomenarem C, les entitats comercials, B, i l'Administració, A. En funció de quins siguin els actors involucrats en una transacció comercial apareixen els models classificats com a *Business to Business* (B2B), *Business to Costumer* (B2C), *Costumer to Costumer* (C2C) o *Costumer to Administration* (B2A).

Els darrers anys s'ha pogut constatar un augment en l'interès pels sistemes distribuïts que involucren relacions comercials. Hi ha un nombre elevat de models que les empreses poden adoptar a l'hora d'establir els seus comerços virtuals. Probablement el model més conegut és aquell en el qual el comerciant posa a la venda determinats productes, ja siguin productes que requeriran un enviament físic o productes digitals que es poden servir a través de la xarxa.

Els models de negoci han estat utiltizats per a crear aplicacions a Internet. Un model de negoci és una descripció d'alt nivell d'un tipus d'aplicació que conté les característiques comunes que es poden trobar en exemples específics del model. A continuació es llisten altres models de negoci propis del comerç electrònic:

- **Botiga electrònica**. És la forma més habitual d'establiment comercial a la Xarxa. Es basa en una empresa que presenta un catàleg de productes als seus clients potencials a través d'Internet, proporcionant mecanismes per a facilitar que els consumidors puguin adquirir els seus productes. Per tant, aquests establiments hauran d'incloure un mecanisme per a permetre la realització de la comanda i el pagament dels productes. Els sistemes de pagament habitualment són diversos, des de pagaments de tipus tradicional, com el pagament contra reemborsament, pagaments basats en targeta de crèdit o bé sistemes de pagament totalment específics de les compres electròniques. En aquesta assignatura es descriuran ampliament els sistemes de pagament electrònics que millor s'adapten al comerç electrònic i que satisfan els requeriments de seguretat i privacitat.

La sofisticació d'aquests establiments varia des d'una presentació simple d'un catàleg estàtic a catàlegs interactius amb continguts multimèdia i manteniment d'espai per a incloure els comentaris dels clients. El model de botiga electrònica proporciona una presència global, una manera barata de presentar els productes a l'audiència i decrementar els costos de promoció i màrqueting.

- **Subhastes en línia**. Llocs on se subhasten objectes acceptant les licitacions dels usuaris dins d'un període. Depenent del sistema utilitzat es pot permetre la participació anònima dels usuaris. Només l'usuari que hagi aconseguit l'objecte subhastat serà identificat. L'empresa en línia obté beneficis cobrant comissió a totes les parts participants o a algun subconjunt d'elles.

- **Centres comercials**. Un centre comercial és una col·lecció de botigues electròniques normalment relacionades amb un mateix servei o producte. Habitualment els centres comercials són gestionats per una empresa que cobra a les botigues pel fet d'administrar la seva presència: manteniment del lloc web, màrqueting i gestió de transaccions i pagaments.

- **Portals**. Un portal és un lloc web que conté catàlegs i gestiona grans volums d'informació. Pel fet de contenir un gran nombre d'enllaços aquestes pàgines representen un lloc d'entrada a la Xarxa. Els portals poden ser horitzontals o verticals. Un portal vertical ofereix l'entrada a un conjunt d'informació relacionada amb un mateix tema. Un portal horitzontal proporciona informació sobre una àrea gran. Es poden incloure enllaços als establiments que venen productes o serveis. El portal pot cobrar per visita realitzada a l'establiment electrònic o bé pot rebre una tarifa per incloure l'establiment en el portal.

- **Ajustament dinàmic de preus**. En determinades implementacions es permet fer l'ajustament dinàmic de preus. El preu es converteix en una variable oberta a negociació. En alguns casos el preu el proposa un client individual; la proposta es valora i se'n decideix la possible acceptació. En altres casos es requereix l'agrupament dels clients per tal de negociar un preu conjuntament. El seu èxit vindrà determinat tant pel preu sol·licitat com pel nombre d'usuaris interessats.

- **Proveïment electrònic**. És el terme utilitzat per a descriure la licitació de béns i serveis. Si una empresa decideix que requereix alguns productes, per tal de dur a terme la compra, primer anunciarà públicament les seves necessitats i convidará a un nombre d'empreses a presentar ofertes pel negoci.

  Hi ha un nombre d'avantatges en la realització del procés de contractació electrònica. Per als proveïdors significa que sovint hi ha més oportunitats de licitació, i que es redueixi el cost de presentació d'ofertes de licitació i de

col·laboració amb altres empreses. Per a les ofertes de l'empresa que ofereix hi ha una reducció important en els costos.

