UNIVERSITAT DE BARCELONA
Facultat d'Economia i Empresa

L'empremta digital i els seus reptes

Una aproximació a què és, com és utilitzada i els seus avantatges i desavantatges

Anna Chun Wu Esteban Reales

Tutor: José Antonio Rodríguez Díaz

Juny 2023

Treball Final de Grau

Departament de Sociologia

RESUM

La recopilació de dades massiva és al centre d'importants debats per part d'investigadors i acadèmics de diferents camps científics, alhora que la normalització del seu ús ha generat un gran nombre de preocupacions socials que van des de la vigilància massiva fins a la predicció d'hàbits de consum. Aquest fenomen emergent aporta reptes i desafiaments que apunten a un canvi social i tecnològic.

En aquest treball es pretén realitzar una aproximació al concepte d'empremta digital i *Big Data*. Es vol estudiar aquestes noves tècniques d'obtenció i manipulació d'informació i les seves utilitats.

Paraules clau: empremta digital - Big Data – xarxes socials – control – protecció de dades.

ABSTRACT

Mass data collection is at the center of important debates by researchers and academics in different scientific fields, while the normalization of its use has generated a large number of social concerns ranging from mass surveillance to prediction consumption habits. This emerging phenomenon brings challenges that point to a social and technological change.

In this work, it is intended to make an approach to the digital fingerprint and Big Data concept. We want to study these new techniques for obtaining and manipulating information and their uses.

Keywords: digital footprint - Big Data - social networks - control - data protection.

ÍNDEX

I. INTRODUCCIÓ

El món actual ja no és comprensible sense el concepte d'Internet, i no es poden ignorar els rastres d'informació que queden a la xarxa dels milions d'usuaris que es connecten diàriament. Tenim el telèfon mòbil amb nosaltres la gran part del temps i en fem ús d'aquest molt seguit. Els mòbils deixen un rastre de la nostra localització a cada moment, dels llocs on comprem, del que busquem per Internet o de les pàgines a les que accedim, de dades personals i de comentaris a les xarxes socials. Aquest rastre que deixen a Internet les persones és anomenat empremta digital. És el que ens representa a l'espai digital, i en la majoria dels casos és beneficiosa per a l'usuari, però en d'altres pot ser realment nociva, ja que mai no és irrellevant. S'ha arribat a un punt en què les tecnologies digitals s'han tornat invisibles. Algunes persones poden afirmar que les seves vides no s'han digitalitzat en cap mesura, que les seves maneres de treballar, socialitzar, moure's per l'espai, participar en la vida familiar o les relacions íntimes han canviat poc perquè es neguen a utilitzar dispositius informàtics. No obstant això, aquests individus parlen des d'una posició que només serveix per posar en relleu com de discreta pot ser la digitalització de les persones, ja que fins i tot les persones que defugen de l'ús d'un telèfon intel·ligent, d'una càmera digital o d'una plataforma de xarxes socials, es veuen en una situació d'interacció amb les que sí que en fan d'ús. Així mateix, pot donar-se el cas de que imatges digitals o fitxers d'àudio d'aquestes persones realitzats amb aquestes tecnologies es pengin i es facin circular per altres sense el seu coneixement o consentiment.

Aquests registres representen el *Big Data*, i és informació sobre nosaltres que pot servir a tercers per guanyar diners o conèixer les nostres preferències i poder vendre millor els seus productes. Aquesta nova eina d'anàlisi de dades és especialment útil a l'hora de detectar patrons de compra nous i oferir experiències de client més personalitzades, a més d'una millor comprensió del nou comportament dels consumidors.

Es definirà el problema de recerca al voltant a l'estudi de les noves tècniques d'obtenció i manipulació de dades en la societat actual. Per això s'incorporarà el concepte de *Big Data*, que és un terme utilitzat per descriure el gran volum de dades que composen Internet i la possibilitat d'obtenir informació sobre les persones. Les dades que els individus proveeixen a les xarxes socials digitals són fonamentals per definir la personalitat de cadascun de ells i tenir una idea més clara a l'hora de dirigir-los missatges, propostes, idees, etc. De fet, el *Big Data* pot ser definit com un registre i sistematització d'empremtes digitals de tot allò que realitzem "*online*" i "*offline*", i que pot quedar consignat en algun dispositiu digital.

