LA PRIVACITAT A LA XARXA

Com s'utilitzen i comercialitzen les nostres dades personals a Internet.

Alumna: Gemma Pascual Manzanares
Tutora: Arantxa Uribe-Echevarria Diago

Treball de final de Grau
Grau de Comunicació
Universitat Oberta de Catalunya
Curs 2019-2020

Resum

Les nostres dades personals i, en general, gran part de la nostra vida està registrada a Internet. Quin és el tractament real de les nostres dades a la xarxa? En tenim consciència?

Pràcticament tots els nostres dispositius (telèfon mòbil, ordinador, rellotges intel·ligents, electrodomèstics intel·ligents, assistents de veu...) registren una gran quantitat d'informació personal i, sense adonar-nos-en, acceptem les condicions de privacitat d'aplicacions que diàriament utilitzem.

Arran d'això ha sorgit una nova indústria de tràfic de dades i la seva comercialització, organitzacions que controlen i s'aprofiten de les nostres dades personals per oferir-nos productes i serveis.

En aquest treball de final de grau vull demostrar, a partir de l'estudi i l'anàlisi del tractament de les nostres dades personals a Internet, si les empreses que comercialitzen amb elles ho fan d'una manera lícita i legal. El dret a la privacitat i la intimitat és un dret fonamental que sembla que cada vegada sigui menys valuós pel fet d'exposar-nos tant a la xarxa; ara bé, les organitzacions les tracten simplement amb finalitats comercials?

El Reglament General de Protecció de Dades vigent detalla tots els drets i obligacions que tenen tant les organitzacions com l'usuari a l'hora d'utilitzar les nostres dades personals. I això, ho compleixen les organitzacions d'aquesta "nova indústria"?

Aquest control i les seves possibles conseqüències crea un cert neguit social, per això també mostraré alternatives a les eines que normalment utilitzem, un conjunt d'eines que ens permeten no estar tan exposats, buscadors alternatius i aplicacions que respecten la nostra intimitat.

Paraules clau

Protecció de dades, privacitat, dades personals, comerç de dades, Big Data, Data Brokers.

Abstract

Our personal details and, in general, most of our lives are recorded on the Internet. But how is this data used on the Internet? Are we aware of this?

One is not being made fully aware when accepting the privacy conditions of the apps which are used in our every day, how much of our personal data (virtually all our devices, the cell phone, laptop, smartwatch, other smart electronic gadgets, the assistant voice virtual, etc...) can catch.

As a consequence of this, a new growing industry of data traffic and its commersalitation have arisen. These new businesses control and take advantage of our personal details to offer targeted products and services according to our customer profile.

In this thesis, I want to demonstrate, through the analysis and the study of the use of personal data on the Internet, whether the companies which sell them are treating them in a correct and legal way.

It is well known the right of privacy and confidentiality is a fundamental right. This right seems to be less important since we spend so much time on the Internet. Though, are the corporates using personal information exclusively with commercial goals?

The current General Data Protection Regulation (GDPR) details the rights and duties of the companies as the users stand when the personal data is used. But, is the "new sector" accomplishing and following them?

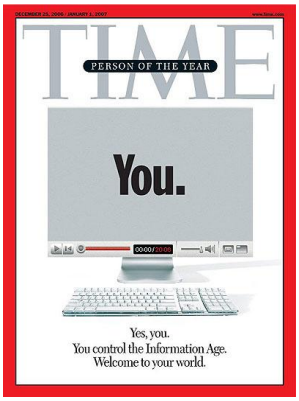
Furthermore, the fact that Internet users are more monitored over time is generating a social concern. I will provide some other options to the tools commonly used which allow us to be less present at alternative browsers and other applications that respect our privacy.

Key words

Data protection, privacy, personal data, data trade, Big Data, Data Brokers.

ÍNDEX

1. Introducció.



Time és una revista d'informació general que es publica setmanalment als Estats Units des de 1923. Cada any la revista *Time* treu un número especial titulat "persona de l'any" per reconèixer una persona, grup, idea, lloc o màquina que ha tingut una influència destacable en els successos i esdeveniments de l'any. Aquesta en va ser la portada l'any 2006: un ordinador a la pantalla del qual estava escrit: *You* (tu). Sens dubte una metàfora que podríem descriure així: malgrat la importància de les noves tecnologies en la nostra societat, la persona més important de l'any és cadascú de nosaltres. Es reivindicava així la humanització d'aquestes noves tecnologies i la importància de l'individu, al servei del qual estan.

Actualment, les grans empreses, els grans de Silicon Valley (Google, Apple, Facebook, Amazon i Twitter, coneguts com el grup GAFAT) formen un quintet, la capitalització borsària del qual supera el bilió i mig de dòlars, més que les quatre petrolieres més grans del món. I les dades que constitueixen la riquesa d'aquestes empreses estan destinades a créixer exponencialment amb els objectes connectats que ens faciliten la vida i que espien tots els nostres moviments i comportaments[1].

TIP FACE és l'algoritme de reconeixement facial de Facebook i té una precisió del 97%; molt més eficaç si el comparem amb la precisió que tenia l'FBI fa uns anys, que era del 82%. *Amazon recognation* és capaç de reconèixer més de cent persones en una sola fotografia. Per il·lustrar la importància de l'ús d'aquests algoritmes podem veure com a la SuperBowl, un dels esdeveniments anuals esportius més importants a nivell mundial, s'utilitzen drons equipats amb càmeres que estan connectats a servidors per a la vigilància en comptes de policies[2].

Amb això podem fer-nos una idea del "nou negoci" que s'està creant a partir de les nostres dades i la importància que tenen per a les grans empreses. Aquest treball consisteix en fer un estudi de com s'utilitzen i comercialitzen les nostres dades personals a Internet,

quins drets tenen les empreses per fer-los servir i quins drets tenim nosaltres mateixos.

Diàriament estem en contacte directe amb dispositius que recopilen una gran informació personal: mòbil, ordinador, rellotges intel·ligents, electrodomèstics intel·ligents, assistents de veu... i un llarg etcètera d'objectes que envien les nostres dades a on, a qui? Amb quina finalitat?

Moltes vegades no ens adonem que estem cedint les nostres dades personals de manera gratuïta, donant un consentiment per tal que es faci ús de les nostres dades de manera que aquestes empreses puguin lucrar-se. Però som conscients de les dades que estem compartint i oferint a la xarxa?

1.1. Justificació.

Com es tracten les nostres dades personals a la xarxa, què es fan amb elles, qui les vol i perquè, és un tema molt interessant i que actualment crea un cert neguit social[3]. Pensar que cada cop més estem en constant contacte amb aparells intel·ligents capaços de saber-ho pràcticament tot de nosaltres; i ho saben.

De fet, pel fet de ser un treball de final de grau de Comunicació, m'agradaria situar-lo a la base de la piràmide per saber com podem comunicar, a qui i de quina manera. És a dir, un dels punts clau per fer una bona comunicació és concretar quin és el nostre públic objectiu, i per saber-ho hem de conèixer una sèrie d'informació d'aquest target. Per exemple, ens interessarà saber on viu el nostre públic objectiu, saber si és de Barcelona, Girona, Lleida... però no que viu exactament al carrer Muntaner, 34 1r 2a, que té una nomina d'*x* al mes i una infinitat de dades que sobrepassi la privacitat i la intimitat de l'usuari. Cal tenir tanta informació personal dels usuaris?

Com que és un tema molt interessant i que, personalment, em crida molt l'atenció, vull aprofundir-hi i saber quin és el tractament real de les empreses web i d'aplicacions que es lucren amb una gran quantitat de dades personals nostres.

És un estudi que podrà ser molt útil tant per als usuaris (nosaltres mateixos) com per a les empreses que tracten amb les nostres dades

personals, perquè vegin si les tracten de la manera correcta i per fer una reflexió sobre si el que compartim i busquem a la xarxa queda registrat i si hi ha organitzacions que es lucren amb les nostres dades per oferir-nos productes i serveis a partir d'aquesta informació que els hi regalem, sovint sense adonar-nos.

1.2. Objectius.

1.2.1. Objectiu general.

Vull que aquest treball de final de grau serveixi com una mena de guia per saber a què ens exposem dia a dia quan ens descarreguem una aplicació i acceptem les seves polítiques d'ús i privacitat sense llegir-les ni fer-ne gaire cas (o gens). Quin és l'objectiu de les empreses que tenen les nostres dades i què fan amb elles, amb quina finalitat, perquè són tan valuoses i, sobretot, a nivell legal, què és el que realment poden saber i el que no de nosaltres, si hi ha alguna mena de filtre o topall per ésser controlats... en definitiva, fer un estudi de com es tracten les nostres dades a Internet.

1.2.2. Objectius específics.

- Com comuniquen les empreses del sector web i aplicacions les seves polítiques de protecció de dades i privacitat? Ho fan de la manera correcta? Respecten el reglament?
- Com a usuaris, som conscients de la gran quantitat de dades que tenen sobre nosaltres? En tenim accés?
- Qui pot fer servir les nostres dades?
- Com ens podem protegir, els usuaris? Existeixen alternatives?
- Com afecta tota aquesta nova indústria a les empreses?
- Què és el Big Data i com funciona?
- A què es dediquen els Data Brokers? Que fan amb les nostres dades? Treballen de manera segura i respectant els usuaris?

1.3. Metodologia.

La meva inspiració per fer el Treball de Final de Grau sobre el tracte de les nostres dades personals a la xarxa té el seu origen en dos documentals que vaig veure a TV3: *Big Data, Big Brother*, del programa *No pot ser!* de Jordi Basté; i *Big Data. Ciutadans sota control*, del programa *Sense ficció*. Al llarg del treball hi haurà moltes referències i cites d'aquests dos documentals.

El pla de treball per elaborar aquest TFG s'ha basat en recollir informació procedent de documentals, xerrades, conferències, lectura de llibres, articles, pàgines web i diferents entrevistes a professionals del sector. Entre aquests professionals en destacaria:

- José María Alonso Cebrián, popularment conegut com a **Chema Alonso**, és membre del Consell Executiu de Telefónica, hacker i expert en ciberseguretat espanyol.
- **Sergio González**, expert en tecnologia, actualment col·laborador a l'*Hormiguero* (Antena 3).
- **Helena Matute**, catedràtica de Psicologia Experimental a la Universitat de Deusto.
- I especialment i com a principal referent per aquest treball **Marta Peirano**, escriptora i periodista espanyola experta en tecnologia que dirigeix des de setembre de 2013 la secció cultural del diari digital eldiario.es. Va fundar CryptoParty Berlín, una iniciativa al voltant de qüestions sobre privacitat i seguretat a Internet. Va ser fundadora d'Elástico, un col·lectiu multidisciplinari amb el qual va codirigir el 2005 el projecte COPYFIGHT sobre cultura lliure. Marta Peirano porta més de vint anys al sector i és una de les grans referents d'aquest tema. He vist moltes entrevistes, conferències, ponències, articles... de Marta Peirano i m'ha ajudat i inspirat molt per fer aquest treball. El seu llibre *El enemigo conoce el sistema: Manipulación de ideas, personas e influencias después de la economía de la atención* també m'ha servit de referència i gran ajuda.

També vaig fer una **enquesta** a cent persones amb la intenció de veure i poder demostrar com es comporten els usuaris davant la cessió de dades personals i si varia segons l'edat[4]. Vaig poder comprovar que és un tema que en general importa. L'enquesta es pot

veure al final del treball a l'apartat *annex*, amb les respostes que va donar cada grup d'edat a cadascuna de les diferents preguntes. Els resultats que vaig obtenir estan representats amb gràfics que faciliten la seva comprensió i que justifiquen les conclusions que n'he tret.

Per últim, tota una bibliografia que ens proporciona una base estructural i de qualitat a l'estudi de com s'utilitzen i comercialitzen les nostres dades personals a Internet.

1.3.1. Marc teòric.

Abans de començar la lectura del treball caldrà tenir clars una sèrie de conceptes per facilitar la comprensió del que hi exposo; per tant, l'apartat de **Consideracions prèvies** serà una mena de guia amb algunes paraules clau que més endavant es tracten en profunditat.

Seguidament, al punt del **Reglament General de Protecció de Dades (RGPD)**, exposo la normativa i les lleis que han de complir les empreses que utilitzen les dades personals dels usuaris. És un apartat on explico tant els drets de les empreses com els drets que tenen els usuaris quan algú fa ús de les seves dades personals (dret d'accés, dret de rectificació, dret de suspensió...). És molt important tenir clara la normativa del que estem a punt d'analitzar, per tant, és essencial veure quin és el reglament actual.

Un cop es presenten els conceptes i la normativa vigent comença l'estudi i l'anàlisi de resultats del treball a partir d'estadístiques, llibres que he consultat, xerrades, vídeos, etc. Plantejo un treball on, a partir de tot l'estudi i els casos reals, veurem com s'utilitzen i comercialitzen les nostres dades personals a Internet, amb quins objectius, com funciona la indústria de les dades a la xarxa a partir del **Big Data**, qui són i com treballen els **Data Brokers**... a partir d'entrevistes, conferències i consultes a diferents professionals del sector.

2. Consideracions prèvies.

TIC: Diem tecnologies de la informació i la comunicació al conjunt de tecnologies que permeten l'adquisició, producció, emmagatzematge i tractament de comunicació, registre i presentació d'informacions amb veu, imatges i dades en senyals de naturalesa acústica, òptica o electromagnètica. Les TIC inclouen l'electrònica com la tecnologia base que suporta el desenvolupament de les telecomunicacions, la informàtica i l'audiovisual[5].

Intel·ligència artificial: La intel·ligència artificial és el camp científic de la informàtica que es centra en la creació de programes i mecanismes que poden mostrar comportaments considerats intel·ligents. La intel·ligència artificial (IA) és el concepte segons el qual les màquines pensen com els éssers humans i serveix per acumular característiques i capacitats que tradicionalment només estaven lligades a d'intel·lecte humà[6].

Dades: Una dada és una representació simbòlica (numèrica, alfabètica, algorítmica, espacial, etc.) d'un atribut o variable quantitativa o qualitativa. Les dades descriuen fets empírics, successos i entitats. És un valor o referent que es rep per diferents mitjans, els valors representen la informació que el programa manipula en la construcció d'una solució en el desenvolupament d'un algoritme[7].

Algoritme: Un algoritme és un conjunt finit d'instruccions o passos que serveixen per a executar una tasca o resoldre un problema. És una seqüència finita d'instruccions realitzables, no ambigües, l'execució de les quals condueix a una resolució d'un problema. Aquesta definició es pot generalitzar des del punt de vista sistèmic, si se se suposa que l'algorisme pot ser dissenyat per rebre i aprofitar una determinada entrada donant com a resultat una sortida, que pot resoldre un problema determinat[8].

Hacker: Un *hacker* és una persona que pels seus avançats coneixements en l'àrea de la informàtica té un gran desenvolupament i és capaç de realitzar moltes activitats desafiants i il·lícites des d'un ordinador. Un *hacker* en plenitud té la capacitat de dominar en un bon percentatge aspectes com el llenguatge de programació, manipulació de *hadware* i *software*, telecomunicacions... per lucrar-

se, donar-se a conèixer, per motivació o simplement com a passatemps[9].

Identificació biomètrica: és una tècnica per identificar individus mitjançant mesures biomètriques; en biologia, és el conjunt de tècniques científiques de mesura i el seu tractament matemàtic i o bioestadística per mesurar paràmetres d'éssers vius. Per poder identificar una persona mitjançant un sistema de seguretat s'han de comparar les seves característiques amb una base de dades, per fer això s'extrauen uns punts biomètrics i es mesuren les distàncies entre ells per tal de reconèixer les característiques biomètriques de la persona a identificar. El reconeixement de persones per a sistemes de seguretat mitjançant càmeres s'ha convertit en aquests darrers anys una de les formes més comunes de reconeixement. Per poder arribar a fer una identificació exitosa s'hauria de tenir una base de dades amb moltes imatges de l'individu i anar-les comparant una a una, i aquestes amb totes les possibles identificacions. Això seria molt costós, és per això que es busquen les característiques biomètriques que diferencien a cada persona i es busquen uns punts per a poder fer la identificació[10].

Públic objectiu/target: El públic objectiu (o target) són aquells clients potencials que volem que consumeixin els nostres productes o contractin els nostres serveis. És aquell grup de persones o empreses tipus que una companyia ha de prendre com a referència a l'hora d'elaborar les seves estratègies de màrqueting[11].

ID: En aquest treball es farà referència a l'ID com a l'usuari; persona que utilitza o treballa amb un sistema, producte o servei; públic, privat, empresarial o professional; en qualsevol moment del seu cicle de vida (disseny, fabricació, transport, utilització, residu)[12].

Segmentació: La segmentació de mercat és el procés de dividir un mercat en grups uniformes més petits que tinguin característiques i necessitats semblants. Això no està arbitràriament impost sinó que es deriva del reconeixement que el total de mercat està fet de subgrups anomenats segments. Aquests segments són grups homogenis[13].

Identitat digital: És tota la informació que hi ha publicada a Internet sobre una determinada persona. Són dades que poden haver estat publicades per la pròpia persona i també dades que poden haver acabat a la xarxa per causes alienes: les ha publicat una altra

persona, un diari, una escola... Es pot obtenir una gran quantitat d'informació d'una persona realitzant unes simples consultes a un buscador[14].

Smart: Tot el que anomenem *smart* són dispositius que es dediquen a l'extracció deliberada, massiva i persistent de dades; no solament dels seus usuaris sinó que, en general, dels ciutadans, ja que en un moment donat, tot i que sembli obvi, podem deixar de ser usuaris però no ciutadans.

Cookie: Un bescuit, galeta o cookie és un fragment d'informació enviat des d'un servidor de pàgines web a un navegador que pot ésser retornada pel navegador en posteriors accessos a aquest servidor. El navegador guarda aquesta informació en forma d'arxiu de text al disc dur del visitant de la pàgina web per tal que certes informacions puguin ser recuperades en posteriors visites. Els usos més freqüents són: guardar el nom d'usuari i contrasenya per evitar tornar-ho a introduir, mantenir un seguiment de les compres en una botiga virtual, utilitzar opcions de continguts o disseny escollides anteriorment, obtenir informació sobre els hàbits de navegació de l'usuari i obtenir informació de l'ordinador del visitant, com l'adreça IP, sistema operatiu o tipus de navegador[15].

3. Reglament General de Protecció de Dades (RGPD).

Molts dels objectes que ens envolten en el nostre dia a dia són aparells intel·ligents. Tot està connectat a Internet, que recull les nostres dades i les envia no sabem on, ni perquè. El telèfon mòbil és el dispositiu utilitzat amb major freqüència per accedir a Internet: un 90,1% dels usuaris el fan servir per connectar-se, seguit de l'ordinador portàtil amb un 68,7%, i l'ordinador de sobretaula amb el 55,9%. Per sota trobem que accedeixen amb la tablet el 47,7% dels usuaris i molt per sota, un 27,1%, a través de la televisió, la consola de sobretaula, els rellotges intel·ligents, la consola portàtil i, per últim, els assistents de veu intel·ligents[16].