- **Comunitats virtuals**. Una comunitat virtual és un lloc web que ven algun producte o servei. En aquest sentit no hi ha diferència d'una botiga electrònica. La característica que distingeix una comunitat virtual és que l'operador del lloc web facilita que els clients d'un producte o un servei interactuïn entre ells, per exemple, indicant maneres de millorar un producte. Les tecnologies utilitzades per aquesta interacció inclouen llistes de correu, taulers d'anuncis i llistes de preguntes freqüents. L'objectiu de les comunitats virtuals és fidelitzar els clients i permetre a l'empresa que gestiona la pàgina web rebre una gran quantitat de comentaris sobre el producte o servei que ven. Els clients se senten atrets per les empreses associades a les comunitats virtuals. Una empresa pot obtenir beneficis de les comunitats virtuals de nombroses maneres: es pot cobrar per la participació en la comunitat o es pot beneficiar de majors vendes a clients atrets per la base de coneixements en poder de l'empresa i de la reducció de costos de suport.

- **Subministrament d'informació**. Els llocs web descrits en aquest model de negoci ofereixen accés a informació, en general informació empresarial. Per exemple, un lloc web que ofereix els resultats d'enquestes de satisfacció del client per a un producte podria ser utilitzat per les empreses que oferissin aquest producte així com per organitzacions de consumidors. Les empreses que encaixen en aquest model solen obtenir ingressos per subscribció o bé a través d'un càrrec per cada transacció d'informació.

- **Subministrament de confiança**. En aquest mòdul es tractaran diverses aplicacions segures de comerç electrònic que requeriran la interveció de terceres parts que proporcionin confiança a les diverses parts involucrades.

  Aquest model de negoci descriu aquelles empreses o organitzacions que presten algun servei relacionat amb la seguretat o la confiança. Un exemple de les funcions dels subministradors de confiança és la funció de certificació que un lloc web associat a una empresa és, realment, el lloc d'aquesta companyia.

- **Productes i serveis gratuïts**. Pot semblar paradoxal incloure els productes o serveis gratuïts en la categoria de models de negoci. Aquestes llocs no ingressen res pels productes o serveis que ofereixen; obtenen els ingressos indirectament, per exemple a través de publicitat o mitjançant la recepció dels ingressos procedents dels llocs que cal visitar abans de poder accedir abans al servei o producte.

2. Bases de seguretat per al comerç electrònic

Per a desenvolupar un sistema de comerç electrònic segur són necessaris serveis de seguretat avançats, com veurem en aquesta assignatura. Però també són serveis de seguretat que han estat objecte d'altres assignatures, i fins i tot, formen part dels coneixements bàsics necessaris per a poder cursar aquest màster.

En general se suposa que ens enfrontem amb dos possibles tipus d'atacants: passius i actius. Els atacants passius són els que poden tenir accés a la informació intercanviada entre un remitent i un destinatari, però no la poden manipular. Per contra, l'atacant actiu, a més de tenir accés al contingut de la informació, també la pot manipular: modificar, inserir nova informació, etc.

Els serveis de seguretat generalment previstos són els següents: confidencialitat, integritat, autenticitat, no-repudi i disponibilitat. L'últim servei de seguretat, molt vinculat als atacs de denegació de servei (DoS, *denial of service*), no els repassarem aquí, atès que les tècniques per a protegir-nos-en no acostumen a basar-se en tècniques criptogràfiques.

El servei de confidencialitat té per objecte protegir les comunicacions enfront d'escoltes no autoritzades, és a dir, que només els extrems autoritzats de la comunicació poden tenir accés al contingut de la informació. Protegir la informació quan estigui en trànsit no vol dir garantir al cent per cent la confidencialitat de la informació intercanviada. Els atacs d'anàlisi de trànsit permeten recuperar una informació determinada de l'intercanvi sense necessitat d'accedir al contingut de la informació. Per exemple, podem deduir que dues empreses estan negociant algun tipus de contracte, fusió, etc. del fet que intercanvien un elevat nombre de correus en un període de temps de manera anòmala. Tot i no tenir accés al contingut dels correus, podem deduir informació només observant els extrems de la comunicació.

L'objectiu del servei d'integritat és que el destinatari d'una informació podrà determinar si la informació ha estat manipulada mentre estava en trànsit. Observeu que l'objectiu fixat no és que no es pugui manipular la informació, que seria desitjable però generaria un cost molt elevat (fins i tot fregaria l'impossible), sinó que no sigui donada per bona una informació que no és exactament la que va enviar el remitent. Un cop detectada la manipulació (que la informació no és íntegra), el destinatari hauria de descartar aquesta informació i, de manera opcional, sol·licitar-ne (implícitament o explícitament) la retransmissió.

El servei d'autenticitat té per objecte que els extrems d'una comunicació puguin verificar que estan dialogant amb qui creuen estar dialogant, és a dir, que no es produeix una impersonació. Novament, la definició no pretén fer que sigui impossible aquesta impersonació, sinó que es pugui detectar per a poder actuar un cop detectada.

Finalment, tenim el servei de no-repudi, que de manera genèrica té per objectiu no permetre que una entitat que ha participat en una comunicació ho pugui negar *a posteriori*. El servei de no-repudi es pot classificar en diferents subtipus, entre els quals els més importants són el no-repudi en origen i el no-repudi en destinació. El primer no permet negar al remitent d'un missatge haver-lo enviat, i el segon no permetrà al destinatari d'un missatge haver-lo rebut. El segon servei serà objecte d'un tema d'aquesta assignatura.