1.1. OBJECTIUS I HIPÒTESI

En aquest treball es parteix de la hipòtesi de que la gent no és totalment conscient de la seva empremta digital, dels seus usos ni dels perills que comporta. En aquest treball de recerca es pretén arribar a:

I. Conèixer què és l'empremta digital i els seus usos.
II. Conèixer el motiu de la creixent normalització de l'ús de les nostres empremtes digitals, ja sigui per empreses, organitzacions polítiques, etc.
III. Evidenciar que l'empremta digital és un fenomen social recent i molt poderós.
IV. Cercar solucions per a protegir la nostra empremta digital, si és possible.

1.2. METODOLOGIA

Per aconseguir els objectius del treball, la metodologia s'ha organitzat en dues parts. La primera és una investigació de les fonts secundàries, fonamentalment a través de llibres i articles acadèmics, obtinguts, en bona part, de fons oficials com ISI Web Of Science, Cercabib i Google Schoolar. Per realitzar la recerca de les fonts d'informació s'ha hagut de fer una cerca sistemàtica d'articles i llibres que abordessin aquest tema i donessin resposta a una sèrie de qüestions. En primer lloc havien de parlar del fenomen de l'empremta digital i el *Big Data*. Havien de parlar sobre el paper dels governs i/o les empreses, i l'ús que li donen, així com sobre els pros i contres de l'empremta digital, sobre l'opinió pública i sobre regulacions de protecció de dades. A part d'articles científics, també s'ha fet ús d'articles de revistes sensacionalistes, articles d'opinió, publicacions a les xarxes socials, etc. per tindre un altre punt de vista. S'ha recorregut a Twitter, Reddit i Discord per conèixer el que els usuaris diuen sobre l'empremta digital i el *Big Data*. A Twitter s'han fet cerques de *tweets* amb el *hashtag bigdata (#bigdata)*. A Reddit s'han fet cerques de discussions que tractin qualsevol dels dos conceptes. Finalment a Discord s'han trobat comunitats i grups de gent que parlen del tema en línia.

La segona part ha sigut una investigació quantitativa on s'ha creat una enquesta i extret informació d'altres enquestes oficials anteriorment realitzades, per contrastar o complementar la informació de les fonts secundàries. L'enquesta d'elaboració pròpia s'ha enviat a persones de totes les edats i nivells educatius. Ha servit per saber si els enquestats coneixien el terme de l'empremta digital i per conèixer si els usuaris veuen aquest fenomen com una cosa positiva o negativa. Les enquestes realitzades per altres empreses dóna una mostra més extensa i un ventall més ampli de preguntes i respostes.

II. MARC TEÒRIC

L'empremta digital i el *Big Data* són dos conceptes diferents però relacionats entre ells. L'empremta digital fa referència a la informació que deixem en línia sobre nosaltres mateixos. Estem acostumats a mirar tota mena d'informació a Internet, però, també ens estan mirant a nosaltres. Cada vegada que busquem informació a la web, quan compartim alguna cosa a les xarxes socials, enviem un missatge instantani o enviem un correu electrònic, anem deixant un rastre d'informació. Les empremtes digitals poden oferir comoditat, com per exemple, a l'hora d'iniciar una sessió a una aplicació, ja que podem tenir desat el nostre usuari i contrasenya. L'elaboració de un perfil es basa en la recopilació d'informació i cerques dels usuaris i l'extracció de dades de configuració de les aplicacions, de geolocalització, dels programes instal·lats, etc. Si combinem tota aquesta informació i les dades extretes es confeccionarà el que anomenem empremta digital única de cada dispositiu i, per tant, és diferent per a cada usuari.

D'altra banda, el *Big Data* fa referència a grans conjunts de dades que es poden analitzar per obtenir informació útil. Aquest rastre pot ser utilitzat per determinades organitzacions en benefici seu segons siguin els seus interessos. És un tema d'interès i de preocupació ja que cada vegada creix més i la gent parla d'aquest. L'any 1989 Erik Larson utilitza per primera vegada el terme Big Data, en un article sobre el màrqueting i com es faran servir les dades dels clients, en els termes que actualment coneixem (IGN, 2017).

El desenvolupament dels cercadors des de mitjans de la dècada dels 90 del segle passat i l'alt grau de centralització de la informació, materialitzada en la creació de gegants repositoris de dades gestionats per grans empreses privades o pels Estats, van acabar cridant l'atenció sobre les potencialitats de l'ús d'una informació tan enorme. L'augment significatiu de la capacitat d'emmagatzematge i de la velocitat del processament van completar el quadre que va donar lloc al sorgiment del *Big Data*, que no és cap altra cosa que el conjunt de tècniques usades per a la selecció, el maneig i la interpretació de milers de milions de dades que permeten inferir tendències, extraient informació de miríades de casos puntuals que estan succeint o han succeït. Per exemple, determinar les variacions en temps real de la demanda d'un producte, incloent-hi el color preferit pels consumidors, és un dels casos més comuns de l'aplicació d'aquest tipus de tècniques.