Albert Agustinoy, soci responsable de l'àrea de propietat intel·lectual i noves tecnologies del bufet Cuatrecasas, explica[17] que aquesta *hiperconnectivitat* podria convertir-se en "la responsable de que perdem el control de qui recull i amb quina finalitat les nostres dades".

Primer de tot hem de tenir clar què són i a què ens referim quan parlem de les nostres dades personals. Entenem per dades personals qualsevol informació relacionada amb una persona física viva, identificada o identificable, incloent-hi el seu nom, fotografia, correu, adreça, dades bancàries, publicacions a les xarxes socials, informació mèdica, dades biomètriques i la seva orientació sexual.

L'article 4 del RGPD ho defineix com "tota informació sobre una persona física identificada o no identificable (la informació interessant). Es considerarà persona física identificable tota persona que la seva identitat es pugui determinar, directament o indirectament, en particular mitjançant un identificador com, per exemple, un nom, un número d'identificació, dades de localització, un identificador en línia o un o més elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona".

Al desembre de 2018 va entrar en vigor la nova Llei Orgànica 3/2018 de Protecció de Dades i Garantia dels Drets Digitals (LOPDGDD). El

seu principal objectiu és adaptar la llei espanyola a la normativa europea, definida pel RGPD. La finalitat de la LOPDGDD és protegir la intimitat, privacitat i integritat de l'individu, complint amb l'article 18.4 de la Constitució Espanyola.

L'Agència Espanyola de Protecció de Dades (AEPD) ha creat una *Guia del ciutadà*[18] que recull tota la informació necessària amb la finalitat que els ciutadans estiguin ben informats dels seus drets en relació amb el tractament dels seus drets personals, l'assessorament davant denúncies i reclamacions, i qualsevol altra qüestió en relació amb aquests drets.

Aquesta nova llei presentava unes importants modificacions[19], evidentment adaptades al temps actual on les noves tecnologies juguen un paper protagonista en la gestió de les nostres dades personals. Entre tots els canvis i modificacions les més rellevants són:

- **Legitimació de les administracions públiques per a l'ús i cessió de les dades personals.**

L'article 6 del RGPD estableix les bases de legitimació per al tractament de les dades de caràcter personal, de les quals dues serveixen per la utilització (i cessió) de les dades de caràcter personal per part de l'Administració Pública: quan el tractament respongui a una obligació legal i quan aquest sigui necessari per al compliment d'una missió realitzada en l'interès públic o en l'exercici de poders públics. La LOPDGDD introdueix un nou article 8 on aclareix quan es pot considerar el tractament en el compliment d'una obligació legal: "quan així ho prevegi una norma de Dret de la Unió Europea o una norma de la Llei", les quals podran determinar les condicions generals del tractament, els tipus de dades objecte del mateix, les cessions que procedeixin i imposin condicions especials al tractament.

- **Delegat de Protecció de Dades.**

La LOPDGDD amplia els suposats en els que s'obligui la designació d'un Delegat de Protecció de Dades i estableix que es tindran especialment en compte l'obtenció d'una titulació universitària que acrediti coneixement especialitzats en dret i la pràctica en matèria de protecció de dades. També es reconeix el paper del DPD com l'òrgan

intermediari de control pel que l'afectat podrà, prèviament presentant una reclamació, dirigir-se al DPD de l'entitat contra la que es reclami.

- **Xarxes socials.**

Les xarxes socials actualment tenen un gran paper en la nostra vida quotidiana per això cal una regularització. S'introdueix l'article 94 de la LOPDGDD relatiu al "Dret a l'oblit en serveis de xarxes socials i serveis equivalents", recollint el dret de tota persona a que siguin suprimits, amb una simple sol·licitud.

- **Protecció de Dades a persones mortes.**

S'incorpora l'article 3 que contempla que les persones vinculades al mort per raons familiars o de dret, així com els seus hereus, podran dirigir-se al responsable o encarregat per a sol·licitar l'accés, rectificació o supressió, amb l'excepció de que el difunt ho hagués prohibit expressament o que així ho estableixi la llei.

- **Regim jurídic dels empleats.**

Es modifiquen les dues normes bàsiques que regulen les relacions laborals: el text refós de la Llei de l'Estatut dels Treballadors relatiu al seu dret a la intimitat en relació amb l'entorn digital i la desconnexió i la Llei de l'Estatut Bàsic de l'Empleat Públic. Ambdós casos, recull el dret a la intimitat en l'ús de dispositius digitals posades a disposició i davant de l'ús de dispositius de vídeo vigilància i geolocalització. Així com la desconnexió digital: els treballadors i empleats públics tindran dret a la desconnexió digital amb la finalitat de garantir, fora del temps de treball legal o establert, el respecte del seu temps de descans, permisos i vacances, així com la seva intimitat familiar i personal.

- **Importants modificacions de normes.**

S'introdueixen modificacions a les següents normes rellevants:

- Llei Orgànica del Poder Judicial.
- Llei del Procediment Administratiu Comú.
- Llei de Transparència, Accés a la Informació Pública i de Bon Govern.
- Llei Orgànica del Règim Electoral General.
- Llei General de Sanitat.

- Llei reguladora de la Jurisdicció Contenciosa-administrativa.
- Llei d'Enjudiciament Civil.
- Llei Orgànica de les Universitats.
- Llei bàsica reguladora de l'autonomia del pacient i de drets i obligacions en material d'informació i documentació clínica.
- Llei Orgànica d'Educació.

- **L'ús de les nostres dades per als partits polítics.**

L'article 25 bis a la Llei Orgànica del Règim Electoral General, relatiu a "l'ús de mitjans tecnològics i dades personals en les activitats electorals". Aquesta modificació ja provocat inclús la pronuncia de l'Agència Espanyola de Protecció de Dades ja que permet la recopilació de dades personals relatives a les opinions polítiques de les persones per part dels partits polítics en el marc de les seves activitats electorals.

3.1. Els drets de les empreses.

La normativa de protecció de dades obliga a les empreses i les autoritats a garantir la protecció de la informació dels seus usuaris i clients. El RGPD[20] estableix complir els següents principis i pràctiques:

- **Legalitat del tractament de dades**: la recollida, emmagatzematge, ús i transmissions de dades personals a tercers. Només està permès amb l'exprés consentiment de l'interessat.
- **Transparència**: les empreses i autoritats públiques estan subjectes a un rendiment de comptes, documentació i proves. Hauran d'informar sobre tots els procediments de tractament de dades personals quan l'interessat ho sol·liciti.
- **Ús limitat**: l'ús de dades haurà d'estar restringit a objectius específics i no ser arbitrari.
- **Minimització de dades**: totes les organitzacions estan obligades a recollir només les dades que siguin estrictament necessàries per al compliment dels seus objectius i garantir que el volum d'informació emmagatzemada estigui el més minimitzada possible.
- **Correcció del processament de dades**: les dades emmagatzemades sempre han d'estar correctament i estar actualitzades sempre que sigui necessari.

- **Limitació d'emmagatzematge**: existeix una obligació d'eliminar dades amb regularitat i des del moment en que ja no sigui necessari per als objectius d'una organització, si s'han emmagatzemat il·legalment o si ha expirat un període predeterminat per concedir aquestes dades.
- **Integritat i confidencialitat**: les empreses i autoritats han de prendre amplies mesures per a la protecció interna de dades personals. A més de l'ús de programes d'encriptació i software de seguretat, això també inclou la formació detallada dels treballadors encarregats del processament de dades.

L'article 83, apartat 5 del RGPD estableix que la violació d'aquests principis pot donar lloc a una multa de fins a 20 milions d'euros o fins al 4% del volum de negocis anual global. Aquesta norma també ofereix un incentiu financer per empènyer a complir les seves directrius, però segueix sense poder garantir la seguretat absoluta de les dades personals. Per això, és una responsabilitat dels consumidors protegir la seva privacitat per iniciativa pròpia.

3.2. Els nostres drets com usuaris.

Fins ara hem vist quins són els drets de les empreses envers les nostres dades personals, ara bé, quins són els drets que tenim nosaltres mateixos sobre les dades que hem cedit?

La normativa de protecció de dades[21] permet que es pugui exercir davant el responsable del tractament els teus propis drets d'accés, rectificació, oposició, supressió (dret a l'oblit), limitació del tractament, portabilitat i de no ser objecte de decisions individualitzades.

Són uns drets que es caracteritzen per:

- El seu exercici és gratuït.
- Si les sol·licituds són infundades o excessives (de caràcter repetitiu) el responsable podrà:
  - Cobrar un cànon proporcional als costos administratius suportats.
  - Negar-se a actuar.
- Les sol·licituds s'han de respondre en un termini d'un mes.
- El responsable està obligat a informar-se sobre els mitjans per exercir aquests drets. Els mitjans han d'ésser accessibles i no es pot denegar aquest dret.

- Si la sol·licitud es presenta per mitjans electrònics, la informació es facilitarà per aquests mitjans quan sigui possible, excepte que l'interessat sol·liciti que sigui diferent.
- Si el responsable cursa la sol·licitud, informarà al cap d'un mes, de les raons de la no-actuació i la possibilitat de reclamar davant una Autoritat de Control.
- Es poden exercir els drets directament o per mitjà del teu representant legal o voluntari.
- Hi cap la possibilitat de que l'encarregat sigui qui atengui la sol·licitud per compte del responsable si ambdues parts ho han establert al contracte o acte jurídic que els vinculi.

3.2.1. Dret d'accés.

El dret d'accés és el dret a poder-te dirigir al responsable del tractament per conèixer si està tractant o no les teves dades de caràcter personal i, en el cas de que s'estigui realitzant aquest tractament, obtenir la següent informació:

- Un còpia de les teves dades personals que són objecte del tractament.
- Els fins del tractament.
- Les categories de dades personals que es tracten.
- Els destinataris o les categories de destinataris als que se li comuniquen o seran comunicades les dades personals, en particular, els destinataris a països tercers o organitzacions internacionals.
- El termini previst de conservació de les dades personals, o si no es possible, els criteris utilitzats per determinar aquest termini.
- L'existència dels drets de l'interessat a sol·licitar al responsable: la rectificació o supressió de les seves dades personals, la limitació del tractament de les seves dades personals o oposar-se a aquest tractament.
- El dret a presentar una reclamació davant una Autoritat de Control.
- Quan les dades personals no s'hagin obtingut directament de tu, qualsevol informació disponible sobre el seu origen.
- L'existència de decisions automatitzades, inclosa l'elaboració de perfils, i al menys davant d'aquests casos, informació significativa sobre la lògica aplicada, la importància i les conseqüències previstes del tractament per a l'interessat.
- Quan es transfereixin dades personals a un tercer país o a una organització internacional, tens dret a ser informat de les garanties adequades en les que es realitzaran les transferències.

3.2.2. Dret de rectificació.

L'exercici d'aquest dret suposa que es podrà obtenir la rectificació de les pròpies dades personals que siguin inexactes sense dilació indeguda del responsable del tractament.

Tenint en compte el fins del tractament, es te dret a que es completin les dades personals que siguin incomplertes, incloses mitjançant una declaració addicional.

A la sol·licitud s'haurà d'indicar a quines dades es fa referència i la correcció que s'ha de fer. A més, quan sigui necessari, s'haurà d'acompanyar la sol·licitud de la documentació que justifiqui la inexactitud o el caràcter incomplert de les teves dades.

3.2.3. Dret d'oposició.

Aquest dret, com el seu nom indica, suposa que et pots oposar a que el responsable realitzi un tractament de les dades personals a les següents suposicions:

Quan siguin objecte de tractament basat en una missió d'interès públic o en l' interès legítim, inclosa l'elaboració de perfils:

- El responsable haurà de tractar les dades a no ser que s'acreditin motius imperiosos que prevalguin sobre els interessos, drets i llibertats de l'interessat, o per a la formulació, l'exercici o la defensa de reclamacions.

Quan el tractament tingui com a finalitat el màrqueting directe, inclosa també l'elaboració de perfils anteriorment citada:

- Exercint aquest dret per aquesta finalitat, les dades personals deixaran de ser tractades per aquests fins.

3.2.4. Dret de suspensió.

Es podrà exercir aquest dret davant el responsable sol·licitant la supressió de dades de caràcter personal quan concorri alguna de les següents circumstàncies:

- Si les dades personals ja no són necessàries en relació amb les finalitats per a les que van ser recollides o tractades.

- Si el tractament de les dades personals s'ha basat en el consentiment que es va prestar al responsable, i es retira, sempre que el citat tractament no es basi en una altra causa que ho legitimi.
- Si t'has oposat al tractament de les teves dades personals al exercitar el dret d'oposicions en els següents casos:
    - El tractament del responsable es fonaments en l'interès, legítim o en el compliment d'una missió d'interès públic, i no han prevalgut altres motius per legitimar el tractament de les dades.
    - A que les teves dades personals siguin objecte de màrqueting directe, incloent l'elaboració de perfils relacionats.
- Si les dades personals han sigut tractament il·lícitament.
- Si les dades personals s'han de suprimir pel compliment d'una obligació legal establerta al Dret de la Unió o dels Estats membres que s'apliquin al responsable del tractament.
- Si els drets personals s'han obtingut en relació amb l'oferta dels serveis de la societat de la informació mencionats a l'article 8, apartat 1 (condicions aplicables al tractament de dades dels menors en relació amb els serveis de la societat de la informació).

3.2.5. Dret a la limitació del tractament.

Consisteix en obtenir la limitació del tractament de les dades que realitza el responsable. L'exercici presenta dues vessants:

Es pot sol·licitar la suspensió del tractament de les dades:

- Quan s'impugni la exactitud de les dades personals, durant un termini que permeti al responsable la seva verificació.
- Quan s'hagi oposat al tractament de les dades personal que el responsable realitza en base a l'interès legítim o missió d'interès públic, mentre es verifica si aquests motius prevalen sobre els teus.

Sol·licitar al responsable la conservació de les pròpies dades:

- Quan el tractament sigui il·lícit i t'hagis oposat a la supressió de les dades i es sol·licita la limitació del seu ús.
- Quan el responsable ja no necessiti les dades personals per als fins del tractament, però l'interessat els necessiti per a la formulació, l'exercici o la defensa de reclamacions.

3.2.6. Dret a la portabilitat.

La finalitat d'aquest dret és reforçar encara més el control de les dades personals, de forma que quan el tractament s'efectuï per mitjans automatitzats, rebràs les teves dades personals en un format estructurat, d'ús comú, de lectura mecànica i interoperable, i podràs transmetre'ls a un altre responsable del tractament, sempre que el tractament es legitimi en base al consentiment o al marc de l'execució d'un contracte.

Tot i això, aquest dret, per la seva pròpia naturalesa, no es pot aplicar quan el tractament sigui necessari per al compliment d'una missió d'interès públic o a l'exercici de poders públics conferits al responsable.

3.2.7. Dret a no ser objecte de decisions individuals automatitzades.

Aquest dret pretén garantir que no siguis objecte d'una decisió basada únicament en el tractament de les teves dades, inclosa l'elaboració de perfils, que produeixi efectes jurídics sobre tu o t'afecti significativament de forma similar.

Sobre aquesta elaboració de perfils, es tracta de qualsevol forma de tractament de les teves dades personals que avaluï aspectes personals, en particular analitzar o predir aspectes relacions amb el teu rendiment a la feina, situació econòmica, salut, les preferències o interessos personals, fiabilitat o el comportament.

No obstant, aquest dret no serà aplicable quan:

- Sigui necessari per la celebració o execució d'un contracte entre tu i el responsable.
- El tractament de les dades es fonamenti en el teu consentiment prèviament prestat.

En aquest dos primers casos, el responsable ha de garantir el teu dret a obtenir la intervenció humana, expressar el teu punt de vista i impugnar la decisió.

- Aquest autoritzat pel Dret de la Unió o dels Estats membres i s'estableixin mesures adequades per salvaguardar els drets i llibertats i interessos legítims de l'interessat.

Aquestes excepcions no s'aplicaran sobre les categories especials de dades (art. 9.1), a no ser que s'apliqui l'article 9.2 lletra a) o g) i s'hagin pres les mesures adequades citades anteriorment.

3.2.8. Dret d'informació.

Quan es recullen les teves dades de caràcter personal, el responsable del tractament ha de complir amb el dret de la informació.

Per al compliment d'aquest dret, l'AEPD recomana que aquesta informació se't faciliti per capes o nivells de manera que:

- Se't faciliti una informació bàsica en un primer nivell, de forma resumida, al mateix moment i al mateix mitjà en que es recullen les dades personals.
- Se't remeti la resta d'informacions, en un mitjà més adequat per a la seva presentació, compressió i, si es desitja, arxiu.

La informació a facilitar per capes o nivells és:

- 1a Capa: informació bàsica (resumida):
  - La identitat del responsable del tractament.
  - Una descripció senzilla de les finalitats del tractament, inclosa l'elaboració de perfils existents.
  - La base jurídica del tractament.
  - Previsió o no de cessions. Previsió o no de transferències a tercers països.
  - Referència a l'exercici de drets.
- 2a Capa: informació addicional (detallada):
  - Dades de contacte del responsable. Identitat i dades del representant (si existeix). Dades de contacte del delegat de protecció de dades (si existeix).
  - Descripció ampliada dels fins del tractament. Terminis o criteris de conservació de les dades. Decisions automatitzades, perfils i lògica aplicada.
  - Detall de la base jurídica del tractament, en els casos d'obligació legal, interès públic o interès legítim. Obligació o no de facilitar dades i conseqüències de no fer-ho.
  - Destinataris o categories de destinataris. Decisions d'adequació, garanties, normes corporatives vinculants o situacions específiques aplicables.
  - Com exercir els drets d'accés, rectificació, supressió i portabilitat de les dades, i la limitació o oposició al seu

tractament. Dret a retirar el consentiment prestat. Dret a reclamar davant l'Autoritat de Control.

Suposant que hi hagi dades personals que no hagin estat obtingudes directament de tu, se't facilitarà, a més de la informació indicada anteriorment:

A la informació bàsica (1a capa, resumida):

- La font (procedència) de les dades.

I a la informació addicional (2a capa, detallada):

- La informació detallada de l'origen de les dades, inclús si procedeixen de fonts d'accés públic.
- La categoria de dades que es tracten.

Aquesta informació es facilita dins d'uns terminis raonables, com a màxim un mes, a no ser que:

- Si les dades personals s'han d'usar per a una comunicació amb l'afectat, com a molt en el moment de la primera comunicació amb aquest afectat.
- Si està previst comunicar-lo a un altre interessat, com a molt en el moment en que les dades personals siguin comunicades per primer cop.

3.2.9. Dret Schengen.

El Sistema d'Informació de Schengen (SIS) és un sistema d'informació a gran escala que facilita la cooperació entre les autoritats nacionals de control de fronteres, duanes i policia al denominat Àrea Schengen.

Com a complement al sistema d'informació SIS, hi ha el sistema d'informació de visats (VIS) que permet a les autoritats competents la implementació de la política comú de vises sobre els visats de curta durada (fins a 90 dies).

La normativa que regula el sistema VIS reconeix el dret dels ciutadans afectats a l'exercici dels drets d'accés, rectificació i supressió, així com determinades limitacions als mateixos.