Cal remarcar que si aconseguim proporcionar el servei de no-repudi en origen estem proporcionant també els serveis d'integritat i autenticitat. Si una entitat no pot negar haver emès un missatge determinat, vol dir que aquest missatge no ha estat manipulat (integritat) i que sabem qui n'ha estat l'originador (autenticitat). En cas contrari, si el missatge hagués pogut ser manipulat, o hi hagués dubtes sobre l'origen del missatge, l'emissor del missatge podria (i amb motiu) negar haver generat aquest missatge. Veurem que la inversa no és certa, és a dir, que si aconseguim els serveis d'integritat i autenticitat no necessàriament cobrim el servei de no-repudi en origen.

Mecanismes

Repassarem de manera breu els mecanismes utilitzats per a aconseguir els serveis definits anteriorment. Es tracta de la criptografia de clau secreta, la criptografia de clau pública (amb la infraestructura de clau pública que normalment comporta) i les funcions resum (o funcions *hash*).

La criptografia de clau secreta consisteix en l'aplicació d'algorismes sobre la informació que volem protegir fent servir una clau secreta que ha de ser compartida entre el remitent i el destinatari de la informació. El remitent duu a terme l'operació d'encriptació amb la clau k sobre el missatge M i obté un criptograma C:

$$C = E_k(M)$$

El destinatari ha de realitzar l'operació de desencriptació amb la mateixa clau per recuperar el missatge original:

$$D_k(C) = M$$

Amb aquest tipus de criptografia clarament obtenim el servei de confidencialitat, atès que només qui coneix la clau secreta (remitent i destinatari) pot

realitzar les operacions d'encriptació i desencriptació. Els algorismes d'encriptació i desencriptació poden ser (i en realitat han de ser) coneguts per tota la comunitat, ja que l'únic requisit que demanem és que siguin segurs (que no tinguin debilitats).

No és tan obvi, però ben utilitzats (si introduïm codis de redundància) també obtenim els serveis d'integritat i autenticitat. Un espia pot manipular la informació mentre estigui en trànsit, però com que desconeix la clau utilitzada no pot produir una informació encriptada (la que circula pel canal de comunicacions) que sigui donada per bona pel destinatari. Per tant, obtenim el servei d'integritat. D'altra banda, només remitent i destinatari poden realitzar les operacions d'encriptació amb la clau secreta *k* (només ells dos la coneixen). Si el destinatari rep una informació encriptada correctament amb la clau secreta *k*, sap que aquesta informació ha de procedir del remitent. Per tant, obtenim el servei d'autenticitat.

Tot i haver obtingut els serveis d'integritat i autenticitat, no hem obtingut el servei de no-repudi en origen. Aquesta aparent contradicció es resol pensant que el servei de no-repudi s'invoca davant de tercers, és a dir, amb el servei de no-repudi en origen volem convèncer tercers que el remitent ha enviat un determinat missatge. Mitjançant la criptografia de clau secreta no ho podem aconseguir, ja que el remitent sempre podrà negar haver enviat un missatge, i encara que el destinatari disposi d'un missatge encriptat amb la clau secreta *k* i estigui segur que l'ha enviat el remitent, aquest podrà al·legar que l'encriptació ha estat duta a terme pel destinatari, perquè també coneix l'algorisme i la clau secreta *k*.

La criptografia de clau secreta, a més de no proporcionar no-repudi en origen, ens planteja un segon problema que és el de la distribució de claus. Hem indicat que el remitent i el destinatari han de compartir una clau secreta *k*, però la qüestió és com comparteixen aquesta clau secreta. A més, per a dotar de més seguretat el sistema, aquesta clau s'ha de canviar periòdicament (cada sessió, cada missatge, etc.).

Per a resoldre els dos problemes sorgeix la criptografia de clau pública, en la qual cada usuari disposa d'un parell de claus. Una de les claus es fa servir per a dur a terme les operacions d'encriptació i desencriptació. Una de les claus ha de ser coneguda pels interlocutors del propietari del parell de clau, que denominarem clau pública, i l'altra només ha de ser coneguda pel propietari del parell de claus, que denominarem clau privada. Per simplificar l'explicació, suposarem que es poden utilitzar en qualsevol ordre (com és el cas de l'algorisme d'encriptació asimètrica RSA).