Actualment s'ha convertit en una eina de control molt utilitzada per les empreses amb l'objectiu de conèixer les nostres preferències o, fins i tot, per contractar a gent. Es podria dir que el principal objectiu de l'anàlisi del *Big Data* és transformar immenses quantitats de dades incorrelades en una cosa útil per a la presa de decisions. Les possibilitats que ofereix *Big Data* són pràcticament infinites i es pot trobar una aplicació pràctica a gairebé tots els sectors. Algunes poden ser més intuïtives, com la detecció de tendències complexes que permetin

prendre decisions en mercats d'actius financers o avançar-se a qualsevol tipus de desastre natural o meteorològic. D'altres, més sociològiques: mitjançant l'anàlisi de patrons de text a Twitter es pot entendre i predir el comportament i el sentiment d'un grup social o detectar *gaps* de coneixement entre els més joves per establir plans d'estudi. També podeu augmentar la nostra qualitat de vida millorant diagnòstics mèdics gràcies a la correlació de multitud de proves mèdiques digitals.

El 2001, Doug Laney va detallar que el *Big Data* es caracteritzava per tres trets: volum, velocitat i varietat. Des de llavors altres autors han atribuït altres qualitats, com la característica de valor (Marr, 2014) A continuació, definirem aquestes característiques:

1) Volum: tradicionalment, les dades s'han generat de forma manual. Ara provenen de màquines o dispositius i es gesten de manera automàtica, per la qual cosa el volum que cal analitzar és massiu. Aquesta característica del Big Data es refereix a la mida de les quantitats de dades que es generen actualment.
2) Velocitat: el flux de dades és massiu i constant. Les empreses, per tant, han de reaccionar molt ràpid per poder recopilar-los, emmagatzemar-los i processar-los.
3) Varietat: l'origen de les dades és altament heterogeni. Provenen de múltiples suports, eines i plataformes: càmeres, *smartphones*, cotxes, sistemes GPS, xarxes socials, registres de viatges, moviments bancaris, etc.
4) Veracitat: les empreses han d'assegurar-se que les dades que estan recopilant tinguin validesa, és a dir, que siguin les adequades per als objectius que s'hi pretenen assolir.
5) Valor: el valor que generen les dades, una vegada convertides en informació, es pot considerar l'aspecte més important. Amb aquest valor, les empreses tenen l'oportunitat de treure el màxim profit a les dades per introduir millores en la seva gestió, definir estratègies més òptimes.

L'usuari d'Internet ha passat de tenir una actitud passiva, com a simple receptor d'informació, a adoptar una posició activa, com a generador de contingut. Un bon ús de les dades també pot aportar oportunitats a sectors més tradicionals com el transport, la salut o la indústria manufacturera. La millora de l'anàlisi i el processament de les dades, especialment del *Big Data*, permetrà:

- Transformar les indústries de serveis d'Europa generant una àmplia gamma de productes i serveis d'informació innovadors.
- Augmentar la productivitat de tots els sectors de l'economia mitjançant la millora de la intel·ligència empresarial.
- Abordar de manera més eficient molts dels reptes que afronten les nostres societats.

- Millorar la recerca i accelerar la innovació.
- Aconseguir reduccions de costos mitjançant serveis més personalitzats;
- Augmentar l'eficiència en el sector públic.

Bona part d'aquestes dades ofereixen informació sobre les activitats humanes. Els humans deixem un rastre digital, voluntàriament o involuntària, quan fem activitats. Estem envoltats de dispositius i sensors que permeten el seguiment de la nostra activitat. Així, per exemple, deixem la nostra empremta digital quan utilitzem el nostre telèfon mòbil, paguem amb una targeta de crèdit, utilitzem el transport públic amb la nostra targeta de transport o quan participem a les xarxes socials. Aquestes dades constitueixen una matèria primera molt valuosa per a l'estudi del comportament humà. Permeten analitzar directrius i processos de mobilitat que no es poden estudiar (almenys de la mateixa manera) amb estadístiques oficials o amb enquestes. Així, per exemple, les despeses amb targetes bancàries permeten saber on compres o què compres. De la mateixa manera, les dades de les empreses telefòniques serveixen per dur a terme la posició corresponent al client per a l'ús de serveis telefònics, però també s'utilitzen per dur a terme estudis de mobilitat o *geomarketing*. Com s'ha mencionat anteriorment, l'empremta digital conté informació molt valuosa per les empreses. Amazon recomana llibres relacionats amb els nostres gustos, Spotify fa el mateix amb les cançons i els artistes, i Facebook ens proposa persones que potser coneixem. Ja hi ha nombrosos exemples de com aquesta tecnologia forma part de la nostra vida i sembla tenir el consentiment dels ciutadans.