4. Big Data.

A Holanda, l'any 1941, tenien un cens[22] on incloïen les religions dels ciutadans amb la intenció de saber quants catòlics hi havia, quants protestants, quants jueus... per saber com havien de repartir el pressupost de cada comunitat a cada església o sinagoga. Quan van arribar els nazis, gràcies a aquest cens (el que podríem dir avui dia una base de dades), ja es van trobar la feina feta i només el 10% dels jueus holandesos va sobreviure a la Segona Guerra Mundial. Amb aquest exemple veiem que compartir les nostres dades ens fa vulnerables i l'únic que pot evitar posar-hi fre som nosaltres mateixos.

Actualment la Xina està desenvolupant el major sistema de vigilància conegut al món, amb una indústria del reconeixement facial que és capaç d'identificar persones que ni tan sols s'hagin connectat a Internet[23]. Tenen entre 4 i 6 milions de càmeres que vigilen els seus ciutadans, els quals representen un 20% de la població mundial.

És a dir, 1.200 milions de persones són vigilades constantment per càmeres instal·lades pràcticament arreu de les ciutats connectades als servidors que disposen de sistemes de reconeixement facial i que estan gestionades per les tres grans empreses xineses del sector: Alibaba, Tencent i Baidu. A més, als Estats Units, es fan servir aquestes dades per localitzar els immigrants i refugiats i així poder separar-los dels seus fills i tancar-los.

El terme Big Data fa referència a tot un conjunt de dades o combinacions de conjunt de dades que el seu volum, complexitat i velocitat de creixement dificulten la seva captura, gestió, processament o anàlisi mitjançant tecnologies i eines convencionals,

com les bases de dades relacionades i estadístiques convencionals, dins del temps necessari perquè siguin útils.

El Big Data és tan útil per a les empreses perquè proporcionen un punt de referència amb una gran quantitat d'informació i dades que poden capacitar a les organitzacions per identificar els problemes dels usuaris.

Quan parlem del Big Data no ens referim només a les dades sinó sobretot a la capacitat de poder-les explotar per extreure informació i coneixement de valor per a les organitzacions. La seva finalitat és poder dissenyar nous productes i serveis sobre la competència o en general el mercat actual.

Vicenç Aguilera, auditor en seguretat informàtica, ha fet la prova de descarregar una aplicació d'un joc de trens per a nens aparentment inofensiva. A través del seu ordinador, amb un programa a l'abast de tothom, ens mostra que aquesta aplicació pot recopilar molta informació de l'usuari, la qual descarrega a l'aplicació. Ràpidament genera una gran quantitat de dades i no només es connecta a l'empresa que ha desenvolupat aquest joc sinó que es connecta a altres servidors que els hi proporciona, entre d'altres, quines altres aplicacions tenen els usuaris instal·lades al dispositiu, quina és la seva ubicació... i pot accedir a una gran quantitat de dades que, a priori, no haurien d'estar relacionades amb un joc infantil[24].

La majoria d'experts[25] defineixen el Big Data en termes de les cinc "v":

- Volum: la gran quantitat de dades que pot arribar a recollir.
- Velocitat: l'alt ritme en què es generen les dades sol augmentar constantment i necessita una resposta a temps real per part de les empreses.
- Varietat: trobem dades en diferents formats; des de texts senzills, imatges, vídeos, fulls de càlcul fins a bases de dades senceres.
- Veracitat: han de ser dades fiables i reals. Si unes dades són incorrectes no tenen cap valor i, a més, poder ser altament perjudicials.
- Valor: Aquestes dades amb l'anàlisi corresponent han de generar un benefici per a les empreses.

Per poder classificar aquestes grans dades ho fem segons la seva procedència i la seva estructura. Segons la seva procedència, les dades poden arribar per:

- Web i xarxes socials: informació disponible a Internet com a contingut web. El que generen els usuaris amb la seva activitat a la xarxa.
- Machine-to-machine (M2M): dades generades a partir de la comunicació entre sensors intel·ligent a traves d'objectes d'ús quotidià (rellotges, assistents de veu, electrodomèstics intel·ligents...).
- Transaccions: registres de facturació, de comptes o trucades.
- Biomètrics: dades generades per tecnologia d'identificació per reconeixement facial, empremtes dactilars o informació genètica.
- Per persones: a través del correu electrònic, missatgeria o gravació de trucades.
- Per organitzacions tant públiques com privades: dades relacionades amb el medi ambient, estadístiques governamentals de població i economia, historials clínics...

I segons la seva estructura, aquestes dades poden ser:

- Estructurades: dades que tenen definits el seu format, mida i longitud.
- Semi estructurades: dades emmagatzemades segons una certa estructura flexible i amb unes metadades definides (XML y HTML, JSON, i els fulls de càlcul).
- No estructurades: dades sense format específic, com fitxers de text o contingut multimèdia (fotografies, vídeos i àudios).

Grans empreses d'Internet com Google i Facebook recopilen dades personals dels usuaris, tot i que en la majoria dels casos ho fan servir per fer publicitat individualitzada i així generar beneficis econòmics.

El Big Data no és només un factor competitiu, és el factor considerat més important per part de la majoria de les empreses presents al mercat. Segons un estudi publicat per Accenture[26], el 67% dels executius de grans empreses consideren que el Big Data és extremadament important, mentre que els de les petites empreses només ho considera un 43%. Els executius de grans empreses tenen una percepció del Big Data més àmplia que la de les empreses petites i utilitzen més fonts de dades en les seves iniciatives de Big Data, com a les xarxes socials, dades de visualització o dades sense

estructura. El 62% dels executius de grans empreses afirmen que els alts directius comprenen i recolzen les iniciatives del Big Data mentre que a les empreses petites ho recolzen un 42% dels entrevistats.

Tot i això, els executius confessen que les principals barreres que han hagut de superar les seves organitzacions en l'adopció del Big Data són la seguretat, les limitacions pressupostàries, la falta d'experts en el sector i l'ús continuat de Big Data i analítica i la integració en els sistemes ja existents.

El mateix estudi també va poder corroborar que un 67% dels executius de grans empreses de 19 països diferents considera que el Big Data representa un dels aspectes més importants de la transformació digital.

A la conferència *¿Por qué me vigilan si no soy nadie?*[27] que va donar Marta Peirano al TEDxMadrid al 2015 explica que "no ens comportem igual quan sabem que ens estan vigilant; la millor manera de vigilar a una població és que no sàpiguen quan se'ls està vigilant".

Simplement amb el que portem al nostre moneder ja estem donant pràcticament tota la nostra vida en dades: el DNI, el carnet de conduir, la targeta bancària, la targeta del transport públic, les targetes de fidelització dels supermercats... A vegades, sense parar-hi importància, fins i tot les targetes de fidelització dels supermercats tenen massa dades personals de nosaltres. De fet, fa vint anys, la base de dades personals més gran del món la tenia Wal-Mart, una cadena de supermercats nord-americana que a partir de les compres dels seus clients sabien quant cobraven, quant invertien en fer la compra, quin tipus d'aliments i productes, per a quantes persones, quan marxaven de vacances...

Kenneth Cukier, periodista de *The Economist* i autor del llibre *Big Data*, ens adverteix que la informació que tenim actualment disponible és molt més gran del que ha estat mai al passat perquè coneixem els mecanismes per recopilar-la, emmagatzemar-la i processar-la i hi ha un incentiu econòmic per fer-ho ja que és una informació molt valuosa. Aquest gran avatar que ens segueix i ens envolta és com un esperit de la mitologia grega. Encara vivim en la nostra corporalitat física, encara estem en l'univers del nostre pensament, però com que no ho veiem no volem entendre que

aquesta gran penombra que tenim al darrere és molt més gran i molt més valuosa... i no podem protegir-la[28].

El més sorprenent de tot això és la falta d'importància que se li dóna al problema; és a dir, acceptem que se'ns vigili i controli les vint-i-quatre hores del dia i ens és igual... La NSA (Nacional Security Agency) utilitza les plataformes que milions de persones fem servir per espiar-nos[29].

5. Data Brokers.

Quan Facebook encara era una xarxa universitària, Mark Zuckerberg li va confiar a un amic que, si ho necessitava, disposava de milers de dades de professors i alumnes de Harvard: correus electrònics, fotografies, números de la Seguretat Social... Quan el seu amic li va preguntar com els havia aconseguit, Zuckerberg li va respondre que la gent, no sabia perquè, simplement confiava en ell[30].

Actualment tots sabem que estem controlats, però no fins al punt en què realment ho estem. Els genis d'avui dia estan a Silicon Valley, treballant, amb una gran motivació i un sou increïble, envoltats de professionals i a un lloc fantàstic; creant aplicacions que siguin imbatibles, irresistibles i fins i tot addictives.

Tots estem submergits en un sistema del qual depenem pràcticament per a tot i en el que confiem per a tot, malgrat que no sabem com funciona. Hi ha gent que sí que sap com funcionen els seus mecanismes de control: els que els dissenyen i els agents que han invertit temps, diners i esforços en conèixer-los per a poder-los *hackejar*.

Les grans empreses estan interessades en les nostres dades personals ja que les utilitzen per alimentar algoritmes predictius d'intel·ligència artificial. El que fan els algoritmes és preveure què passarà al futur i què fer per prevenir segons quines coses.

"A Europa tenim la Llei de Protecció de Dades més restrictiva del món però la nostra capacitat per implementar aquesta legislació és bastant petita -pensa Marta Peirano- ja que qui controla realment el que les grans aplicacions emmagatzemen estan als Estats Units"[31].

Francesc Grau, especialista en Internet social, està segur que "de la mateixa manera que actualment ho compartim tot amb altres usuaris virtuals, no ho faríem si tinguéssim a tots aquells mateixos seguidors davant nostre, mirant-nos als ulls"[32].

Els Data Brokers (o venedors de dades) són empreses que es dediquen a recopilar, processar i vendre informació dels usuaris, amb permís consentit o sense, a terceres empreses que estiguin interessades en tenir aquesta informació.

Un Data Broker pot emmagatzemar unes 3.000 dades per consumidor. Són especialistes en convertir dades que en un principi no tenen cap valor, en informació de gran rellevància per les empreses que ho necessiten: informació de registres públics i de fonts privades que inclouen, entre d'altres, informació del cens, canvi de registres d'adreces, registres de vehicles, informes de mitjans i tribunals, llistes de registre d'electors, historial de compres, transaccions amb targetes bancàries i un llarg etcètera d'informació personal. Com més íntima i personal sigui aquesta informació, més valor tindrà.

La figura del Data Broker neix arran de les recerques que fem a Google, el que publiquem a les xarxes socials, les compres per Internet, els formularis que omplim quan els registrem a pàgines web, entre d'altres molts exemples. I així anem deixant el nostre rastre al món digital.

La finalitat dels Data Brokers i les empreses a les que venen les dades personals és oferir-nos tot un ampli ventall de productes i serveis molt més personalitzats, ja que tenen moltes dades nostres i poden saber quins són els nostres interessos i desitjos. S'asseguren un major impacte en els seus anuncis i ofertes, atraient molt més fàcilment, i també més ràpidament, el seu públic objectiu i per tant majors ingressos. Depenen de llocs web amb aplicacions de registre i cookies per trobar els consumidors en línia i així enviar-los anuncis per Internet basats en les seves activitats fora de la xarxa.

Ricard Martínez, president de l'Associació Professional Espanyola de Privacitat, explica[33] que "la professió del Data Broker no està regulada com a tal a la Unió Europea, i les seves activitats poden versar sobre dades personals de qualsevol naturalesa". També diu que aquests tractaments de dades poden ser "altament valuosos i socialment positius".

Pels Data Brokers no som persones, som algoritmes. El nostre perfil és automàtic, existeix encara que ningú li doni importància.

El nostre historial són els nous antecedents.

5.1. Exemple – Tap tap.

TAPTAP[34] és una multinacional *adtech* espanyola de VC, fundada el 2010, actualment present al sud d'Europa, Amèrica del Sud i Amèrica del Nord. La plataforma Sonata de TAPTAP proporciona informació intel·ligent i geoespacial per al perfil de públic, l'activació de publicitat dinàmica i l'atribució d'anuncis offline/online. Les marques i agències mundials utilitzen Sonata a més de 85 països per interactuar de manera eficient amb audiències omnicanals digitals i, sobretot, centrades en el mòbil.

És un empresa dedicada a la publicitat digital amb presencia a més de 15 països, 20 milions d'euros de facturació anual i uns 70 treballadors. Sonata és el producte que ofereix TapTap: una plataforma que divideix el món en celes de 500 metres quadrats i creua dades de tota mena, tant personals com les provinents de fonts públiques. Poder accedir a tota la informació que necessitin i la llista de variables que poden incorporar asseguren que és il·limitada. Són Data Brokers: compren bases de dades personals a les aplicacions i serveis digitals que extreuen informació dels seus usuaris, les creuen amb d'altres, extreuen conclusions sobre què vol el client i venen el resultat a les empreses perquè els mostrin la publicitat adequada mitjançant la seva localització (on és el consumidor, on és el producte, on és el comerç...).

Álvaro del Castillo, fundador i director executiu de TapTap, comenta[35] que "el món parla del Big Data, però amb el Big Data no es pot fer res a no ser que puguis harmonitzar [les dades] i donar-les-hi un sentit. El que es fa a TapTap és harmonitzar les dades en base al senyal local. Obtenim el senyal del lloc, li donem un sentit i el correlacionem amb d'altres."

D'altra banda, Álvaro Mayol, cap de producció, comenta: "imagina que volem fer una campanya a Madrid i a Barcelona. El que buscarem seran les zones amb major afinitat a les condicions que busca l'anunciant basant-se amb moltes variables, ja siguin dades dinàmiques, com els interessos de l'audiència basant en la seva navegació digital; o bé dades estàtiques, com el perfil demogràfic de la zona. Anem afegint capes per tractar de buscar la major afinitat i la major cobertura possible".

1

Veiem a l'esquerra la ciutat de Barcelona i a la dreta la ciutat de Madrid; ambdues des de l'aplicació de Sonata, on el color de les celes expressa l'índex d'afinitat a una determinada campanya de publicitat després d'haver-hi aplicat els filtres d'informació pública i de dades personals.

[1] Imatges: programació de l'aplicació Sonata de TapTap. Article del diari ElDiario.es 21/10/2019. Disponible a: https://www.eldiario.es/tecnologia/trabaja-empresa-compra-venta-personales-sentido_0_955054905.html

6. Comerç de dades.

Andrew Keen, periodista i autor d'*Internet no és la resposta*, confirma que "les grans empreses utilitzen l'ús que fem de la tecnologia per explotar-nos, per destruir la nostra singularitat interior. Per això Google, que val gairebé un milió de milions de dòlars, és una de les empreses més rendibles de la història. Nosaltres, els usuaris, som el producte de Google"[36].

Ja veiem que gràcies al Big Data i la seva comercialització a la xarxa i als Data Brokers, les nostres dades estan en un constant intercanvi perquè les empreses es lucrin a partir dels nostres interessos. Moltes vegades amb només navegar per una pàgina web o fer servir una aplicació, ja estem donant permís perquè es guardin i s'utilitzin les nostres dades personals.

Tot i que l'usuari mitjà poc a poc va prenent consciència d'aquest problema i del que comporta, segons una anàlisi de la consultora We Are Social[37] , el 63% dels usuaris estan preocupats pel tractament que es fan de les seves dades personals a Internet.

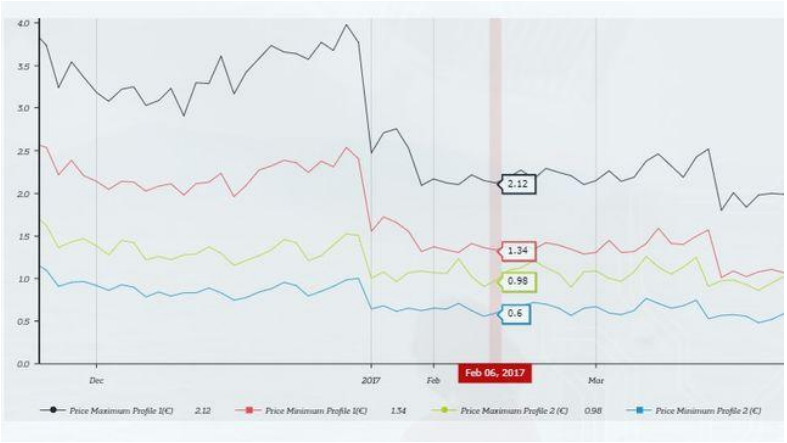
Al 2017, Andrew Ng, en aquell moment un alt directiu de Baidu (el Google xinès), va confessar que "a la majoria de companyies tecnològiques sovint es llancen productes no per ingressos sinó per dades... i després monetitzen les dades a través d'un producte diferent".

Elies Campo, enginyer i desenvolupador de negoci actualment a Telegram, explica[38] que "som animals socials, ens agrada estar connectats i interactuar amb éssers humans i les tècniques que s'utilitzen per implementar aquests productes són unes tècniques molt similars a les que utilitzen les màquines recreatives (escurabutxaques) de recompensa variable. El nostre cervell segrega dopamina i es crea un micromoment de plaer que fa que vulguem tornar a experimentar aquesta experiència." Aquesta dependència crea addicció, provoca depressió, soledat i aïllament. Als joves, fins i tot agressivitat i fracàs escolar.

6.1. Casos.

Les nostres dades, com hem vist, tenen preu. El preu depèn del que els anunciants estiguin disposats a pagar per publicitar-se. El preu final, però, no és públic; tot i que Facebook ens ofereix unes xifres orientatives. Ángel Cuevas, investigador de la Universitat Carlos III de Madrid, explica[39] que "es una puja que, a més, varia molt al llarg dels temps. Per exemple quan arriba el *Black Friday*, el preu que els anunciants estan disposat a pagar per mostrar els seus anuncis als usuaris creix molt. També hi ha una diferencia entre el cap de setmana i la resta de dies".

Esdeveniments puntuals o estacionals, com ara el *Black Friday* o Nadal, augmenten l'interès dels anunciants però els investigadors de la Universitat Carlos III també han descobert que a les èpoques típiques de consum la demanda per arribar a un determinat públic també va augmentar quan van haver les eleccions nord-americanes. "Les eleccions no augmenten els preus per defecte, però sí que observem que en certs estats, per certes audiències, patien canvis significatius. Intentem veure si amb la variació de preus entre diferents perfils d'usuaris i de diferents estats, podia existir un canvi de tendència entre els favorables a Trump i a Clinton", explica Cuevas. En aquesta fotografia podem veure la interacció amb els *clics* d'una publicitat de Facebook dels usuaris homes espanyols interessants en política, en color verd i blau, en comparació amb el mateix perfil d'usuaris americans, en color vermell i negre.



La Facebook Data Valuation Tool (FDVT) es pot descarregar com una aplicació per al navegador per mesurar en temps real quant valen les dades que està generant l'usuari.

Facebook mai no ha amagat que ven l'accés a la seva base de dades amb informació dels seus usuaris com a mètode infalible per

augmentar els missatges publicitaris. Facebook sap més coses de tu que tu mateix[40], té un registre de l'activitat online dels seus usuaris, que actualment són 2.449 milions.