D'aquesta manera, si un remitent vol enviar una informació confidencial a un destinatari, ha de xifrar el missatge *M* amb la clau pública del destinari PU_B:

$$C = PU_B(M)$$

Només qui conegui la parella de la clau pública utilitzada podrà dur a terme l'operació de desencriptació (continuem suposant que els algorismes són públics i segurs). En aquest cas només el destinatari coneix la clau secreta PR_B, amb la qual pot realitzar l'operació de desencriptació:

$$PR_B(C) = M$$

D'aquesta manera hem aconseguit proporcionar el servei de confidencialitat, ja que només el destinatari pot recuperar el missatge M enviat pel remitent. Observeu, però, que no es proporciona el servei d'integritat i el d'autenticitat, ja que qualsevol espia que conegui la clau pública del destinatari pot produir un criptograma C', que serà donat per bo. De fet, la criptografia asimètrica o de clau pública no se sol fer servir per al servei de confidencialitat (perquè és molt costosa computacionalment), però la podrem utilitzar per a resoldre un dels dos problemes que teníem plantejats: l'intercanvi de claus de criptografia simètrica. Si canviem el missatge genèric M de l'exemple anterior per una clau secreta k, ja disposem del mecanisme perquè remitent i destinatari puguin intercanviar tantes claus secretes com vulguin:

$$K = PU_B(k)$$
$$PR_B(K) = k$$

Quedaria per resoldre ara el problema de com coneix de manera segura la clau pública del destinatari el remitent de la informació. La resposta és el que es coneix amb el nom de *certificats de clau pública*.

Tot i que hem resolt el problema de distribució de claus de la criptografia simètrica, i aconseguim el servei de confidencialitat amb la criptografia asimètrica, sembla que aconseguim menys serveis dels que ja teníem amb la criptografia anterior. Però vegem com la criptografia de clau pública ens permet aconseguir el servei de no-repudi en origen. Per a fer-ho, en comptes d'utilitzar la clau pública del destinatari, farem una encriptació amb la clau privada del remitent sobre el missatge M:

$$C = PR_A(M)$$

El destinatari (i de fet qualsevol usuari que conegui la clave pública del remitent) pot dur a terme l'operació de desencriptació:

$$PU_A(C) = M$$

I si el resultat d'aquesta operació és adequat, vol dir que el missatge procedeix del remitent, i a més no ho podrà negar *a posteriori*, ja que és l'únic usuari que coneix la clau privada PR_A que permet fer l'operació d'encriptació. Per tant, aconseguim el servei de no-repudi en origen (recordem que també aconseguim el d'integritat i el d'autenticitat), i per això se sol denominar aquest ús

de la criptografia asimètrica *servei de signatura digital* (perquè permet complir funcions anàlogues a la signatura manuscrita).

Si combinem els dos possibles usos de la criptografia asimètrica, veiem que podem aconseguir els quatre serveis de seguretat que volíem proporcionar als usuaris del sistema.

Un altre cop queda per resoldre com sap el destinatari de manera segura si PU_A és la clau pública de A o si és d'un impostor. Hem dit que la solució són els certificats de clau pública, és a dir, uns documents electrònics signats digitalment per una entitat, denominada *autoritat de certificació*, que acredita que un determinat usuari és el propietari d'una determinada clau pública (i per tant de la seva parella, la clau privada corresponent).

Ja hem indicat que la criptografia de clau pública és molt costosa computacionalment, i per aquest motiu no se sol utilitzar per a xifrar els missatges i aconseguir el servei de confidencialitat. Per aquesta raó, no seria eficient haver de xifrar tot el missatge per a aconseguir el servei de no-repudi en origen i es fan servir les funcions resum (o funcions *hash*, de l'anglès). Les funcions *hash* són funcions unidireccionals que realitzen un resum de mida fixa d'un missatge de mida arbitrària:

$$h = H(M)$$

La condició que s'imposa a aquestes funcions perquè siguin útils és que sigui computacionalment impossible trobar dos missatges que produeixin el mateix resum, però que sigui computacionalment poc costós fer una operació de resum.

Amb la introducció d'aquestes funcions *hash*, les operacions que s'han de fer per a aconseguir el servei de no-repudi en origen canviaran. Ara el primer pas que cal que faci el remitent és un resum de la informació que ha de protegir, i és sobre el resum sobre el qual fa l'operació d'encriptació amb la seva clau privada:

$$f = PR_A[H(M)]$$

Ara el remitent ha de transmetre el missatge M i la signatura f, perquè el destinari pugui verificar la correcció de la signatura digital realitzada pel remitent. D'una banda, el destinatari tornarà a realitzar un resum del missatge rebut:

$$H(M) = h'$$

I d'altra banda, desxifrarà la signatura rebuda amb la clau pública del remitent:

$$PU_A(f) = PU_A[PR_A[H(M)]] = H(M) = h$$

Si els dos resums coincideixen vol dir que la signatura digital és correcta. Si difereixen en un o més bits, significa que el missatge o la signatura, o tots dos, han estat manipulats mentre estaven en trànsit, o en qualsevol cas que la signatura no és correcta i que, per tant, no es podrà imputar aquest missatge al remitent que suposadament l'ha enviat.

El caràcter unidireccional de les funcions *hash*, a més de servir per a les signatures digitals, és útil per a les aplicacions que requereixen altres serveis de seguretat.

