EAPC - Gestió de la informació: transparència i protecció de dades

Les dades i la competència: l'estratègia indispensable per incidir en el capitalisme de vigilància

27-01-2023

Les empreses competeixen entre si per tal d'aconseguir que els clients potencials optin pels seus productes o serveis en detriment dels que ofereixen altres competidors.

A ningú no se li escapa que la principal variable de competència és, habitualment, el preu. No obstant això, el preu no és l'únic element en el qual els consumidors basen les seves decisions de consum; també són rellevants aspectes qualitatius, entre els quals hi ha la protecció de dades.

Ara bé, relativament pocs operadors econòmics busquen diferenciar-se de la competència mitjançant l'oferiment de productes o serveis especialment respectuosos amb la privacitat dels seus usuaris.

En termes generals, no es va més enllà de complir la regulació vigent en matèria de protecció de dades. L'oferta de serveis predominant consisteix en serveis digitals sovint oferts a un cost de 0 €, ja que el model de negoci es basa en la màxima extracció de dades per rendibilitzar-les en un altre mercat diferent (a títol d'exemple, oferir un servei de navegació a cost 0 € que assisteix en la conducció i que permet a l'oferent obtenir múltiples dades que posteriorment rendibilitza en un altre mercat com pot ser el de la publicitat). En termes econòmics, és el que s'anomena "mercat de doble cara", en què en una de les cares l'únic objectiu perseguit consisteix a extreure la màxima informació.

També hi ha un desequilibri entre la freqüència d'innovacions tecnològiques que permeten captar informació personal, fins i tot sense que el subjecte en sigui conscient –com poden ser les ulleres que poden gravar en vídeo–, i l'aparició de mesures de protecció de la privacitat. Fins ara, la tecnologia s'ha emprat més per obtenir dades que no pas per poder-nos protegir de l'extracció de dades, ja que seria factible, per exemple, que s'obligués que cada cop que algú m'intenta enregistrar mitjançant unes ulleres m'arribi un missatge al telèfon que m'alerti d'aquesta situació i que, si clico que no ho autoritzo, se n'impedeixi la gravació.

En definitiva, el model imperant sembla que és el denominat per Shoshana Zuboff "capitalisme de vigilància", de tal manera que l'oferta en termes de privacitat es podria millorar si els operadors tinguessin els incentius adients per fer-ho.

Tal com s'ha assenyalat, el principal incentiu de tota entitat és obtenir clients i, per tant, ingressos. Així doncs, el primer mecanisme que contribuiria a revertir la situació descrita té relació amb els consumidors (demanda).

1. Increment del grau de valoració de la privacitat per part de la demanda

La primera condició necessària perquè els oferents tinguin incentius per competir en la dimensió qualitativa "privacitat", consisteix que els usuaris potencials siguin sensibles sobre la privacitat i la valorin especialment.

En aquest sentit, vaig tenir ocasió d'exposar en el meu últim apunt "La protecció de dades més enllà de la intimitat" que la protecció de dades és essencial per a la protecció efectiva de tots els nostres drets com a persona fins al punt que es pot afirmar que "les teves dades són els teus drets".

Per aquest motiu és tan rellevant la **sensibilització**.

2. Reducció de l'asimetria informativa

Un segon element indispensable consisteix a assegurar que l'usuari té la informació necessària per poder efectuar la seva decisió de consum.

Imaginem que s'ofereix un mateix servei amb una doble opció: pagar 1 € i que l'oferent no recopili les nostres dades personals i no pagar però l'oferent recopila les nostres dades personals. Fins i tot assumint que l'usuari potencial és especialment sensible a la privacitat i que abonar 1 € no li comporta una despesa difícil d'assumir, podria no optar per la primera opció si no té garanties o si no pot saber realment que l'oferent no recopilarà les seves dades personals.

Per això és especialment recomanable que hi hagi **certificacions** que permetin assenyalar adequadament la qualitat en termes de privacitat. En cas que no es redueixi l'asimetria informativa, el que cal esperar és una cursa cap a baix (*race to the bottom*), ja que els oferents consideraran que l'usuari no percep aquestes millores i garanties de privacitat i probablement acabaran oferint únicament la segona opció.

3. Garantir la possibilitat d'elecció

El tercer condicionant necessari és que l'usuari sigui efectivament lliure d'escollir.

El primer pas en aquest sentit consisteix a garantir que l'usuari sempre coneix quan s'estan recopilant les seves dades. Així, tal com s'exposava més amunt, la tecnologia podria contribuir a ajudar-nos a registrar totes les peticions d'accés a la nostra informació i a poder-la gestionar de manera automatitzada, per exemple especificant una única vegada al nostre dispositiu mòbil les nostres preferències de privacitat.