Tot i que Marc Elena, especialista en Facebook, comenta[41] que "com a usuaris no hem d'estar preocupats perquè es venguin les nostres dades, ja que és una informació que no es ven per persona, sinó per segmentar a partir del sexe, dels gustos, dels interessos... dels usuaris".

L'Associació d'Internatutes també ha desenvolupat una web amb l'eina per analitzar les cotitzacions de determinades audiències al llarg del temps. Es tracta de TestdePrivacidad[42] per difondre, informar i sensibilitzar sobre la importància de la privacitat a l'entorn digital i donar a conèixer iniciatives que permeten una millor gestió de la privacitat dels usuaris de noves tecnologies.

A Espanya, una de les referents en aquest àmbit és Helena Matute, catedràtica de Psicologia Experimental a la Universitat de Deusto. Els seus estudis aprofundeixen en les estratègies que utilitza la indústria digital per aconseguir que els seus usuaris acceptin l'actual tecnologia potencialment perillosa per als seus drets de privacitat sense adoptar una perspectiva crítica. Diu que "l'objectiu d'aquesta nova indústria es guanyar diners, però tot el que hi ha al mig els és igual. La seva finalitat és vendre, ja sigui un producte o el president del país. Coneixen molt bé les nostres debilitats i els porten una gran avantatge en el coneixement de determinats aspectes del comportament humà i com manipular-lo [...]. Quan parlem de fer servir les nostres dades no parlem només de dades de l'e-mail, de la data de naixement o del carrer on vivim. Moltes d'aquestes dades són sobre la nostra personalitat, i a partir d'elles fan experiments psicològics i de manipulació del comportament. És un aspecte que les lleis actuals tampoc controlen, suposa experimentació feta amb humans sense consentiment i sense cap norma ètica", alerta Matute[43].

6.1.1. Google.

Google és actualment una de les empreses més poderoses a nivell mundial i qui porta el control de molts de nosaltres ja que és el buscador més utilitzat a Internet. També ofereix altres productes i serveis com Google Drive, el correu electrònic (Gmail), Google Maps, Google Street View, YouTube, Google Play, Google Llibres, Google Notícies... i molts més. Gràcies als milers de servidors i centres de dades a tot el món, Google processa més de 1.000 milions de cerques diàries i el seu motor de cerca és el lloc web més visitat al món.

De vegades, vist el nivell en què es troba Google i del que pot arribar a saber de tots nosaltres quan es té tanta informació i tant poder, pot jugar en contra de l'usuari.

Al 2019 Google va accedir a informació de pacients d'Ascension, una de les majors companyies de salut dels Estats Units. Van firmar un acord secret per emmagatzemar i analitzar les dades personals dels pacients amb l'objectiu de millorar el servei mèdic, reduir costos i salvar vides, segons va expressar Tarip Shaukat[44] , president de Google Cloud. Ni el servei mèdic del centre ni els seus pacients van tenir constància d'això quan se'ls hauria d'haver notificat des d'un bon principi. Tanmateix, la xarxa hospitalària va publicar que estaven operant amb uns requisits estrictes de l'organització per a la manipulació de dades i era tot legal.

De fet, Google registra tots els nostres moviments a la xarxa i ho especifica prèviament a la seva política d'ús i privacitat: registra les nostres cerques, els vídeos que veiem, les visualitzacions i interaccions amb els anuncis que ens apareixen, informació sobre veu i àudio quan utilitzem aquestes funcions, activitat de compra, usuaris amb els quals ens comuniquem i compartim continguts, activitats en llocs web i aplicacions de tercers que utilitzen els nostres serveis, l'historial de navegació, la nostra ubicació... ens controla en cada moviment que fem i com el fem.

Sergio González, expert en tecnologia, explica[45] que tot i que Google permeti desactivar els controls de Google, recomana no fer-ho perquè atès que és una informació que tard o d'hora la tindran serà millor que la tinguem per nosaltres mateixos; és a dir, com ell diu, "en el

moment que desactives la informació, l'única persona que no tindrà aquesta informació seràs tu mateix".

6.1.2. Els filtres i FaceApp.

Els filtres d'Snapchat, Instagram, TikTok... tan populars avui dia, són una combinació entre realitat augmentada, intel·ligència artificial i computació visual, entre d'altres àrees del coneixement. Un *mappeig* de la nostra cara píxel a píxel per identificar el nostre rostre.

A l'estiu de 2019 es va fer viral l'aplicació FaceApp, un programa on es podia, entre d'altres funcions, envellir la fotografia de qualsevol persona. Va ser una app que molta gent va voler fer servir per comprovar com seria en un futur i en qüestió d'hores ja havia arribat a milers de descàrregues a Play Store i a Apple Store.

2

FaceApp utilitza un sistema neuronal basat en intel·ligència artificial que analitza la fotografia de forma automàtica als seus servidors per crear el filtre que vulguem amb un gran realisme. FaceApp, però, ha disparat les alarmes perquè el servidor rus ofereix unes polítiques de privacitat i condicions d'ús que no s'actualitzen des de gener de 2017 i no estan adaptades al Reglament General de Protecció de Dades actual.

[2] Imatge 1: Exemple del famós filtre d'envelliment de FaceApp amb diferents polítics. Article del diari *El País*. 18/07/2019. Disponible a: https://elpais.com/tecnologia/2019/07/17/actualidad/1563358803_598879.html Imatge 2: Exemple del famós filtre d'envelliment de FaceApp amb el jugador de futbol Leo Messi. Article del diari *El País*. 18/07/2019. Disponible a: https://elpais.com/tecnologia/2019/07/18/actualidad/1563475837_354416.html

Com explica Vanesa Alarcón, especialista en dret de noves tecnologies, la política de privacitat[46] que utilitza FaceApp "no és del tot transparent, hi ha una sèrie de riscos relacionats amb què l'usuari no sàpiga perquè pot ser utilitzada la informació que recull l'aplicació, com s'emmagatzema aquesta informació... ja que no compleix amb el Reglament General de Protecció de Dades vigent a la Unió Europea". Fins i tot la seva política de privacitat diu que treballen amb un localitzador dins del nostre terminal al qual podrien accedir a la resta de la nostra informació personal, més enllà de la que proporciona l'aplicació.

Dani Creus, analista de seguretat de Kaspersky, també adverteix[47] dels riscos de compartir fotografies amb tercers. Pensem que des del moment que pugem una fotografia hem d'assumir que estem perdent la nostra intimitat. Kaspersky explica que, a hores d'ara, el millor aliat de l'usuari a Internet és "el sentit comú".

D'altra banda, Yaroslav Goncharov, creador de FaceApp, al seu moment va confirmar que l'aplicació es troba desbordada davant la demanda per part dels usuaris d'eliminar les fotografies dels seus servidors, una tasca que per a ells en aquest moments és prioritària. Contràriament al que estableix la seva política de privacitat (apartat 3) i, per tant, que l'usuari es veu obligat a acceptar, Goncharon reafirma que "no venen ni comparteixen dades a tercers".

Les dades biomètriques com ara la cara, la veu o l'empremta permeten que l'usuari sigui reconeixible sense fer res, només pel fet d'introduir-les al mòbil. La millor opció, assegura Marta Peirano, és utilitzar el número PIN. Perquè les nostres cares siguin reconeixibles per als sistemes de reconeixement facial han de tenir les nostres cares a una gran base de dades, per això hi ha tantes aplicacions de filtres, editors de fotografies... són aplicacions amb accés a la nostra càmera selfie en tot moment i estem entrenant, sense ésser conscients, algoritmes de reconeixement facial[48].

6.1.3. Avast.

Avast és un programa antivirus conegut internacionalment que al desembre de 2019 va reconèixer que la companyia recollia i venia informació sobre els hàbits de navegació dels seus usuaris. Ondrej

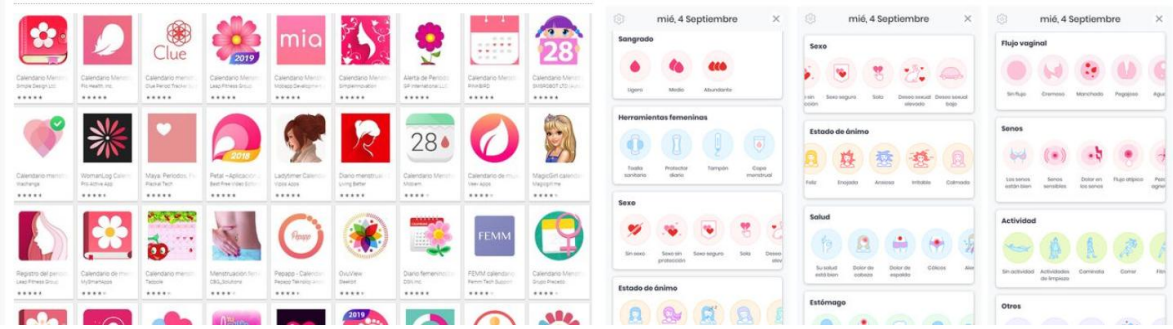
Vlcek, CEO d'Avast, va assegurar[49] que la informació que veien era anònima ja que no es podia rastrejar ni associar a cap usuari. Vlcek va fer aquesta declaració perquè les dades que havien recollit no estaven associades al nom, a l'e-mail o a l'adreça IP de la persona; però si es combinen amb altres informacions com les URL sí que es poden analitzar per exposar la identitat de qualsevol.

Dos periodistes de PCMag i Motherboard van tenir accés a la documentació interna que estava venent Avast i aquests van confirmar que sí que es podien associar a usuaris concrets; de fet, era informació que recollia tots els clics, totes les cerques, compres i visites web.

Jumpshot és una companyia que ofereix dades de més de cent milions de dispositius mòbils i ordinadors. Empreses com Google, Microsoft, Pepsi, Home Depot... entre d'altres, també compren dades a través de Jumpshot com ho va fer Avast. Aquestes (i probablement altres empreses) podien veure amb gran detall tots els moviments dels usuaris que tinguessin l'antivirus instal·lat.

6.1.4. Apps menstruació.

Actualment tenim un gran ventall d'aplicacions de tota mena: per jugar, per fer receptes, per fer esport, per trobar feina, per buscar parella... i dins de l'àmbit de salut, també tenim una gran oferta. Centrant-nos ens les aplicacions menstruals, són aplicacions que porten un control sobre la menstruació i ajuden a les dones i a l'aplicació a recopilar una gran quantitat de dades molt més personals de les que hem vist fins ara. [3]



[3] Imatge 1: el que ens trobem quan entrem al buscador d'aplicacions menstruals de GooglePlay o AppleStore. Imatge 2: tota la informació que demana a les seves usuàries una aplicació menstrual.

Podem veure que Google Play ofereix moltes aplicacions d'aquesta mena. Aleshores, perquè n'hi ha tantes? A què treu cap aquest interès de tantes empreses oferint un mateix servei, pràcticament calcat? Recordem que el capitalisme de la maternitat és uns dels mercats publicitaris més rentables, i aquestes aplicacions pregunten a les seves usuàries pels seus hàbits de vida: si fumen i en quina quantitat, si beuen alcohol, com dormen, amb quina freqüència tenen relacions sexuals i com són, l'aspecte de la pell, l'estat d'ànim... i moltes més preguntes íntimes que, segurament, no explicarien a qualsevol.

Una investigació de Privacy International[50], ONG de referència en la vigilància del respecte al dret de la privacitat per part de governs i empreses, va destapar com moltes d'aquestes aplicacions s'utilitzen per oferir i vendre aquesta informació íntima a tercers; aquestes dades, doncs, tenen un gran interès per als anunciants. L'anàlisi no es va centrar en els usos i condicions de les aplicacions, les opcions de privacitat o qualsevol altra informació visible de l'app, ha registrat quins són els paquets de dades que envien les aplicacions i a qui. Les principals aplicacions que van descobrir que "traficaven" amb dades van ser: Mia (desenvolupada per Mobapp Development Limited), Maya (Plackal Tech), Calendario menstrual & Calculadora de ovulación (PinkBird), Mi calendario (Grupo Familia) i Mi Period Tracker (Linchpin Health). Tant Mia com Maya són de les més populars a Espanya amb milions d'usuàries que, segons aquesta anàlisi, són les més indiscretes.

6.1.5. Spotify.

Spotify és un programari de flux de dades de música. Gràcies a un model d'igual a igual permet escoltar la música que ofereix (milions d'arxius sonors) de forma instantània sense temps de descàrrega. Es poden fer cerques de temes musicals per artista, àlbum o llistes de reproducció creades pels propis usuaris. És una de les plataformes de música més importants d'arreu del món amb 200 milions d'usuaris.

Spotify compta amb un departament clau en la seva estratègia de negoci: la missió de dades. En la qual, des de 2016, treballen

psicòlegs socials, físics de partícules i neurocientífics computacionals amb l'objectiu d'estudiar a fons el comportament dels usuaris per vendre aquesta informació de com són els consumidors a partir de la música que escolten. Clay Gibson, el cap de producció de l'empresa, explica[51] que el seu lema en aquesta part de negoci és "Ets el que escoltes"; i el que escoltes està vinculat a qui ets com a persona, com et sents, on has estat i què has viscut. La manera com els usuaris interactuen amb Spotify al llarg del dia proporciona una gran observació per començar a entendre aquestes coses, diu Gibson. La missió de dades forma part de la propaganda amb la que Spotify ven als anunciants el seu valor com a plataforma publicitària.

Aquesta idea va sorgir l'any 2015 quan Brian Benedik, aleshores responsable de Spotify a Amèrica del Nord, es va adonar que uns 400.000 usuaris havien creat una llista de reproducció de música per a les seves barbacoes... i era comercialment explotable! És més fàcil que Coca-Cola o Nescafé vulguin anunciar-se a usuaris que associïn la marca a un estat d'ànim i amb aquesta estratègia. Els beneficis generats pels anuncis d'Spotify van créixer un 276,5% entre 2015 i 2018 i a hores d'ara, Benedik és el cap global d'ingressos de l'empresa.

Gràcies a l'aprovació i a la regulació del Reglament General de Protecció de Dades Europeu, Spotify compta amb un formulari per demanar a l'empresa la nostra informació, on també s'inclouen algunes explicacions per controlar quines de les nostres dades personals tracta. Spotify necessita tractar amb algunes dades personals per poder prestar-nos el seu servei. Si el que volem és que elimini les nostres dades l'única solució és eliminar el nostre compte.

Spotify, a diferència d'altres aplicacions o programes, sí que deixa clar a la seva política d'ús i privacitat que comparteixen dades amb tercers:

Categorías de destinatarios	Motivo para compartir
Proveedores de servicios y otros	Utilizamos proveedores de servicios técnicos que procuran la infraestructura técnica que necesitamos para proporcionar el Servicio Spotify, en particular los proveedores que alojan, almacenan, gestionan y mantienen la aplicación de Spotify, su contenido y los datos que procesamos. Utilizamos proveedores de servicios técnicos para ayudarnos a comunicarnos con usted, como se describe en la Sección 6 (Sección 6) de esta Política. Utilizamos socios de marketing y publicidad para mostrar más contenido personalizado, o para ayudarnos a entender el uso que hace del Servicio Spotify y así brindarle un mejor servicio. También podemos compartir los datos personales con algunos socios de marketing y publicidad con el fin de enviarle comunicaciones promocionales sobre Spotify.
Socios de Spotify	• Si accede al Servicio Spotify a través de una oferta que recibió o adquirió de terceros, como su operador de red móvil, compartimos datos personales con terceros acerca de su uso del Servicio Spotify, como por ejemplo, si se ha utilizado la oferta y en qué medida, se ha activado una cuenta de Spotify, o ha utilizado activamente el Servicio Spotify. • En función de cómo se registre en el Servicio Spotify (por ejemplo, a través del servicio de un tercero o de un proveedor móvil), compartiremos su nombre de usuario de Spotify u otros datos de registro de cuenta según sea necesario para activar su cuenta. • También podemos compartir sus datos personales en un formato seudoanonimizado con nuestros socios del sector de la música para ayudarles a entender cómo funciona el contenido para el que nos autorizan y permitirle escuchar contenido en streaming a través del Servicio Spotify. • De igual manera, compartimos sus datos personales en un formato seudoanonimizado con socios de marketing que nos ayudan con actividades de promoción, y con los anunciantes que nos permiten ofrecer un servicio gratuito.

6.2. Què podem fer per evitar-ho?

L'objectiu de la vigilància és mirar sense ser vist.

El Dr. Karsten Nohl, director de Security Reserch Lab a Berlín, adverteix que "si volem preservar una esfera privada, haurem d'educar de forma molt activa a la seva defensa". Els estats intenten, sens dubte, tot el contrari amb l'excusa de la lluita contra la criminalitat, inclosa la lluita contra el terrorisme, van convencent a la gent que renunciï a una part de la seva intimitat cada any una mica més per reeixir en aquesta lluita. Però aquesta renúncia a la intimitat ajuda molt a aquests "altres estats", als Google i Facebook del món que ens roben cada vegada més espai de la nostra llibertat d'expressió[52].

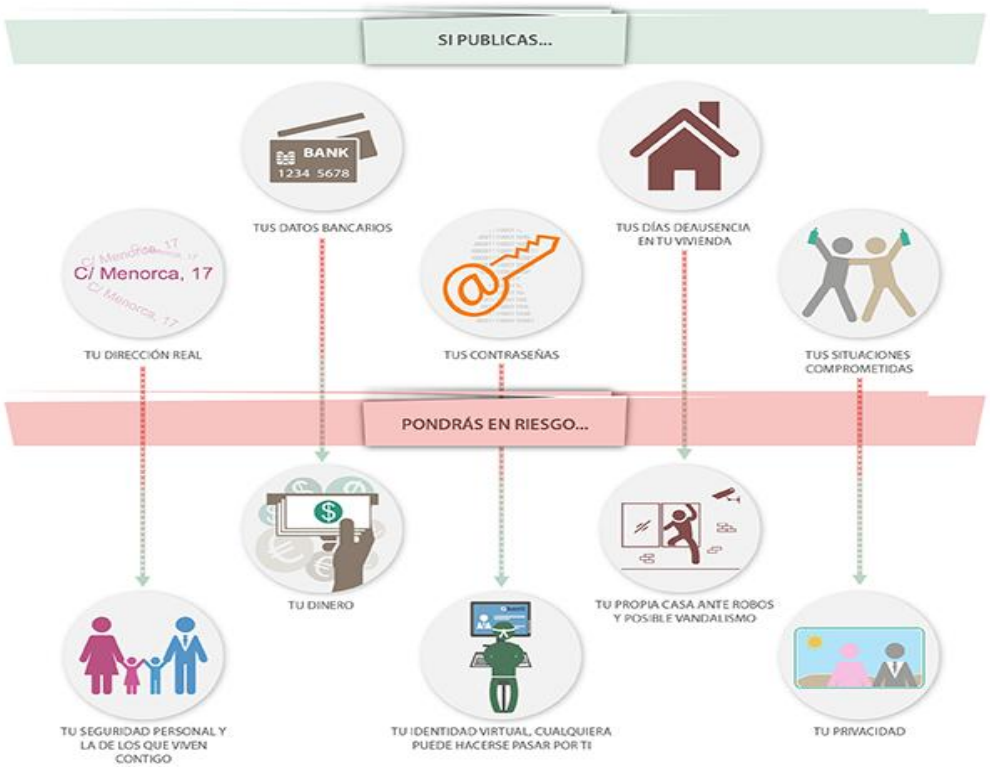
L'Oficina de Seguridad del Internauta (OSI)[53] proporciona la informació i el suport necessari per evitar i resoldre els problemes de seguretat que poden existir en navegar per Internet. La OSI treballa amb l'objectiu d'ajudar als usuaris a portar a terme un canvi positiu de comportament en relació amb l'adopció dels bons hàbits de seguretat a la xarxa, de reforçar la confiança en l'àmbit digital a través de la formació en *ciberseguretat* i crear consciencia; i contribuir a minimitzar el nombre i gravetat d'incidències de seguretat experimentades per l'usuari.