Per acabar aquest breu repàs de conceptes bàsics de seguretat, proporcionarem un exemple d'ús combinat de criptografia simètrica i asimètrica per als quatre serveis de seguretat plantejats. Suposarem una versió simplificada de certificat de clau pública:

$$Cert_A = A,PU_A,PR_T[H(A,PU_A)]$$

És a dir, un document electrònic signat per una autoritat de certificació T, que vincula la clau pública PU_A amb la identitat del remitent A, i amb la suposició que el destinatari de la informació coneix la clau pública de T de manera segura.

El remitent vol enviar el missatge M de manera confidencial i amb el servei de no-repudi en origen. Per fer-ho enviarà al destinatari la informació següent:

$$C = E_k(M),K = PU_B(k),f = PR_A[H(M)],Cert_A$$

Ara el destinatari ha de dur a terme les operacions següents. En primer lloc, ha de recuperar la clau que s'ha fet servir per a xifrar el missatge, per a la qual cosa ha d'aplicar la seva clau privada sobre K:

$$PR_B(K) = k$$

Un cop que disposa de la clau utilitzada pel remitent per a xifrar el missatge, pot desxifrar el criptograma rebut C:

$$D_k(C) = M$$

D'altra banda, cal que verifiqui que el certificat de clau pública del remitent és correcte, utilitzant la clau pública coneguda de l'autoritat de certificació:

$$PU_T(PR_T[H(A,PU_A)]) = H(A,PU_A)$$

Si el resum anterior coincideix amb el que el remitent ha de fer sobre la parella A i PU_A, estarà segur que PU_A és la clau pública del remitent A. Ara pot verificar la signatura feta pel remitent:

$$PU_A(f) = h'$$
$$H(M) = h$$

Si els dos resums coincideixen, el destinatari donarà per bona la signatura digital realitzada pel remitent, i podrà verificar que s'han proporcionat adequadament els serveis de seguretat requerits: confidencialitat (només ell i el remitent tenen accés al missatge M) i no-repudi en origen (el remitent no podrà negar haver enviat el missatge M).

3. Dades i xifres relatives al comerç electrònic

En aquest apartat es reflecteixen algunes dades i xifres relatives al comerç electrònic a Espanya que s'han extret, a més de les pàgines de l'ONTSI (Observatori Nacional de les Telecomunicacions i la Societat de la Informació) i de l'estudi de Market Service (*El comerç electrònic a Espanya 2011)*.

Webs de consulta

En aquest apartat farem servir dades publicades en diferents enquestes, encara que les de referència són les publicades per l'ONTSI, que podreu anar actualitzant a través de la pàgina web www.ontsi.red.es.
També podeu consultar els estudis de *Market Service* que podreu trobar i actualitzar a www.emarketservices.es.
Per a les dades relatives a Catalunya podeu consultar la pàgina web de l'IDESCAT (Institut d'Estadística de Catalunya): www.idescat.cat.

L'evolució de les dades del comerç electrònic en els darres anys són importants i esperançadores, tant pel que fa les vendes en línia que creixen a bon ritme, arribant a facturar quasi 10.000 milions d'euros, l'any 2011, com en el nombre d'internautes compradors que arriba quasi als 11 milions i en el d'empreses que s'incorporen a la Xarxa, que superen les 14.000.

A grans trets, la radiografia de l'evolució de l'estat del comerç electrònic a Espanya és determinada per aquests cinc indicadors que mostren el seu creixement. No obstant això, l'oferta espanyola encara es pot considerar escassa i per aquesta raó, com veurem més endavant, es compren més de la meitat dels béns i serveis en línia a l'exterior mentre que és molt poc significatiu el que els estrangers compren a Espanya.

comerç electrònic	2008	2009	2010	2011	Característica
Empreses: compres	20,3	24,1	23,3	22,5	% sobre el total
Empreses: vendes	11,1	13,1	12,2	14,2	% sobre el total
Particulars: compres	13,3	15,7	17,4	18,9	% sobre població total
Volum de negoci	6.695	7.760	9.114	10.000	Milions d'euros
Facturació total	9,6	11,5	11,5	13,7	% sobre el total

Tot i aquestes dades, encara s'han de superar molts reptes per a igualar-nos als nostres veïns europeus, tal com marca l'Agenda digital europea fixant, entre d'altres, els objectius següents per al 2015:

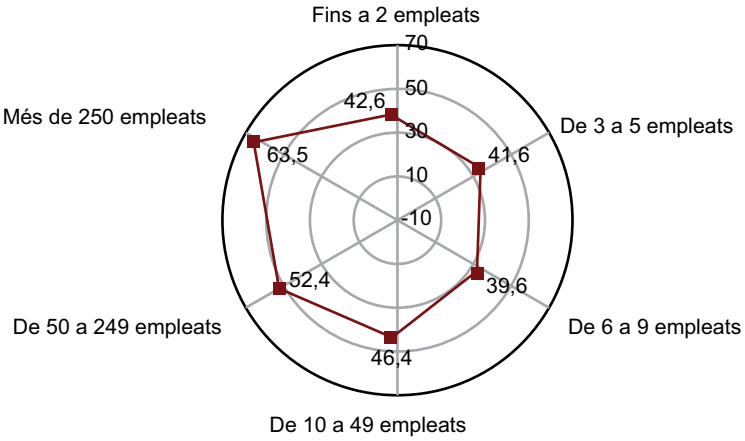
1) Comerç electrònic per a les empreses: un 33% de les pimes haurien d'efectuar compres i vendes en línia (l'any 2011, el 20% han estat compradores i un 11% venedores).