Les noves tecnologies digitals han tingut una influència profunda en la vida quotidiana, les relacions socials, el govern, el comerç, l'economia i la producció i difusió de coneixement. Els moviments de les persones a l'espai, els seus hàbits de compra i la seva comunicació en línia amb altres persones ara és controlada per les tecnologies digitals. Cada cop ens estem convertint en dades digitals, ens agradi o no, i si triem ser-ho o no. L'era del *Big Data* canvia la nostra relació social de moltes maneres. No només inclou el processament de grans quantitats d'informació, també ens presenta l'oportunitat d'accedir a diferents tipus d'informació que ja teníem anteriorment, i utilitzar noves eines, tecnologies i epistemologies per relacionar-nos amb les dades que hem tingut tot el temps (Mohr, 2015).

D'altra banda, va sorgir ja fa temps el boom de les xarxes socials, a les quals hi ha milions de perfils d'usuaris que sovint pugen informació relativa a ells mateixos. En els darrers anys, hi ha hagut una àmplia discussió i publicitat sobre les possibilitats de recerca social, empresa comercial i govern eficient que ofereixen els conjunts massius de dades digitals. Empreses d'informació digital com Facebook, Microsoft i Google, així com grans empreses com Amazon, Target i Walmart, han liderat el camí per adonar-se de les maneres que poden utilitzar les dades que els usuaris aporten voluntàriament sobre si mateixos i que s'utilitzarà per al desenvolupament de productes i publicitat personalitzada (Lupton, 2014).

Fent ús de tota aquesta informació accessible, és possible rescatar dades útils relatives a les consultes demanades per l'usuari mitjançant un servei *web*. Per aquest cas caldria poder disposar dels perfils públics dels usuaris, ja que altrament es faria impossible la recollida d'informació.

El 2008, la campanya electoral d'Obama als Estats Units (EUA) va ser la primera en utilitzar les xarxes socials com un recurs primordial. Va ser increïblement eficaç. Les xarxes socials es van convertir, en aquesta campanya i per primera vegada, en la plataforma d'organització i trobada de votants que volien portar a Barack Obama a la presidència dels EUA. Els assessors de campanya del candidat van dissenyar estratègies que es focalitzaven a aparèixer pràcticament a totes les xarxes socials disponibles. Els missatges de campanya es van virtualitzar com mai havia succeït a la història fins aquell moment. Aquest mètode va ser repetit el 2012 per la reelecció del candidat. El 2016, la companyia Cambridge Analytica va estar a càrrec de la campanya de Donald Trump als EUA i del Brexit al Regne Unit. En tots dos casos, l'equip de campanya va classificar els usuaris de xarxes socials d'acord amb les seves ideologies polítiques. En tots dos casos, també, van guanyar les eleccions. Mentre els altres equips de campanya han confiat en mètodes tradicionals de màrqueting demogràfic massiu, és a dir, l'enviament de missatges particulars d'acord amb la posició demogràfica del consumidor, Cambridge Analytica va utilitzar un model nou. El seu èxit es va basar en una combinació d'elements: ciència del comportament, anàlisi de grans quantitats d'informació a Internet, i publicitat especialitzada. A finals de la dècada del 2010 es va descobrir que havien adquirit les dades de Facebook de manera il·legal. Quan es va fer públic que realment va ser Facebook qui va vendre les dades a una consultoria privada, la població es va escandalitzar. Va sortir a la llum que s'havien recollit informació de 50 milions d'usuaris de la xarxa social sense permís per generar anuncis polítics dirigits a afavorir la campanya presidencial de Trump i el Brexit.

L'atractiu del *Big Data* ha tingut un impacte important en la política sanitària. Moltes unitats de salut pública, hospitals i altres centres sanitaris han posat en marxa sistemes de gestió de dades per intentar millorar, gestionar i planificar les demandes dels seus serveis. Ara n'hi ha molt de debat sobre el poder dels amplis arxius de dades recollits per les tecnologies digitals tant per informar els pacients sobre els seus propis cossos i proporcionar informació als proveïdors de salut sobre l'estat de salut de les poblacions i l'ús de l'assistència sanitària. Segons IBM, el 90% de la informació generada actualment ha estat creada en els dos darrers anys. A causa d'aquest creixement s'ha popularitzat el terme *Big Data*, que està cridat a convertir-se en una de les tendències tecnològiques amb més futur els propers anys.