Gran part de la informació que es pot trobar sobre nosaltres a Internet l'hem compartit a través de les xarxes socials, missatgeria instantània, publicacions a blogs, fòrums... Com més informació hi hagi de nosaltres, més fàcil ho tindran aquells que vulguin fer un ús indegut d'aquesta informació. La OSI adverteix que és important que tothom conegui els riscos a l'hora de fer públiques les nostres dades:

- Dades personals: El DNI o passaport és un clar exemple d'allò que no hem de facilitar a Internet així com així. Aquesta informació, si cau a les mans incorrectes, pot causar molts problemes, entre d'altres, fraus de suplantació de la identitat.
- Correu electrònic: que el nostre correu deixi de ser privat farà que comencem a rebre gran quantitat d'spam, missatges amb intents d'engany (phishing), fraus...
- Dades bancàries: facilitar les nostres dades bancàries ens pot exposar a una pèrdua econòmica. Hem de ser molt previnguts amb les pàgines web on se'ns demanen les dades bancàries per

realitzar compres online i mai facilitar aquestes dades per correu electrònic.

- Ubicació geogràfica: publicar els llocs que solem freqüentar proporciona informació que permet que algú malintencionat pugui localitzar-nos en persona o pugui conèixer la nostra rutina i hàbits diaris. També és una manera d'esbrinar quan no hi som al nostre domicili.
- Fotografies i vídeos: les nostres fotografies i vídeos personals contenen molta més informació que no ens pensem: ubicacions físiques, qui son els nostres amics i familiars, quin és el nostre nivell econòmic, quin aspecte té casa nostra, gustos, preferències... no deixem a l'abast de qualsevol aquest tipus de contingut.



Per això, la OSI aconsella:

- Ser curosos amb la informació que compartim. Un cop publicades a Internet, quedarà permanentment, escapa del teu control i és accessible des de qualsevol lloc del món.
- Configurar adequadament les opcions de privacitat als perfils de les xarxes socials. Controlar qui té accés a les publicacions.

- Conèixer els nostres drets. La Llei de Protecció de Dades (LOPD) obliga a totes les empreses espanyoles a protegir les nostres dades tot i que no a totes les empreses se'ls aplica aquesta llei per estar ubicades a altres països. Abans de fer-ne ús d'un servei, ens hem d'informar i llegir bé les polítiques de privacitat que ofereixen.
- Hem de ser previnguts amb els dispositius i els llocs públics. No hem d'oblidar la seguretat dels nostres dispositius i utilitzar sempre xarxes segures per on compartir informació.
- Si alguna informació publicada sobre tu t'està perjudicant, sol·licita la seva regitada a Google o al servei que correspongui. Tens el dret a l'oblit a Internet.

També podem fer servir criptografia, la criptografia és la ciència i l'art d'escriure missatges en forma xifrada o en codi. És part d'un camp d'estudi que tracta les comunicacions secretes, usades, entre altres finalitats per a:

- Autentificar la identitat d'usuaris.
- Autentificar i protegir el sigil de comunicacions personals i de transaccions comercials i bancàries.
- Protegir la integritat de transferències electròniques de fons.

La criptologia és l'estudi dels criptosistemes: sistemes que ofereixen mitjans segurs de comunicació amb els quals l'emissor oculta o xifra el missatge abans de transmetre'l perquè només un receptor autoritzat (o ningú) pugui desxifrar-lo. Les seves àrees principals d'interès són la criptografia i la criptoanàlisi, però també inclou l'esteganografia com a part d'aquesta ciència aplicada. En temps recents, l'interès per la criptologia s'ha estès també a altres aplicacions, per part de la comunicació segura d'informació i, actualment, una de les aplicacions més esteses de les tècniques i mètodes estudiats per la criptologia és l'autenticitat de la informació digital (també anomenada signatura digital)[54].

Actualment hi ha aplicacions que sí que respecten la nostra intimitat[55]. Les més rellevants, dividides per funcionalitat, són:

- Missatgeria instantània:

Tot i que l'Electronic Frontier Foundation (EFF) deixa clar que cap aplicació de missatgeria pot satisfer perfectament les necessitats de seguretat i comunicació de tots, algunes de les opcions són:

Signal, disponible per a iPhone i Android, per la seva encriptació i les poques metadades que recull de l'usuari.

ChatSecure, una aplicació de missatgeria encriptada disponible per a iPhone.

SilentCircle, centrada en assegurar la ciberseguretat de les comunicacions en entorns empresarials.

Telegram, tot i que compta amb problemes i va haver de treure els seus servidors de Rússia pels assetjaments del Govern de Vladimir Putin, és la més recomanada en diverses llistes com a eina respectuosa amb la privacitat.

- Correu electrònic:

Protonmail, un servei de correu amb unes estrictes lleis de privacitat.

ThunderBird, de la Fundació Mozilla (que també promou un dels navegadors més respectuosos amb la privacitat, Firefox) no té aplicació per a mòbil però es pot consultar des del navegador.

Kolab Now, basada en la privacitat, la seguretat i de codi obert.

- Cercadors:

DuckDuckGo és la més recomanada sota el seu lema "el buscador que no et rastreja".

Startpage, els seus resultats de cerca són molt similars als que ofereix Google perquè utilitza el seu motor de cerca.

- Navegadors:

Tor és la més recomanada. És una xarxa disponible per Android, iPhone, Windows, Mac i Linux. Tor són les sigles de The Onion Router i és un sistema segur i relativament senzill d'utilitzar que permet als usuaris navegar per la web a través d'una xarxa de voluntaris interconnectats afegint "capes" de seguretat. El software xifra automaticament les dades de manera que cap altre ordinador individual a la xarxa té tota la informació d'un usuari.

Firefox és l'altre navegador més recomanat.

- Emmagatzematge:

Per a l'emmagatzematge és on trobem més alternatives de pagament. La recomanació de l'Electronic Privacy Information Center es Own Clowd.

Crytomator permet afegir una capa de xifrat extra.

- Xarxes socials:

RetroShare és la manera més fàcil de començar la teva pròpa xarxa social xifrada.

Mastodon és una opció per a usuaris sense coneixements informàtics, té més de dos milions d'usuaris i és molt similar a Twitter.

- Eines d'oficina:

CryptPad és una alternativa privada per disseny a les populars eines d'oficina i serveis al núvol. Tot el contingut que emmagatzema és encriptat abans de ser enviat. Compta amb suport per a crear documents de text, fulls de càlcul, presentacions de diapositives o enquestes, entre d'altres.

EtherCalc, es centra en els fulls de càlcul. Permet que diversos usuaris puguin modificar un mateix document alhora. És de codi obert i no extrau dades de les activitats.

- Mapes:

OpenStreetMar no compta amb vista satelital ni les fotografies dels carrers fetes per Google.

El programa CookieViz,posat a disposició dels ciutadans per la CNIL, l'agència francesa de protecció de dades, ens permet visualitzar els diminuts artefactes digitals que s'enganxen a la nostra adreça IP per controlar-nos millor. Són petits espies per anomenats cookies, que porten la matèria primera a les agències d'estadístiques i d'anàlisi. Al cap de pocs minuts de connexió, tant si és un lloc informàtic com comercial, una miríade d'aquestes cookies detecten la nostra presència i en registren les nostres dades[56].

7. Conclusions.

L'avenç i el desenvolupament de les noves tecnologies aporta, òbviament, grans beneficis. Tot i això, podem veure que la nostra informació, tant a nivell personal com professional, està molt més exposada a possibles atacs. És inevitable estar-ne exposats i per això el que hem de fer és controlar allò que publiquem, ser prudents a l'hora de compartir opinions i anar amb compte ara que tant Internet com el mòbil són eines necessàries en el nostre dia a dia. Hem vist que les nostres dades personals conformen tota aquella informació relacionada amb una persona física viva, identificada o identificable a partir del seu nom, fotografia, correu, adreça, dades bancàries, publicacions a les xarxes socials, informació mèdica, dades biomètriques i la seva orientació sexual.

Gran part d'aquesta informació que es pot trobar sobre nosaltres a la xarxa l'hem compartit a través de les xarxes socials, missatgeria instantània, publicacions a blogs, fòrums... Aquestes dades són molt valuoses per als Data Brokers (o venedors de dades), empreses que es dediquen a recopilar, processar i vendre informació dels usuaris, amb permís consentit o sense, a terceres empreses que estiguin interessades en tenir aquesta informació. Un Data Broker pot arribar a emmagatzemar unes 3.000 dades per consumidor.

Bill Gates va dir una vegada que "si el teu negoci no és a Internet, el teu negoci no existeix". Passa el mateix amb les persones, amb els usuaris. Tothom, de manera directa o indirecta, apareix a Internet. Aquesta és una informació que és a l'abast de tothom i hem de crear una identitat personal per aconseguir donar la imatge que volem. La majoria d'empreses actualment busquen el nostre nom a LinkedIn o directament a Google per saber qui som o què diu la xarxa de nosaltres. I qualsevol persona amb un mínim de coneixement informàtic pot saber molt més que no ens pensem de nosaltres.

Al desembre de 2018 va entrar en vigor la nova Llei Orgànica 3/2018 de Protecció de Dades i Garantia dels Drets Digitals (LOPDGDD) amb el principal objectiu de protegir la intimitat, privacitat i integritat de l'individu, complint amb l'article 18.4 de la Constitució Espanyola. Era una reforma adaptada a l'actualitat de les noves tecnologies que tenia

en compte aspectes que fins aleshores no estaven dins la llei com ara la protecció de dades a les xarxes socials, a persones mortes, el regim jurídic dels empleats, l'ús de les nostres dades per als partits polítics, etc. La normativa de protecció de dades ha establerts unes normes per a les empreses i per als usuaris. Les empreses que fan servir les nostres dades personals han de complir amb la legalitat del tractament de dades, transparència, han de tenir un ús limitat, minimització de dades, correcció del processament de dades, limitació d'emmagatzematge i confidencialitat i integritat.

D'altra banda, pel que fa als usuaris, la normativa permet que es pugui exercir davant el responsable del tractament els drets d'accés, rectificació, oposició, supressió (dret a l'oblit), limitació del tractament, portabilitat, de no ser objecte de decisions individualitzades, de la informació i, per últim, el dret de Schengen.

Mentre feia aquest treball he pogut contestar les preguntes que em proposava: he pogut confirmar que les empreses que treballen amb les nostres dades personals ho fan amb finalitat publicitària, per poder personalitzar al màxim els productes que ens ofereixen a través del Big Data, una macro base de dades que pot saber-ho tot de nosaltres. En tot cas elaboren informació a partir dels nostres gustos, la nostra ubicació, el nombre de persones que som a casa, els esports que practiquem i molts altres més paràmetres. De fet, fan ús de totes les dades que es proposin tenir al seu abast per arribar al major nombre de persones possible i sobretot personalitzar l'experiència. La gran majoria dels enquestats pensen que les empreses que tenen accés a les nostres dades personals poden arribar a saber-ho tot de nosaltres: un 56% dels menors de vint-i-cinc anys, un 60% de les persones entre vint-i-cinc i cinquanta anys i un 49% dels més grans de cinquanta anys. I és també una gran majoria els que pensen que aquestes empreses ho fan amb finalitats publicitàries: un 67% dels menors de vint-i-cinc anys, un 54% d'entre vint-i-cinc i cinquanta anys i un 56% dels de més de cinquanta anys[57].

Com a usuaris donem consentiment, a vegades sense adonar-nos, perquè el document on ve tota la normativa d'ús i privacitat és tan llarg que ningú és capaç de llegir-lo sencer. És sorprenent que a

l'enquesta realitzada, uns quants dels enquestats van contestar que sí que se les llegeixen sempre (un 6% de les persones d'entre vint-i-cinc i cinquanta anys i un 10% dels majors de cinquanta). Cal tenir en compte que moltes aplicacions, la gran majoria, publiquen el document de les polítiques amb una gran quantitat de pàgines que resulta interminable per qualsevol persona que es descarregui una aplicació. Ho fan expressament perquè quan l'usuari veu que són tres-centes pàgines de document, no ho llegeix i accepta sense mirar res.

També hem vist les alternatives que existeixen per als usuaris que no vulguin compartir les seves dades, tot i que actualment sigui bastant difícil no fer-ho, d'una manera o altra. Tot i que la llei espanyola obliga a totes les empreses de l'estat a protegir les nostres dades, si una empresa està ubicada a un país fora de la Unió Europea no està obligada a fer-ho. Per tant, moltes empreses actualment no ho compleixen. L'Oficina de Seguridad de l'Internauta (OSI)[58] proporciona la informació i el suport necessari per evitar i resoldre els problemes de seguretat que poden existir en navegar per Internet. Per als usuaris que volen protegir les seves dades poden fer servir la criptografia, la ciència i l'art d'escriure missatges en forma xifrada o en codi; o una sèrie d'aplicacions que hem vist que sí que respecten la nostra intimitat a la xarxa.

Hem d'aprendre a valorar i a protegir la nostra informació ja que un cop publicada a Internet en perdem el control i se'n pot arribar a fer un mal ús fins al punt que ens pugui perjudicar.

Ara que la privacitat s'ha modificat radicalment hem de saber controlar-la. Hem creat una empremta digital extensa i permanent a Internet: és la nostra biografia digital amb una infinitat de continguts i de dades.

L'objectiu de la vigilància és observar sense ser vistos. Per tant és molt important, si més no, estar informats.

8. Bibliografia i annexos.

¿Qué es la inteligencia artificial? [en línea] [Data de consulta 16/04/2020] Disponible a: https://www.salesforce.com/mx/blog/2017/6/Que-es-la-inteligencia-artificial.html

A.R. Diario de Mallorca. [en línia] *Cómo borrar nuestros datos personales de Internet* (06/03/2020) [Data de consulta: 30/03/2020] Disponible a: https://www.diariodemallorca.es/vida-y-estilo/tecnologia/2020/03/06/borrar-datos-personales-internet/1492120.html

Accenture [en línia] [Data de consulta: 23/03/2020] https://www.accenture.com/es-es/company-big-data-fundamental-transformacion-digital

Agencia Española de protección de datos [en línia] [Data de consulta: 17/03/2020] Disponible a: https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos

Datalia. Seguridad de la información [en línia] [Data de consulta: 17/03/2020] Disponible a: https://datalia.info/entrada-blog/8-cambios-de-la-nueva-ley-organica-de-proteccion-de-datos-personales-y-garantia-de-los

DEL CASTILLO, Carlos. Eldiario.es [en línia] (19/10/2019) *No todos en Internet te espían: aquí tienes apps para el día a día que respetan tu privacidad.* [Data de consulta: 01/05/2020] Disponible a: https://www.eldiario.es/tecnologia/podrido-respetan-derechos-hacer-ocurra_0_953655115.html

DEL CASTILLO, Carlos. Eldiario.es [en línia] *Así fluctúa el precio de tus datos personales en la bolsa de Facebook.* (05/04/2018) [Data de consulta: 20/04/2020] Disponible a: https://www.eldiario.es/tecnologia/cotizan-mercado-Facebook-precio-fluctua_0_757675161.html

DEL CASTILLO, Carlos. ElDiario.es [en línia] *Así trabaja una empresa española que compra y vende datos personales para hacer publicidad: "Recogemos toda la información posible"* (21/10/2019). [Data de consulta: 23/04/2020]. Disponible a: https://www.eldiario.es/tecnologia/trabaja-empresa-compra-venta-personales-sentido_0_955054905.html

DEL CASTILLO, Carlos. Eldiario.es [en línia] *Hay una carrera por escribir las reglas de la inteligencia artificial (y la industria va ganando).* (11/05/2019) [Data de consulta: 20/04/2020] Disponible a: https://www.eldiario.es/tecnologia/adelantado-Alemania-Espana-Inteligencia-Artificial_0_894861231.html

DEL CASTILLO, Carlos. Eldiario.es [en línia] *Hola, soy la app de tu menstruación y les cuento a otros lo que sé sobre ti* (17/09/2019) [Data de consulta: 09/04/2020] Disponible a: https://www.eldiario.es/tecnologia/Hola-app-menstruacion-vendiendo_0_940706659.html

DEL CASTILLO, Carlos. Eldiario.es [en línia] *Spotify analiza las canciones que escuchas para saber tu estado de ánimo y vende la información a los anunciantes.* (03/07/2019) [Data de consulta: 09/04/2020] Disponible a: https://www.eldiario.es/tecnologia/Spotify-averigua-canciones-informacion-anunciantes_0_916558486.html

Digital Guide IONOS [en línia] [Data de consulta: 10/03/2020] Disponible a: https://www.ionos.es/digitalguide/paginas-web/derecho-digital/datos-personales/

Digital in 2018 Global Overview [en línia] [Data de consulta: 02/04/2020] Disponible a: https://www.slideshare.net/wearesocial/digital-in-2018-global-overview-86860338

El Hormiguero 3.0 (06/09/2019) *¿Cómo espía Google y cuánto sabe de nosotros?* [vídeo en línia]. Disponible a: https://www.youtube.com/watch?v=jVWMPnjhnuU

Eldiario.es [en línia] *Qué era secreto y qué es lo que siempre hemos sabido del escándalo de Facebook y su influencia en las elecciones* (20/03/2018) [Data de consulta: 20/04/2020] Disponible a: https://www.eldiario.es/tecnologia/secreto-escandalo-Facebook-influencia-elecciones_0_752075814.html

Èmfasi. *Els teus resultats, el nostre objectiu* [en línea] [Data de consulta 16/04/2020] Disponible a: https://www.emfasi.com/ca/glosari/public-objectiu-o-target

FaceApp – Privacy Policy [en línia] [Data de consulta: 17/03/2020] Disponible a: https://www.faceapp.com/privacy-en.html

Fundación Ruiz-Funes - Conferencia Marta Peirano (11/03/2019) *Hacia una societat vigilada*. [vídeo en línia]. Disponible a: https://www.youtube.com/watch?v=LyyPUe9SnAw

LABORDE, Antonia. El País [en línia] *Google recolecta datos médicos de millones de estadounidenses* (13/11/2019). [Data de consulta: 04/04/2020]. Disponible a: https://elpais.com/sociedad/2019/11/12/actualidad/1573547087_635266.html