2) Promoció del comerç electrònic: un 50% de la població hauria d'efectuar compres en línia (l'any 2011 s'ha computat un 27% de la població, mentre que a la UE-27 fou d'un 47%).

3) Comerç electrònic transfronterer: un 20% de la població hauria d'efectuar compres transfrontereres en línia (l'any 2011 ha sofert un decrement respecte del 2010 i s'ha computat només un 9%).

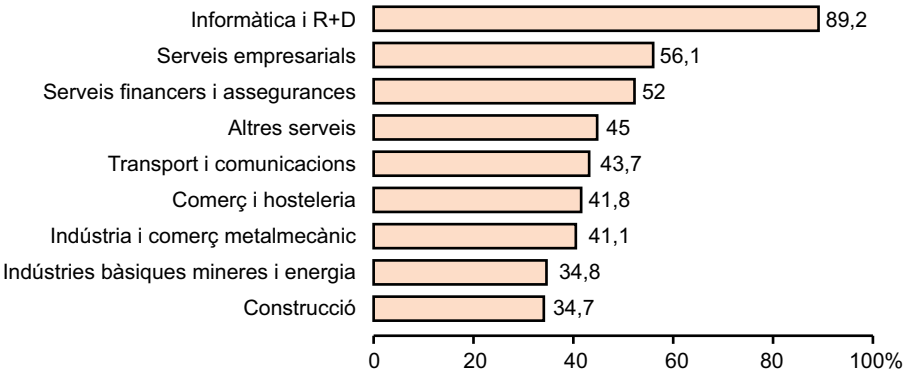
Els dos gràfics següents mostren, respectivament, el percentatge d'empreses usuàries de comerç electrònic, segons la seva grandària, i el sector d'activitat al qual pertanyen:

Empreses que utilitzen comerç electrònic segons tamany



Font: AMETIC/Everis/Red.es

Empreses que utilitzen comerç electrònic per sectors d'activitat (Percentatge/total d'empreses)



Font: AMETIC/Everis/Red.es

Ara com ara, i segons l'enquesta sobre l'ús de les TIC i el comerç electrònic a les empreses 2010/2011 de l'Institut Nacional d'Estadística (INE), el 97,4% de les empreses espanyoles, de 10 o més assalariats, disposa de connexió a Internet, i d'aquestes, un 99,4% ho fan a través de connexions de banda ampla.

Aquestes dades poden facilitar l'assoliment dels reptes de l'Agenda digital. Amb vista al futur, cal destacar el paper que desenvoluparan les xarxes socials en el comerç electrònic ja que el comprador en línia es deixa influenciar per les opinions que circulen per la Xarxa, donant-hi més crèdit inclús que a les especificacions tècniques.

Per això les empreses hauran d'utilitzar tots els mitjans tecnològics disponibles per tal de fer arribar al consumidor les seves ofertes, tenint en compte que els compradors connectats poden ser la clau de l'èxit o del fracàs del producte.

3.1. B2C: Comerç electrònic entre empreses i consumidors

Com a dades estadístiques, cal destacar que més de la meitat de les recerques prèvies a la compra es fan a través d'Internet, ja sigui per mitjà de fonts generades per la marca com les webs de fabricants i botigues, comparadors de preu o cercadors, o mitjançant fonts generades pel mateix usuari, com els blocs o les xarxes socials. D'altra banda, els productes que més es busquen a través d'Internet són els relacionats amb els viatges (78%) i els relacionats amb la telefonia mòbil (71%).

Els homes destaquen sobre les dones en l'ús de comerç electrònic; no obstant això, la bretxa entre ambdós sexes es tendeix a reduir. En tots els grups d'edat es va augmentant el percentatge de persones que fan comerç electrònic, però els qui el lideren són les persones del grup de 25 a 34 anys.

En el període 2010-2011, les transaccions de comerç electrònic des d'Espanya amb l'exterior van suposar un 52,4% del volum de negoci total (7,6% de creixement), mentre que les transaccions des de l'exterior amb Espanya van suposar un 9,2% (30,1% de creixement) i dintre d'Espanya han representat un 38,4% (0,8% de decreixement) del volum de negoci total. De les operacions transfrontereres, respecte a les quantitats gastades en el comerç electrònic interior a Espanya s'ha generat un increment del valor mitjà monetari de cada transacció, mentre que en el comerç electrònic exterior s'ha produït una caiguda d'aquest valor mitjà.