No obstant això, el coneixement no és l'únic entrebanc, atès que caldria que les excepcions a la necessitat d'aconseguir el nostre consentiment fossin les mínimes indispensables per qüestions socialment imperioses (com podria ser el compliment d'una obligació legal, la protecció d'interessos vitals d'una persona, etc.). Així, l'usuari percebria amb tota claredat que gairebé sempre és ell qui controla/decideix sobre les seves dades personals; és a dir, que realment les seves preferències de privacitat tindran efectes.

Finalment, cal també que l'usuari no sigui "captiu" d'un determinat servei, ja que, suposem que es compleixen els diferents requisits exposats fins ara i que un usuari està valorant la possibilitat de canviar el servei de missatgeria instantània que utilitza actualment per un de més respectuós amb la privacitat. Si els seus contactes principals utilitzen el servei de missatgeria instantània poc respectuós amb la privacitat i no s'hi pot comunicar si no utilitza el mateix servei de missatgeria, probablement no es materialitzarà el canvi.

La captivitat també es pot produir a partir de la qualitat que es deriva de l'ús mateix de les dades, perquè les dades són un *input* essencial per millorar els productes i serveis i ho seran cada vegada més en un entorn digital en què predominarà, probablement, la intel·ligència artificial.

Així, és possible que eventualment es posi els usuaris en la dicotomia d'escollir entre consentir la recopilació de les seves dades personals i obtenir un servei amb funcions avançades (personalitzat, millorat, etc.) o bé no acceptar-la i obtenir el servei amb funcions reduïdes.

Els beneficis del processament de dades poden arribar a ser pràcticament irrenunciables i, per tant, fer que la decisió entre entregar o no les nostres dades personals no sigui lliure. L'àmbit sanitari n'és un exemple clar: sense les dades personals dels pacients difícilment poden ser tractats adequadament ni rebre un tractament específic i personalitzat.

El repte és fer possible que la protecció de dades personals no impliqui cap renúncia funcional, de manera que, novament, l'usuari sigui realment lliure de decidir entregar o no les seves dades. En aquest sentit, iniciatives com les de sherpa.ai, basades en l'aprenentatge federat que es produeix a partir de dades que mai no han de sortir del servidor del propietari, són especialment interessants.

En definitiva, la possibilitat real d'elecció exigeix, com a mínim, **coneixement**, que el **consentiment** sigui necessari en la majoria de supòsits i sense haver de sacrificar funcions (**interoperabilitat** i **processament federat**).

Ara bé, tot i que hi hagi una pressió creixent per part de la demanda en el sentit que els models de negoci versin menys sobre l'extracció de dades, cal esperar que els oferents s'hi resisteixin, atès el valor tan significatiu que els reporten les dades al llarg del temps.

Tal com s'indica en el llibre "Access Rules. Freeing data from big tech for a better future", sovint l'estratègia imperant –sobretot per part de les grans empreses tecnològiques– consisteix a obtenir el màxim volum de dades per fer-ne un avantatge competitiu pràcticament irreplicable, atès que amb les dades poden aconseguir fer productes i serveis millors que la competència. Una competència que es veurà incapacitada de competir-hi efectivament si no té accés a un elevat volum de dades.

En altres termes, les dades són una infraestructura essencial per aconseguir que hi hagi competència efectiva en el mercat, de tal manera que el regulador, comptant amb l'opinió experta de les autoritats de competència i de protecció de dades, segurament s'hauria de plantejar com garantir l'accés de tots els operadors a aquest element bàsic per poder competir efectivament en el mercat, no de la captació de la informació, sinó del de treure'n rendiment; un accés que caldria dissenyar de tal manera que es respectés el dret a la protecció de dades.

Essencialment es podria reforçar i promoure el dret a la portabilitat de les dades, així com imposar determinades obligacions de compartició de la informació (obertura de dades). En aquest escenari, seria menys transcendent estratègicament ser el primer a acumular tantes dades

com fos possible i, per tant, caldria esperar que almenys alguns dels oferents fossin més receptius a una possible demanda envers models de negoci menys intensius en extracció de dades.

En qualsevol cas, les dades i la competència constitueixen un dels reptes més rellevants de les societats actuals, tal com ha assenyalat el supervisor europeu a l'opinió 8/2016 i que va propiciar, fins i tot, la creació de la Digital Clearinghouse. Seria aconsellable una col·laboració més estreta entre les institucions vinculades a ambdós aspectes, així com amb el legislador mateix per configurar el millor entorn possible tenint en compte, entre d'altres, els aspectes assenyalats en aquest apunt.

Xavier Puig Soler

Auditor de Sistemes d'Informació de l'Autoritat Catalana de Protecció de Dades