LATE MOTIV - Marta Peirano. (10/02/2020) El *enemigo conoce el sistema | #LateMotiv657*. [vídeo en línia]. Disponible a:https://www.youtube.com/watch?v=fdRLSVAZWAw

MASA NEGREIRA, Andrés. Quo. [en línia] *Así hacen dinero los data brokers con tus datos en Internet* (22/06/2015). [Data de consulta: 23/03/2020]. Disponible a: https://www.quo.es/tecnologia/a43821/data-brokers/

MediaCloud [en línia] [Data de consulta: 10/03/2020] Disponible a: https://blog.mdcloud.es/que-es-big-data-y-para-que-sirve/

MENDIOLA, José. El País [en línia] *Los riesgos de FaceApp, la aplicación de moda* (18/07/2019) [Data de consulta: 06/04/2020]. Disponible a: https://elpais.com/tecnologia/2019/07/17/actualidad/1563358803_598879.html

MOLINS, Albert. LA Vanguardia [en línia] *Los riesgos de usar FaceApp explicados en ocho preguntas* (18/07/2019) [Data de consulta: 06/04/2020]. Disponible a: https://www.lavanguardia.com/tecnologia/actualidad/20190718/463575580285/faceapp-riesgo-uso-privacidad.html

MOLINS, Albert. La Vanguardia [en línia]. *Ya no vale todo con nuestros datos personales*. (11/05/2018) [Data de consulta: 12/03/2020] Disponible a: https://www.lavanguardia.com/tecnologia/20180511/443481490193/reglamento-de-proteccion-de-datos-informacion-personal-usuarios-internet.html

OLIVERO, Emma. Pickaso [en línia] *Informe: Hábitos de Consumo Mobile en España y en el Mundo en 2018* (19/07/2018) [Data de consulta: 23/04/2020] Disponible a: https://pickaso.com/2018/informe-consumo-mobile-2018

OSI (Oficina de Seguredad del Internatua) [en línia] [Data de consulta: 28/04/2020] Disponible a: https://www.osi.es/es/tu-informacion-personal

PEIRANO. Marta. *El enemigo conoce el sistema*. España: Editorial DEBATE, 2019. ISBN: 9788417636395. Disponible a: https://www.casadellibro.com/libro-el-enemigo-conoce-el-sistema/9788417636395/9501752

Protección de datos: Guía ara el Ciudadano [en línia] [Data de consulta: 17/03/2020] Disponible a: https://www.aepd.es/sites/default/files/2019-10/guia-ciudadano.pdf

S.NADAL, M.Victoria. El País [en línia] *Un antivirus vende datos de navegación que permiten identificar a sus usuarios* (18/01/2020) [Data de consulta: 09/04/2020]. Disponible a: https://elpais.com/tecnologia/2020/01/29/actualidad/1580310699_694737.html

TAPTAP [en línia] [Data de consulta: 23/04/2020] Disponible a: https://www.taptapnetworks.com/about-us/

TEDxMadrid – Marta Peirano (22/09/2015) *¿Por qué me vigilan, si no soy nadie?* [vídeo en línia]. Disponible a: https://www.youtube.com/watch?v=NPE7i8wuupk

Test de privacidad [en línea] [Data de consulta 22/04/2020] Disponible a: https://testdeprivacidad.org/

TICS - Tecnologías de Información y Comunicación [en línea] [Data de consulta 16/04/2020] Disponible a: https://www.monografias.com/trabajos89/tics-tecnologias-informacion-y-comunicacion/tics-tecnologias-informacion-y-comunicacion.shtml

TV3 a la Carta - 30 minuts. (25/08/2013). *Penjats@Internet* [vídeo en línia]. Disponible a https://www.ccma.cat/tv3/alacarta/30-minuts/penjatsinternet/video/4612751/

TV3 a la Carta – No pot ser! (14/04/2019). *Big Data, Big Brother* [vídeo en línia]. Disponible a https://www.ccma.cat/tv3/alacarta/no-pot-ser/big-data-big-brother/video/5836380/

TV3 a la Carta – Sense ficció. (09/06/2015). *Big Data. Ciutadans sota control*. [vídeo en línia]. Disponible a https://www.ccma.cat/tv3/alacarta/sense-ficcio/big-data-ciutadans-sota-control/video/5530421/

VIX ¿Qué es un hacker? [en línea] [Data de consulta 16/04/2020] Disponible a: https://www.vix.com/es/btg/tech/13182/que-es-un-hacker

Wikipedia [en línea] [Data de consulta 16/04/2020] Disponible a: https://es.wikipedia.org/wiki/Dato

Wikipedia [en línea] [Data de consulta 16/04/2020] Disponible a: https://ca.wikipedia.org/wiki/Algorisme

Wikipedia [en línea] [Data de consulta 16/04/2020] Disponible a: https://ca.wikipedia.org/wiki/Identificaci%C3%B3_biom%C3%A8trica

Wikipedia [en línea] [Data de consulta 16/04/2020] Disponible a: https://ca.wikipedia.org/wiki/Usuari

Wikipedia [en línea] [Data de consulta 16/04/2020] Disponible a: https://ca.wikipedia.org/wiki/Segmentaci%C3%B3_de_mercat

Wikipedia [en línea] [Data de consulta 16/04/2020] Disponible a:https://ca.wikipedia.org/wiki/Galeta_(inform%C3%A0tica)

Wikipedia [en línea] [Data de consulta 30/04/2020] Disponible a: https://ca.wikipedia.org/wiki/Criptografia

ANNEX

ENQUESTA

A l'abril del 2020 vaig realitzar una enquesta per poder valorar i comprovar si estem al cas de la indústria del tràfic de dades i què en pensen els usuaris amb l'objectiu de contestar les preguntes que em proposo resoldre amb aquest treball.

La primera pregunta era sobre l'edat dels enquestats per posteriorment dividir-los en tres blocs: menors de vint-i-cinc anys, persones entre vint-i-cinc i cinquanta anys i, per últim, més grans de cinquanta anys.

A partir de l'edat, les preguntes eren:

- Creus que els dispositius que fem servir en el nostre dia a dia (mòbil, rellotge intel·ligent, assistent de veu...) respecten la nostra intimitat i privacitat?
  - ✓ Sí.
  - ✓ No.
  - ✓ No ho sé.

- Per a desbloquejar el telèfon mòbil fas servir…
  - ✓ L'empremta
  - ✓ Número pin
  - ✓ Reconeixement facial.
  - ✓ Altres.
  - ✓ No utilitzo el desbloqueig de pantalla.

- Quan et descarregues una aplicació, et llegeixes les polítiques d'ús i privacitat?
  - ✓ No, mai.
  - ✓ Una mica, per sobre.
  - ✓ Només alguns apartats.
  - ✓ Sí, sempre.

- Penses que les empreses que tenen accés a les nostres dades personals ho poden saber tot de nosaltres?
  - ✓ Sí, poden saber-ho tot de nosaltres.
  - ✓ Sí, tot i que només del que en donem consentiment.
  - ✓ No, tot no ho poden saber.

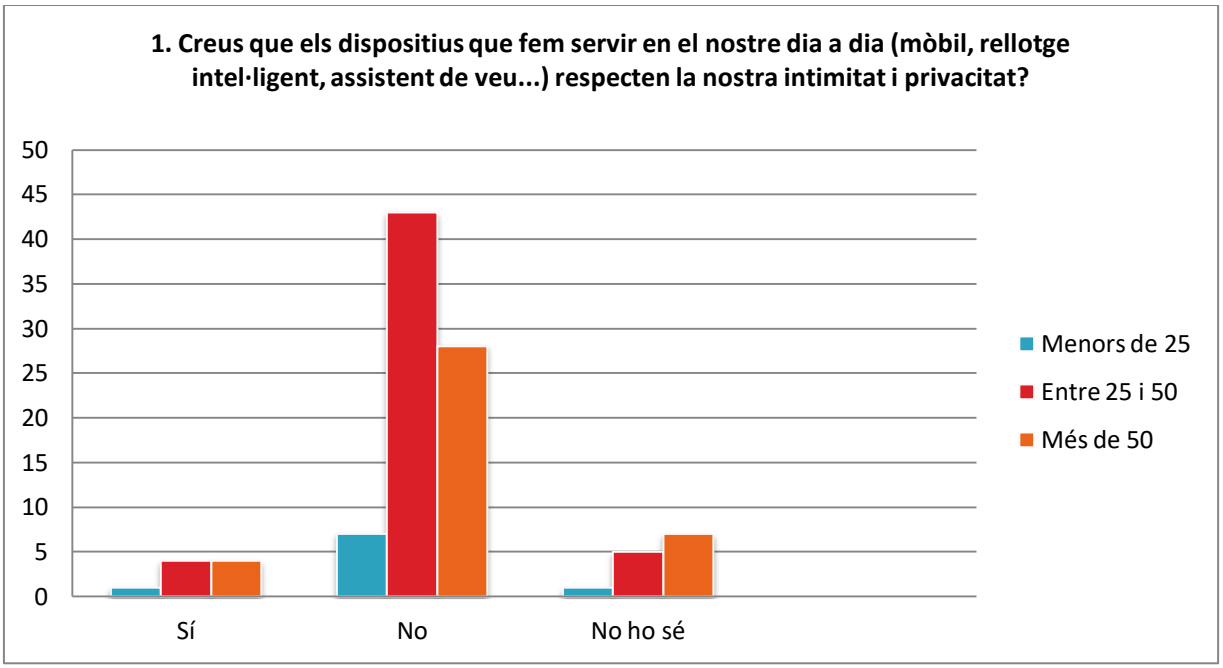
  - ✓ No ho sé.

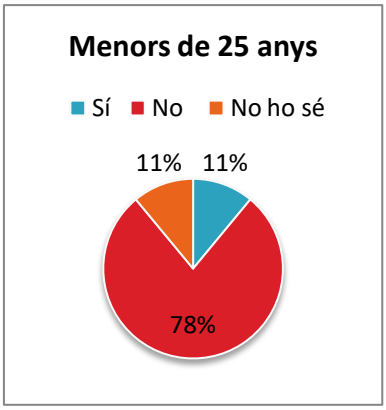
- És un tema que et preocupa?
  - ✓ Bastant.
  - ✓ Poc.
  - ✓ Molt.
  - ✓ Gens.

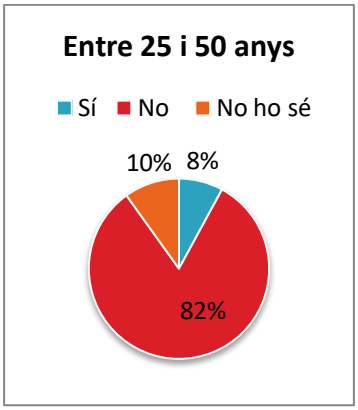
- En quant a l'ús i la privacitat de les nostres dades personals, creus que en fas un ús responsable alhora d'establir els teus límits a la xarxa?
  - ✓ Sí.
  - ✓ No.
  - ✓ No ho sé.

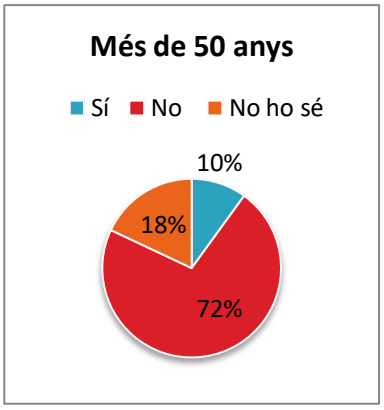
- Quin creus que pot ser el principal interès de les empreses que treballen amb les nostres dades personals?
  - ✓ Finalitats publicitàries.
  - ✓ Finalitats de control.
  - ✓ Finalitats de seguretat.
  - ✓ Finalitats polítiques.
  - ✓ Altres.
  - ✓ No ho sé.
- T'agradaria saber el que aquestes empreses saben de tu?
  - ✓ Sí, estic en el meu dret.
  - ✓ Prefereixo no saber-ho.
  - ✓ Tant me fa.
  - ✓ No ho sé.

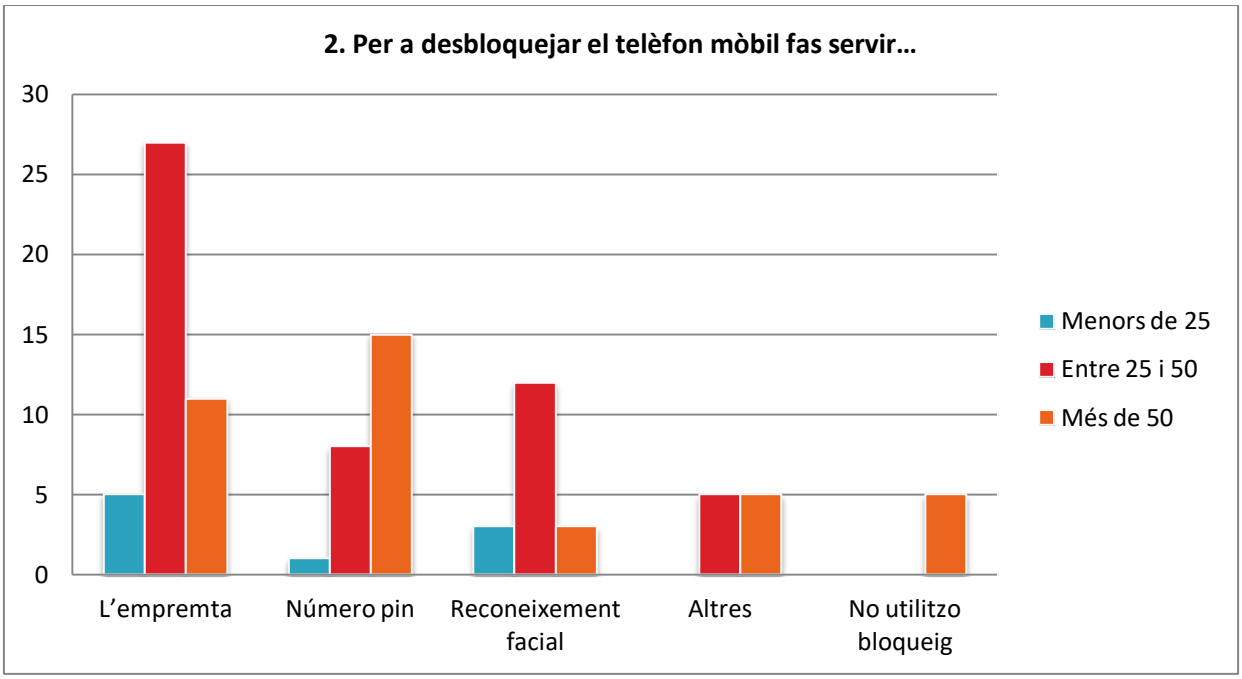
Per presentar els resultats de l'enquesta de manera molt més clara i entenedora, he dividit els resultats en columnes on es mostra què ha contestat cadascun dels tres blocs d'edats (menors de vint-i-cinc anys, entre vint-i-cinc i cinquanta anys i més grans de cinquanta anys), seguidament de gràfics circulars on veurem els tant per cent de les respostes segons les edats dels enquestats.

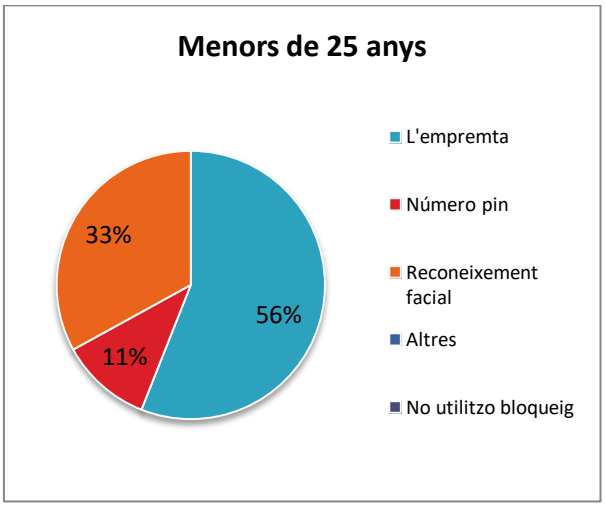

1. Creus que els dispositius que fem servir en el nostre dia a dia (mòbil, rellotge intel·ligent, assistent de veu...) respecten la nostra intimitat i privacitat?
50
45
40
35
30
25
20
15
10
5
0
Sí
No
No ho sé
Menors de 25
Entre 25 i 50
Més de 50

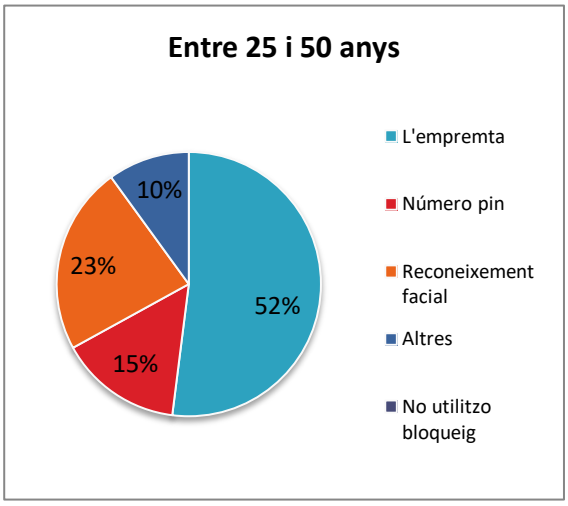

Menors de 25 anys
Sí
No
No ho sé
11%
11%
78%

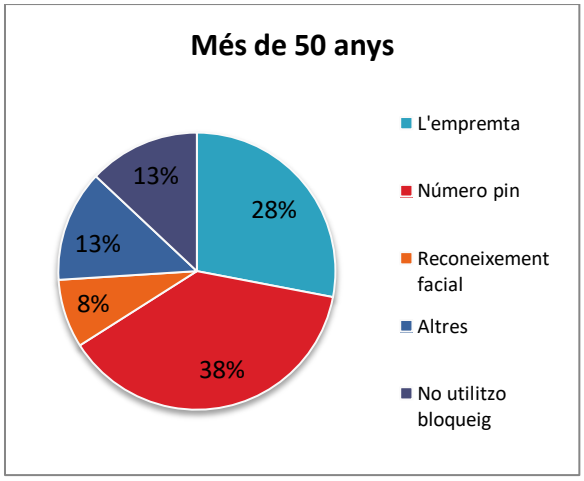

Entre 25 i 50 anys
Sí
No
No ho sé
10%
8%
82%

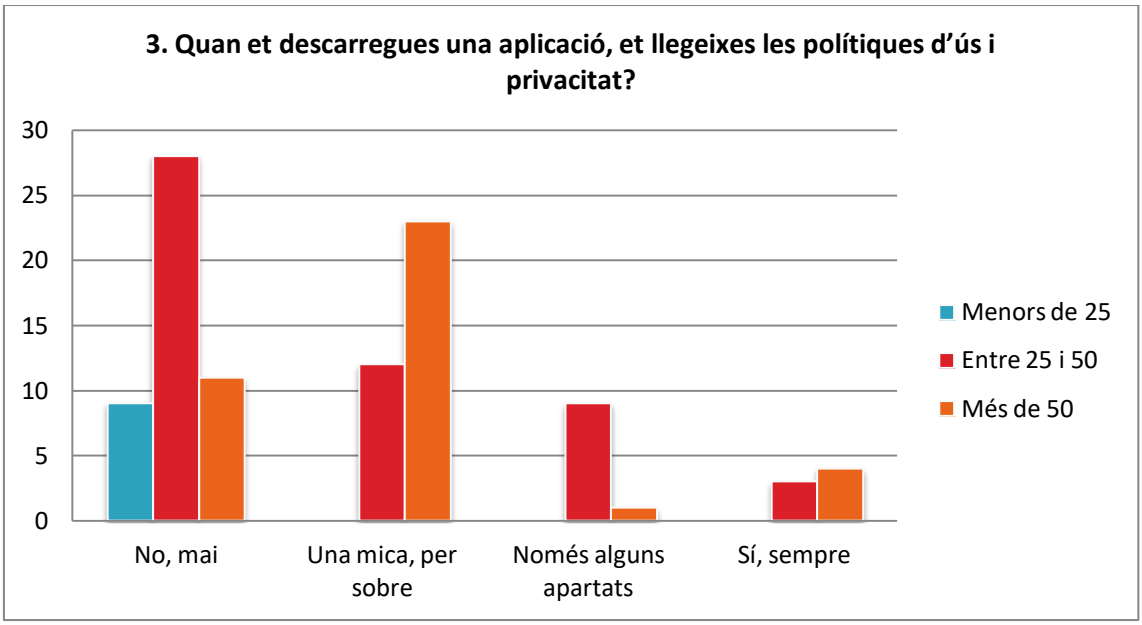

Més de 50 anys
Sí
No
No ho sé
10%
18%
72%

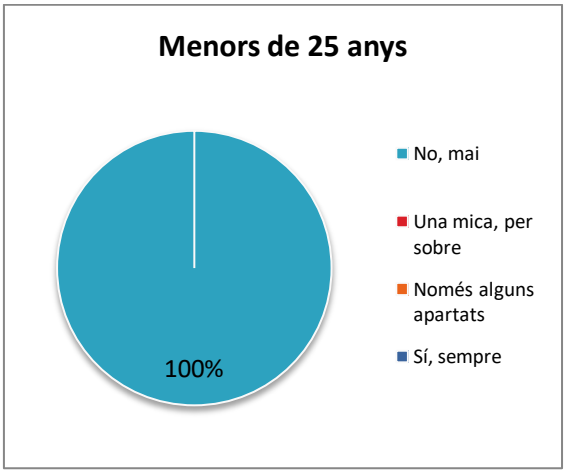

2. Per a desbloquejar el telèfon mòbil fas servir...
30
25
20
15
10
5
0
L'empremta
Número pin
Reconeixement facial
Altres
No utilitzo bloqueig
Menors de 25
Entre 25 i 50
Més de 50