Pel que fa a les branques d'activitat més afavorides en termes de volum de negoci, el sector turístic (que comprèn transport aeri, les agències de viatge, els operadors turístics, els hotels, els apartaments i els càmpings, i el transport terrestre de viatgers) va suposar el 55,6% dels ingressos. En ordre d'importància per ingressos, li van seguir l'educació (10,3%) i les peces de vestir (4,9%). L'Administració pùblica, impostos i Seguretat Social va suposar un 3%.

3.2. B2B: Comerç electrònic entre les empreses

El comerç electrònic entre empreses continua acaparant, amb gran diferència, les vendes a Internet, amb quasi un 90%. Aquestes vendes, durant el 2011, van representar el 13,7% del total de vendes efectuades per les empreses espanyoles, superant el percentatge de 2010 que fou de 11,5%, la qual cosa reflecteix que les empreses espanyoles encara mostren certes debilitats a l'hora d'apostar per les vendes a través d'Internet.

La Unió Europea i l'Amèrica Llatina van ser les àrees geogràfiques que van comprar més béns d'Espanya. En particular, els països de la Unió Europea (UE-27) van gastar un total de 255,5 milions d'euros a través del comerç electrònic, la qual cosa va representar un 81,9% del total. L'Amèrica Llatina va ostentar el segon lloc per despesa total realitzat per via electrònica amb 14,8 milions d'euros, un 4,7% del total.

La facturació que generen les empreses deriva principalment de deu branques d'activitat:

Branca d'activitat	% sobre el volum total
Agències de viatges i operadors turístics	12,4
Transport aeri	12,2
Màrqueting directe	6,3
Transport terrestre de viatgers	6,1
Jocs d'atzar i apostes	4,9
Espectacles artístics, esportius i recreatius	4,1
Programari educatiu	3,7
Peces de vestir	3,5
Publicitat	3
Ordinadors i programari	2,4

Quant a les comunitats autònomes on més s'usa el comerç electrònic, al capdavant se situa Catalunya, en la qual el 45,6% de les empreses en fa ús. El segueix el País Basc amb un 44,9% i Andalusia amb un 44,3%.

El comerç electrònic a través del telèfon mòbil, tot i que l'ùs no està generalitzat a les empreses, es pot afirmar que es va incrementant, situant-se actualment en el 2,5%.

Pel que fa als mitjans electrònics de pagament, un 30,1% de les empreses els utilitza, de les quals un 28,5% de les entitats fa pagaments a través d'Internet, mentre que el 4,4% d'elles fa el cobrament en línia. Els pagaments a través dels mòbils encara són poc freqüents, un 0,1%; per això és important el desplegament de sistemes de pagament en línia, àgils i segurs, per tal de facilitar les compres en el comerç electrònic, en especial en els micropagaments.

Més de la meitat de les empreses que comercialitzen els seus productes a través de la Xarxa utilitza com a mitjà de cobrament electrònic girs, lletres, talons o transferències (55,8%), seguit de l'ùs de la targeta de crèdit o dèbit (43,4%). Altres alternatives com PayPal o cobraments a través del telèfon mòbil són menys utilitzades (11,6% i 1,2%, respectivament).

Els principals webs de comerç eletrònic espanyols són:

web	Contingut
e-bay	El més ampli mercat de segona mà, compra-venda i subhastes
El Corte Inglés	Centre comercial més visitat
Amazon	Una de les primeres companyies en vendre béns (llibres)
BuyVip	Club de vendes privades pertanyent a Amazon
Privalia	Venda privada de tipus generalista, però focalitzat en moda

Entre les raons del perquè s'ha de vendre per Internet, trobem en primer lloc la possibilitat de captar nous clients (37,8%), i, seguidament, el fet que proporciona més agilitat (35,4%,), el de la comoditat (30,7%) i la possibilitat d'arribar a nous mercats (26,9%).

Les empreses que compren a Internet i no venen mitjançant aquesta eina ho fan sobretot per comoditat (51,5%) mentre que per a un 40,9% el principal valor és més agilitat en la gestió i per a un 31% ho és el fet que els preus són millors. Evitar desplaçaments i trobar productes innovadors o nous proveïdors també són esmentats per les empreses que adquireixen productes a través d'Internet, encara que amb menor freqüència.

Sobre el principal fre mostrat per les empreses per a no usar el comerç electrònic, cal destacar el temor a ser objecte de robatoris i estafes, xifra refrendada pel 61% de les entitats que accedeixen a Internet. També s'al·lega, en un 26,8% dels casos, que no tots els productes són adequats per al comerç elctrònic i un 11,6% creu que necessitarien formar específicament el seu personal per a aquest tipus de mercats.

El tema de la seguretat computacional és cada vegada més important per tal de generar confiança en el món del comerç electrònic, en particular, i a Internet en general (incloent la nova versió del treball al núvol (*claude computing*)).

No deixa de ser preocupant el que revela un estudi recent del *Ponemon Institute*: que menys del 30% dels proveïdors de serveis al núvol opina que els seus serveis protegeixen i asseguren substancialment la informació del client, però menys del 50% dels usuaris consideren que la seguretat hagi de ser una prioritat.