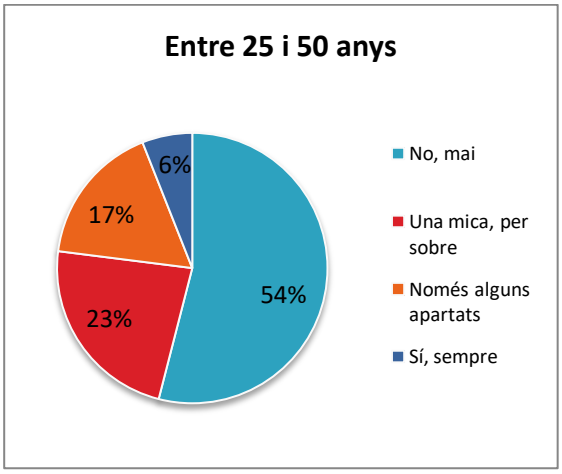

Menors de 25 anys
56%
11%
33%
L'empremta
Número pin
Reconeixement facial
Altres
No utilitzo bloqueig

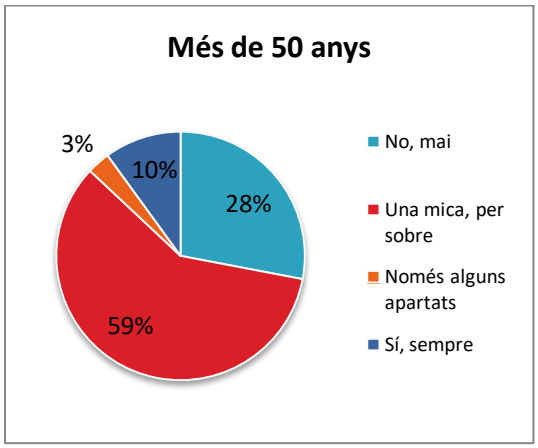

Entre 25 i 50 anys
52%
15%
23%
10%
L'empremta
Número pin
Reconeixement facial
Altres
No utilitzo bloqueig

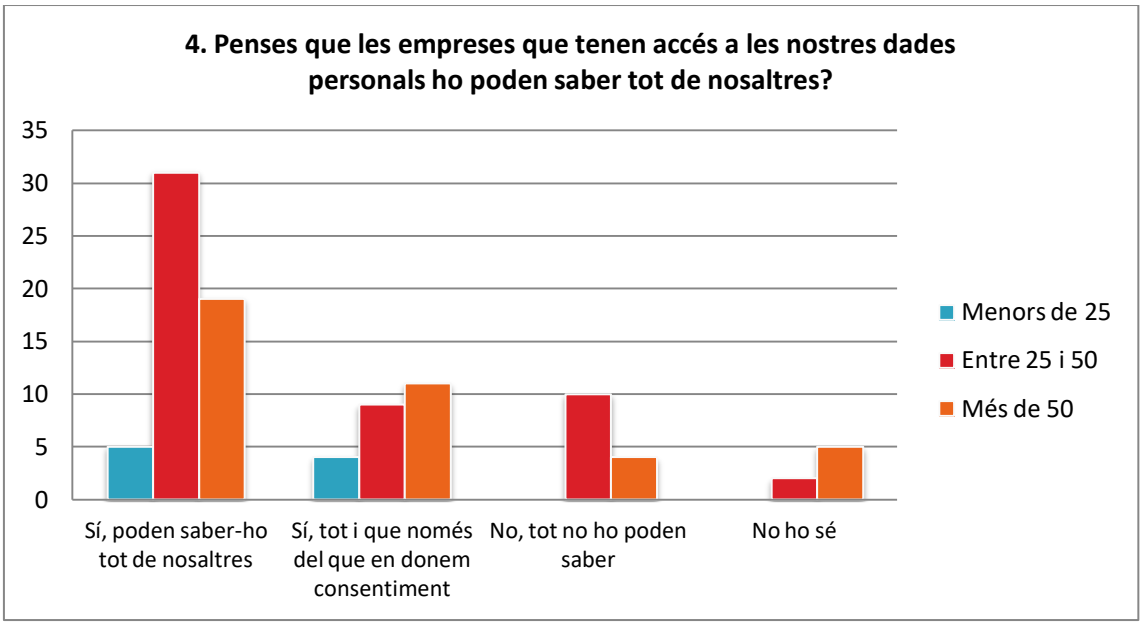

Més de 50 anys
28%
38%
8%
13%
13%
L'empremta
Número pin
Reconeixement facial
Altres
No utilitzo bloqueig

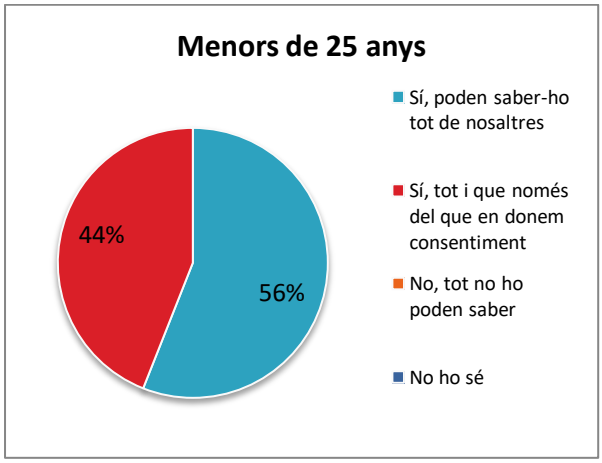

3. Quan et descarregues una aplicació, et llegeixes les polítiques d'ús i privacitat?
30
25
20
15
10
5
0
No, mai
Una mica, per sobre
Només alguns apartats
Sí, sempre
Menors de 25
Entre 25 i 50
Més de 50

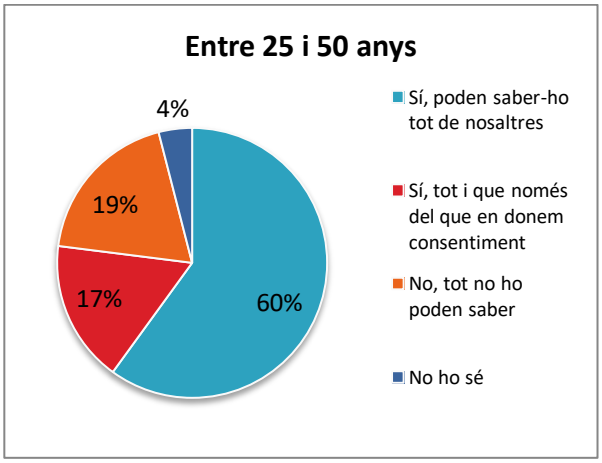

Menors de 25 anys
100%
No, mai
Una mica, per sobre
Només alguns apartats
Sí, sempre

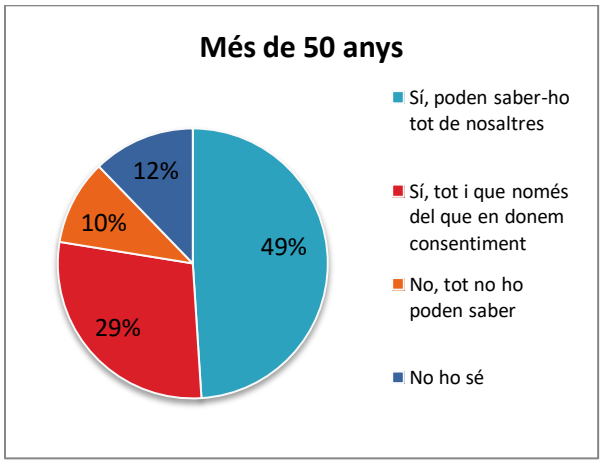

Entre 25 i 50 anys
6%
17%
54%
23%
No, mai
Una mica, per sobre
Només alguns apartats
Sí, sempre

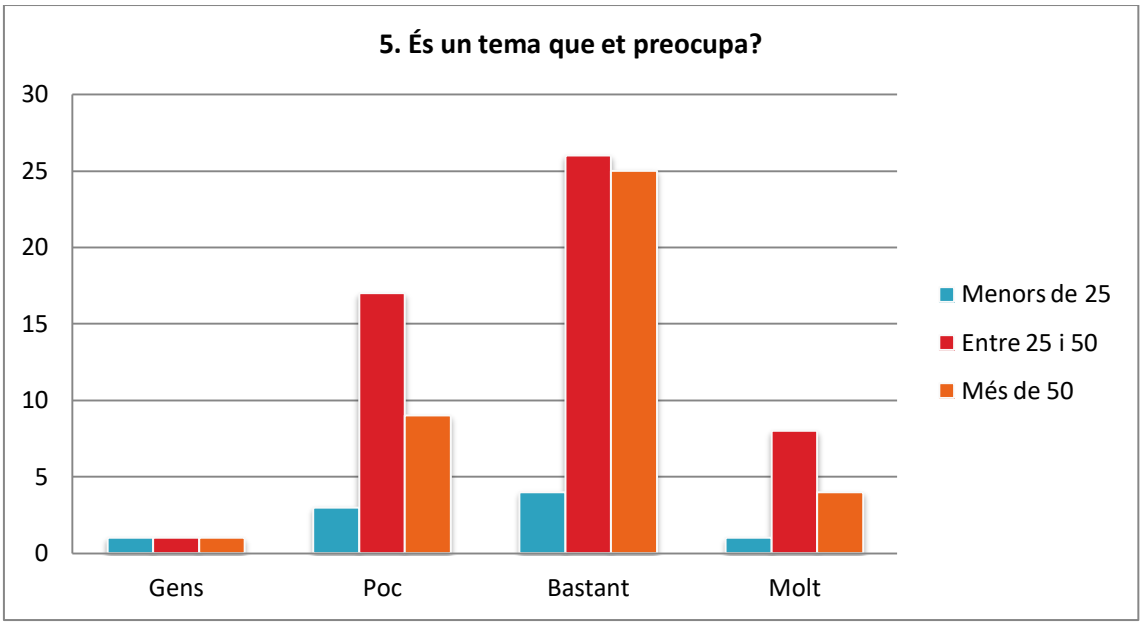

Més de 50 anys
3%
10%
28%
59%
No, mai
Una mica, per sobre
Només alguns apartats
Sí, sempre

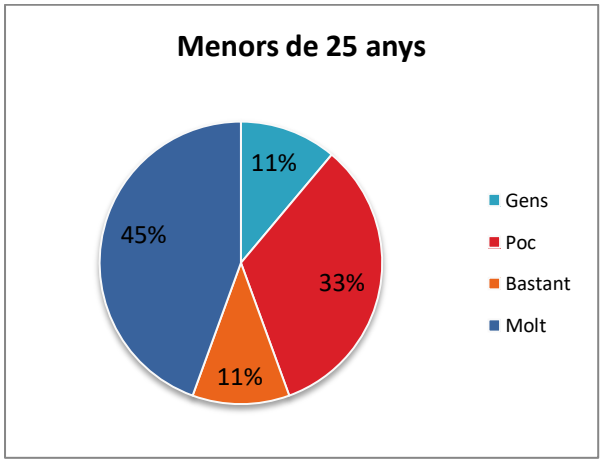

4. Penses que les empreses que tenen accés a les nostres dades personals ho poden saber tot de nosaltres?
35
30
25
20
15
10
5
0
Sí, poden saber-ho tot de nosaltres
Sí, tot i que només del que en donem consentiment
No, tot no ho poden saber
No ho sé
Menors de 25
Entre 25 i 50
Més de 50

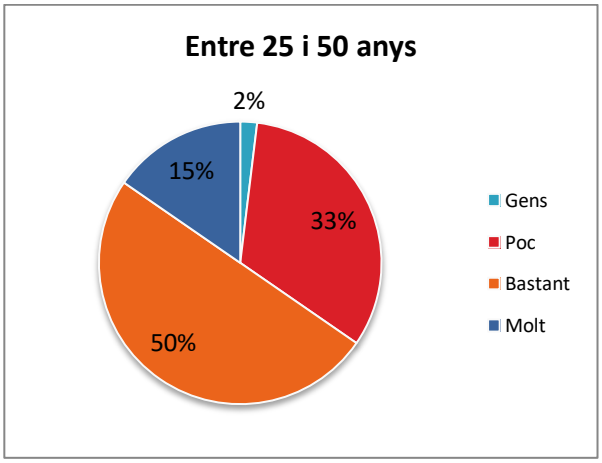

Menors de 25 anys
44%
56%
Sí, poden saber-ho tot de nosaltres
Sí, tot i que només del que en donem consentiment
No, tot no ho poden saber
No ho sé

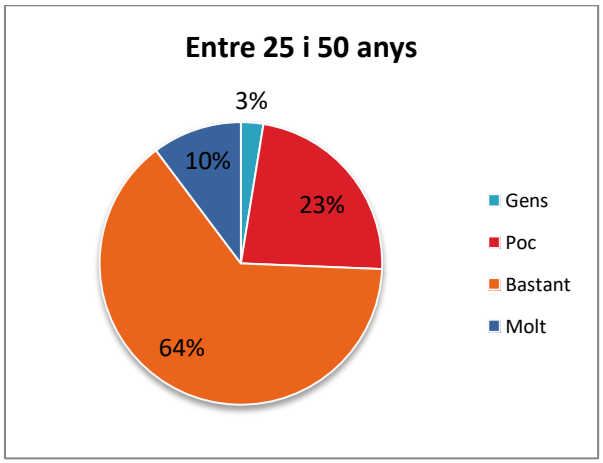

Entre 25 i 50 anys
4%
19%
17%
60%
Sí, poden saber-ho tot de nosaltres
Sí, tot i que només del que en donem consentiment
No, tot no ho poden saber
No ho sé

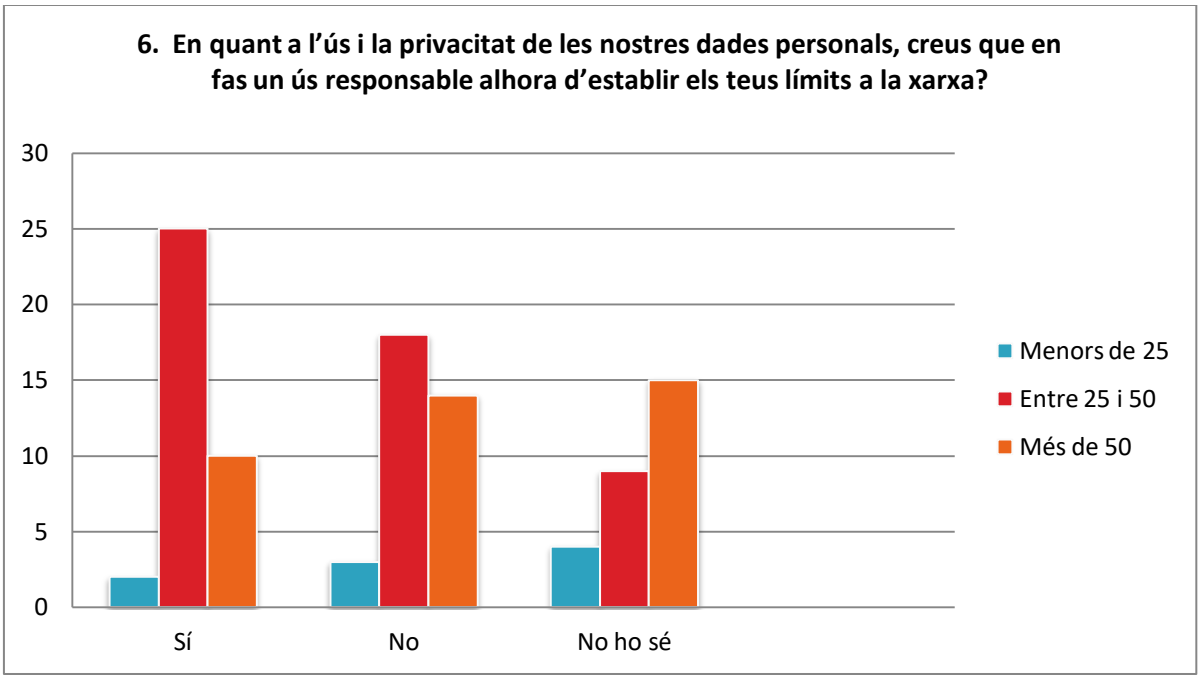

Més de 50 anys
12%
10%
49%
29%
Sí, poden saber-ho tot de nosaltres
Sí, tot i que només del que en donem consentiment
No, tot no ho poden saber
No ho sé

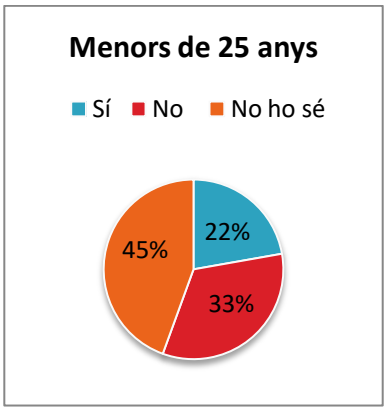

5. És un tema que et preocupa?
30
25
20
15
10
5
0
Gens
Poc
Bastant
Molt
Menors de 25
Entre 25 i 50
Més de 50

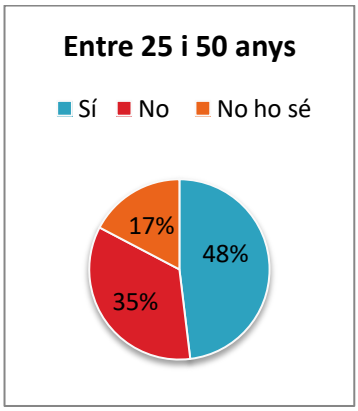

Menors de 25 anys
11%
33%
11%
45%
Gens
Poc
Bastant
Molt

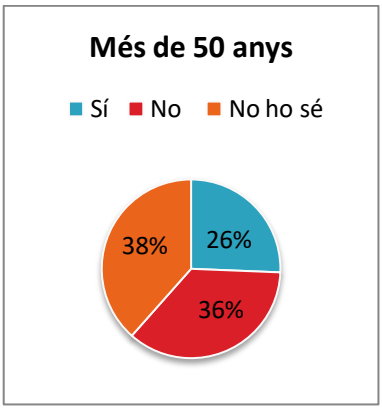

Entre 25 i 50 anys
2%
15%
33%
50%
Gens
Poc
Bastant
Molt

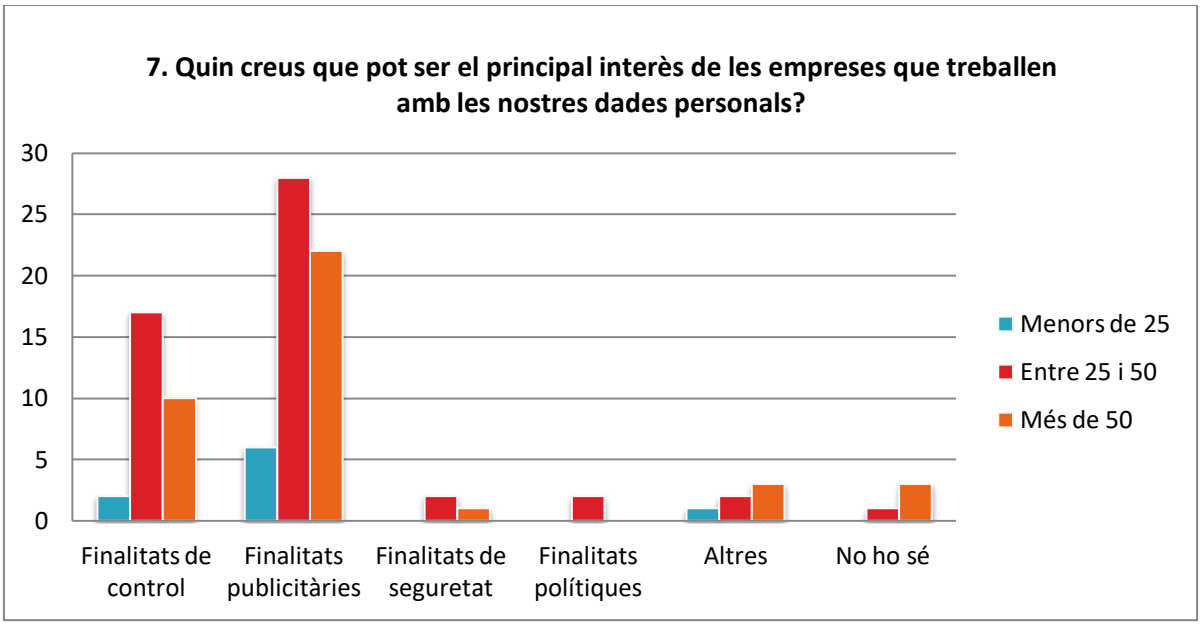

Entre 25 i 50 anys
3%
10%
23%
64%
Gens
Poc
Bastant
Molt

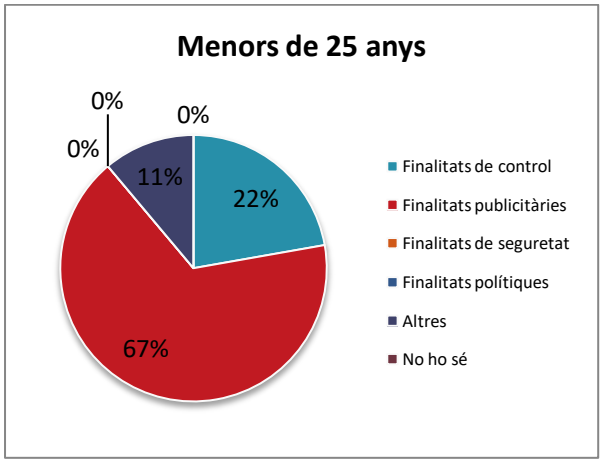

6. En quant a l'ús i la privacitat de les nostres dades personals, creus que en fas un ús responsable alhora d'establir els teus límits a la xarxa?
30
25
20
15
10
5
0
Sí
No
No ho sé
Menors de 25
Entre 25 i 50
Més de 50

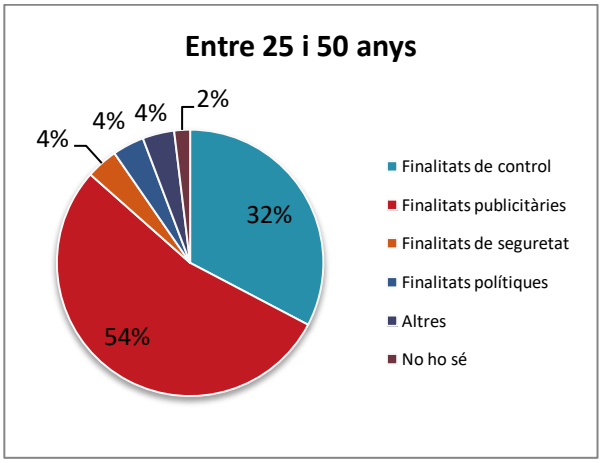

Menors de 25 anys
Sí
No
No ho sé
22%
33%
45%

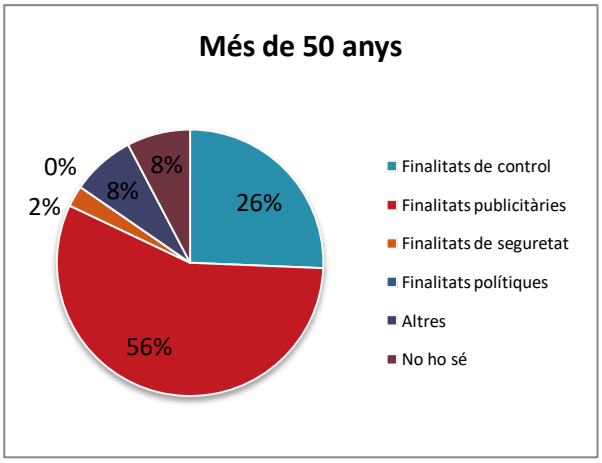

Entre 25 i 50 anys
Sí
No
No ho sé
48%
35%
17%

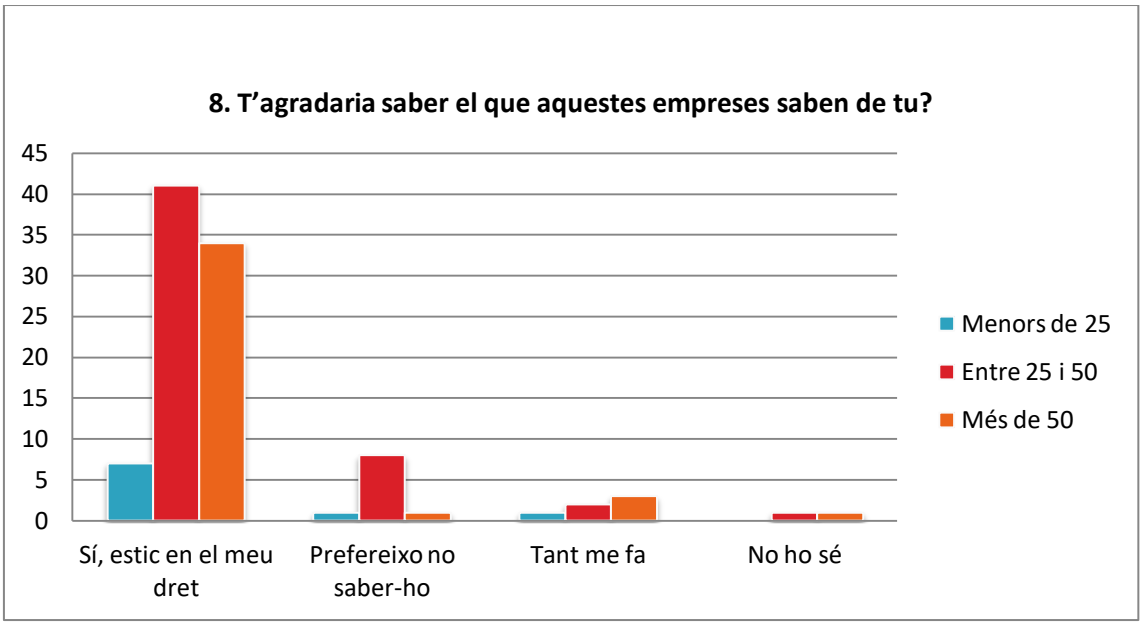

Més de 50 anys
Sí
No
No ho sé
26%
36%
38%

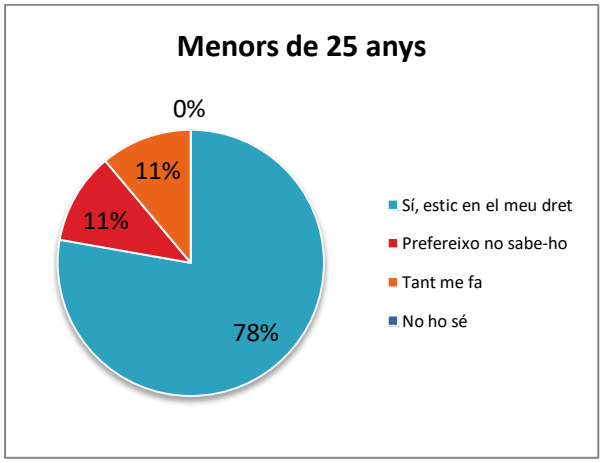

7. Quin creus que pot ser el principal interès de les empreses que treballen amb les nostres dades personals?
30
25
20
15
10
5
0
Finalitats de control
Finalitats publicitàries
Finalitats de seguretat
Finalitats polítiques
Altres
No ho sé
Menors de 25
Entre 25 i 50
Més de 50

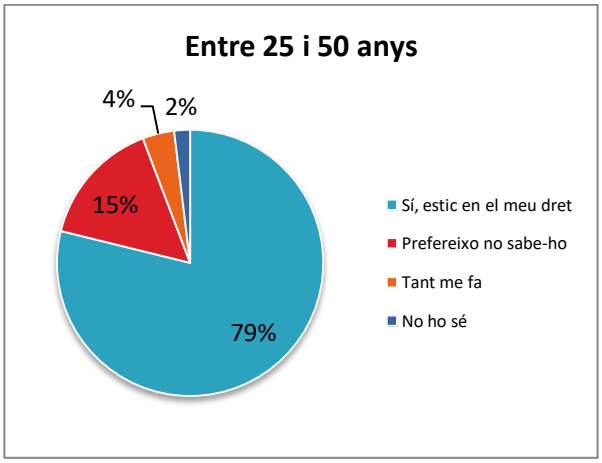

Menors de 25 anys
0%
0%
0%
11%
22%
67%
Finalitats de control
Finalitats publicitàries
Finalitats de seguretat
Finalitats polítiques
Altres
No ho sé

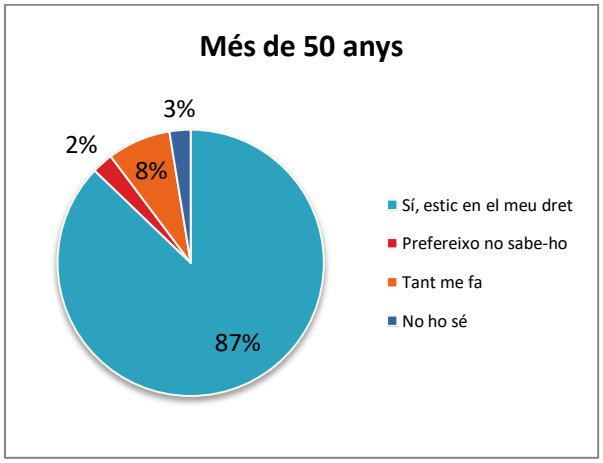

Entre 25 i 50 anys
4%
4%
4%
2%
32%
54%
Finalitats de control
Finalitats publicitàries
Finalitats de seguretat
Finalitats polítiques
Altres
No ho sé


Més de 50 anys
0%
2%
8%
8%
26%
56%
Finalitats de control
Finalitats publicitàries
Finalitats de seguretat
Finalitats polítiques
Altres
No ho sé


8. T'agradaria saber el que aquestes empreses saben de tu?
45
40
35
30
25
20
15
10
5
0
Sí, estic en el meu dret
Prefereixo no saber-ho
Tant me fa
No ho sé
Menors de 25
Entre 25 i 50
Més de 50


Menors de 25 anys
0%
11%
11%
78%
Sí, estic en el meu dret
Prefereixo no sabe-ho
Tant me fa
No ho sé


Entre 25 i 50 anys
4%
2%
15%
79%
Sí, estic en el meu dret
Prefereixo no sabe-ho
Tant me fa
No ho sé


Més de 50 anys
3%
2%
8%
87%
Sí, estic en el meu dret
Prefereixo no sabe-ho
Tant me fa
No ho sé

8.1. Conclusions de l'enquesta.

Un cop feta l'enquesta podem afirmar que la gran majoria d'usuaris d'smartphone, auriculars intel·ligents, assistents de veu, etcètera, creuen que no respecten la nostra intimitat (el 78% dels menors de vint-i-cinc anys, el 82% d'entre vint-i-cinc i cinquanta anys, i el 72% dels més grans de cinquanta anys).

Com hem vist, el mètode més segur de desbloquejar el telèfon mòbil és el número pin, ja que no conté cap dada biomètrica nostre. Els que més utilitzen aquest mètode són les persones de més de cinquanta anys, sent el més utilitzat amb un 38% dels enquestats, seguit de l'empremta i, molt per sota amb un 13%, altres mètodes de desbloqueig o els que directament no utilitzen cap; per últim un 8% utilitza el reconeixement facial. El menys utilitzat per les persones de més de cinquanta anys és el reconeixement facial, mentre que tant pels menors de vint-i-cinc com pel grup de persones d'entre vint-i-cinc i cinquanta anys, és el segon més utilitzat després de l'empremta. Amb un 56% dels menors de vint-i-cinc i un 52% dels d'entre vint-i-cinc i cinquanta, l'empremta és el mètode que més de la meitat dels enquestats fan servir, precisament el mètode que aprofita una de les dades personals nostres més importants i personals, única i identificable.

Quan la majoria dels enquestats es descarreguen una aplicació, no es llegeixen les polítiques d'ús i privacitat. Dels menors de vint-i-cinc anys tots han contestat que mai se les llegeixen, una dada que és preocupant perquè són precisament el grup que més actiu està a la xarxa i publica més contingut personal sense saber quin ús fan les aplicacions de les seves dades. Tanmateix la majoria dels més grans de cinquanta anys diuen que es llegeixen les polítiques una mica, per sobre (58%). El que és sorprenent és que uns quants enquestats han contestat que sí que se les llegeixen sempre (un 6% de les persones d'entre vint-i-cinc i cinquanta anys i un 10% dels majors de cinquanta) tenint en compte que moltes aplicacions, la gran majoria, publiquen el document de les polítiques amb una gran quantitat de pàgines que resulta interminable per qualsevol persona que es descarregui una aplicació. Ho fan expressament perquè quan l'usuari veu que son tres-centes pàgines de document, no ho llegeix i accepta sense mirar res.

La gran majoria dels enquestats dels tres blocs d'edat pensen que les empreses que tenen accés a les nostres dades personals sí que ho poden saber tot de nosaltres.

En general, és un tema que preocupa bastant als usuaris, especialment a les persones de vint-i-cinc anys cap amunt. Tot i això, hi ha un alt percentatge, sobretot del grup de persones d'entre vint-i-cinc i cinquanta anys, que els preocupa poc (amb un 33%) i a un 11% dels menors de vint-i-cinc anys, un 2% dels d'entre vint-i-cinc i cinquanta i un 3% dels de més de cinquanta no els preocupa gens.

La pregunta que més diversitat d'opinions ha estat: "En quant a l'ús i la privacitat de les nostres dades personals, creus que en fas un ús responsable a l'hora d'establir els teus límits a la xarxa?" No hi ha cap resposta que destaqui més que cap altra; de fet, en general, gairebé la meitat dels menors de vint-i-cinc anys han contestat que no saben si en fan un ús responsable (amb un 45%), la majoria dels d'entre vint-i-cinc i cinquanta anys pensen que sí que en fan un ús responsable (amb un 48%). En canvi els més grans de cinquanta anys han tingut molta diversitat d'opinions: un 26% pensa que sí que en fa ús responsable, un 36% pensa que no, i el 38% restant no ho té clar. Aquestes respostes ens demostren i confirmen que no acabem d'estar segurs de si fem un bon ús i això ens crea una certa incertesa.

La majoria d'enquestats coincideixen amb l'afirmació que el principal interès de les empreses que treballen amb les nostres dades ho fan amb finalitats públiques (67% dels menors de vint-i-cinc anys, 54% d'entre vint-i-cinc i cinquanta anys i un 56% dels majors de cinquanta), tot i que hi ha uns quants que pensen que ho fan amb finalitats de control i altres grups molt més reduïts pensen que són per finalitats de seguretat, política i d'altres, mentre que un percentatge molt petit no sap exactament quin és l'interès d'aquestes empreses.

Per acabar, l'última pregunta era per esbrinar si als usuaris els agradaria saber el que aquestes empreses realment coneixen de nosaltres i va ser la pregunta en la qual tots els grups d'edat van coincidir; una gran majoria de tots tres grups va contestar que sí, que estan en el seu dret de saber tot el que aquestes empreses puguin saber d'ells (el 78% dels menors de vint-i-cinc anys, el 79%

dels d'entre vint-i-cinc i cinquanta i un 87% dels majors de cinquanta) mentre que la resta va contestar que els hi era igual saber-ho, altres que preferien no saber-ho i molt pocs no ho sabien.