3.3. B2A: La relació electrònica amb les administracions públiques

L'informe de l'ONTSI (*La Societat en Xarxa 2010*) assenyala que els particulars que han utilitzat Internet per a tractar amb les administracions públiques es troben a dos punts percentuals de la convergència europea (Espanya 39,2% i UE27 41,2%, essent el 50% la fita de l'Agenda digital europea per al 2015).

Espanya es troba en novena posició en el rànquing mundial de desenvolupament de l'administració electrònica, entre els 184 països analitzats en aquesta

classificació de Nacions Unides. I és que al final de 2010, el 99% dels procediments d'alt impacte de l'Administració General de l'Estat eren totalment accessibles a Internet.

Un fet d'especial rellevància és que les empreses utilitzen més la signatura electrònica per a contactar amb l'Administració pùblica (93,5%) que amb proveïdors i clients (20%).

Quant a la relació amb les empreses, continua creixent el percentatge que interacciona amb l'Administració pública per Internet, que se situa, de mitjana, en un 70,1% entre les empreses que tenen accés a Internet. El detall per grandària de les empreses reflecteix que entre les grans i les mitjanes companyies no hi ha molta diferència i en ambdós estrats es comptabilitza més d'un 90% de mitjanes i grans empreses que interactuen amb l'Administració pública a través d'Internet. En les petites, encara que el contacte telemàtic no és tan habitual, té lloc gairebé en un 67% dels casos.

El fet que siguin les administracions públiques qui promouen l'impuls de la societat de la informació a Espanya, i que també ofereixin la possibilitat de realitzar gestions administratives, fa que s'hagin constituït en les promotores de l'ús d'Internet en les seves relacions. Entre les més visitades per les empreses espanyoles, trobem la pàgina de l'Agència Tributària, en la qual el 41,2% de les empreses amb connexió a Internet hi han intereccionat, les pàgines web de les comunitats autònomes (16,3%), de la Seguretat Social (13,8%) i les pàgines pròpies dels ajuntaments (9,4%).

En la distribució geogràfica de l'ús del B2A, per comunitats autònomes, la Rioja es col·loca al capdavant amb un 76,1% de pimes i grans empreses que tenen relació amb l'Administració a través d'Internet. Després se situen Catalunya, Navarra, Madrid i Castella-Lleó, en les quals se supera el 73%.

3.4. Reptes i tendències

L'evolució del comerç electrònic a Espanya està essent desigual. D'una banda s'arriben a noves xifres rècord de facturació, i augmenta cada dia el nombre de consumidors en línia al mateix temps que augmenta la penetració d'Internet entre els particulars, tant en dispositius fixos com mòbils.

Però encara ara el principal repte és implicar les empreses en aquest canal de compra-venda, en el qual els objectius més importants són els preus competitius i la capacaitat de lliurar els béns i serveis en menys de 24 hores. Assolir aquest repte suposa educar les empreses per a atreure i retenir els potencials consumidors en línia. En particular, l'optimització de continguts, tant per a cercadors com per a xarxes socials, i la usabilitat de les pàgines de compra són encara assignatures pendents per a moltes empreses del sector.

Quant a les tendències que s'observen en el mercat, sembla clar que els dispositius mòbils seran grans aliats de les compres en línia. No només creixen les compres a través de telèfons mòbils, sinó que les tauletes comencen a despuntar com a mitjà per a fer compres en línia. De fet els propietaris d'una tauleta estan més lligats a les marques minoristes, fan més compres en línia i visiten més pàgines web que els usuaris de telèfons intel·ligents. Per això es va fent indispensable disposar d'aplicacions per als diferents dispositius mòbils i obrir el ventall de possibilitats per al consumidor i ampliar així les possibles vendes.

D'altra banda, les xarxes socials segueixen a l'alça. A Twitter i Facebook comencen a sortir solucions de comerç electrònic i botigues virtuals, al mateix temps que es van creant xarxes específicament enfocades al comerç electrònic, com ara Xopers.com, on els usuaris comparteixen articles i productes de venda a la Xarxa.

El núvol (*the cloud*) és una altra de les tendències que es poden apreciar en el sector. La facilitat d'implantació, la despreocupació per l'emmagatzematge de dades, l'escalabilitat que permet i el poder accedir des de qualsevol lloc fan d'aquestes solucions una gran ajuda al comerç electrònic (però atenció als riscos inherents a la seguretat, pel que fa la confidencialitat i l'autenticació).

Quant als mercats electrònics, la tendència és clarament cap a la introducció d'eines socials: bé creant solucions híbrides a cavall entre un mercat web (punts de trobada d'empreses compradores i/o venedores de productes i serveis) i una xarxa social, com www.grera.net, bé adaptant les noves funcionalitats que aporten al model tradicional, com va fer www.acambiode.com.

Com a conclusió, i per tot això que hem dit, és interessant prendre posicions de manera activa en aquests nous canals i aprofitar els avantatges que ofereixen.