Les dades suposen, alhora, un avantatge i un risc per a qualsevol organització. Algunes històries terrorífiques sobre robatori de bases de dades de clients colossals tenen més repercussió mediàtica que molts assassinats, i es converteixen en veritables problemes de relacions públiques per a les empreses que els pateixen, fins al punt de fer trontollar des de la confiança dels seus clients fins al propi valor de mercat de les mateixes. En aquest sentit, són il·lustratius els casos de Yahoo el2013 (3.000 milions de comptes afectats), de Marriot Hotels entre 2014 i 2018 (500 milions de clients afectats), i el de l'Hospital Clínic de Barcelona, aquest passat març, el qual va patir una encriptació dels seus sistemes que feia impossible l'accés a la informació dels pacients.

III. REGULACIONS PER LA PROTECCIÓ DE DADES PERSONALS

3.1. ESPANYA

A Espanya hi ha la Llei Orgànica 3/2018 de Protecció de Dades Personals i garantia dels drets digitals. Va ser publicada al BOE per la *Jefatura del Estado*.

Aquesta llei diu que és un dret fonamental la protecció de dades pel qual es garanteix a la persona el control sobre les seves dades, qualsevol dada personal, i sobre el seu ús i destinació, per evitar-ne el trànsit il·lícit o lesiu per a la dignitat i els drets dels afectats. D'aquesta manera, el dret a la protecció de dades es configura com una facultat del ciutadà per oposar-se a que determinades dades personals siguin utilitzades per a fins diferents d'aquell que en va justificar l'obtenció. Per la seva banda, a la Sentència 292/2000, de 30 de novembre, es considera com un dret autònom i independent que consisteix en un poder de disposició i de control sobre les dades personals que faculta la persona per decidir quines d'aquestes dades proporcionar a un tercer, sigui l'Estat o un particular, o quines pot demanar aquest tercer, i que també permet a l'individu saber qui posseeix aquestes dades personals i per a què, podent oposar-se a aquesta possessió o ús. A nivell legislatiu, la concreció i el desenvolupament del dret fonamental de protecció de les persones físiques en relació amb el tractament de dades personals va tenir lloc amb l'aprovació de la Llei Orgànica 5/1992, reguladora del tractament automatitzat de dades personals, coneguda com a LORTAT. Aquesta llei va ser reemplaçada per la Llei Orgànica 15/1999, de 5 de desembre, de protecció de dades personals, a fi de traslladar al nostre dret a la Directiva 95/46/CE del Parlament Europeu i del Consell, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i la lliure circulació d'aquestes dades.

La mateixa norma que vetlla per la privadesa dels ciutadans a l'entorn en línia permet als partits polítics recopilar sense autorització dades personals obtingudes en pàgines web i altres fonts d'accés públic per enviar-los propaganda electoral personalitzada a través del correu electrònic o les xarxes socials. Aquestes activitats, segons la llei, estaran emparades a l'interès públic quan s'ofereixin garanties adequades, però en cap cas la norma detalla en quines circumstàncies rastrejar les dades dels usuaris és d'interès públic ni quines són les garanties sota les quals els partits poden ensumar a la vida electrònica de la gent.

3.2. UNIÓN EUROPEA

La protecció de les persones físiques en relació amb el tractament de dades personals és un dret fonamental. L'article 8, apartat 1, de la Carta dels Drets Fonamentals de la Unió Europea («la Carta») i l'article 16, apartat 1, del Tractat de Funcionament de la Unió Europea (TFUE) estableixen que tota persona té dret a la protecció de les dades de caràcter personal que li concerneixin. Els principis i normes relatius a la protecció de les persones físiques pel que fa al tractament dels seus dades de caràcter personal han de, sigui quina sigui la seva nacionalitat o residència, respectar les seves llibertats i drets fonamentals, en particular el dret a la protecció de les dades de caràcter personal.

La Directiva 95/46/CE del Parlament Europeu i del Consell tracta d'harmonitzar la protecció dels drets i les llibertats fonamentals de les persones físiques en relació amb les activitats de tractament de dades de caràcter personal i garantir la lliure circulació d'aquestes dades entre els Estats membres.

El tractament de dades personals ha d'estar concebut per servir la humanitat. El dret a la protecció de les dades personals no és un dret absolut sinó que s'ha de considerar en relació amb la seva funció a la societat i mantenir l'equilibri amb altres drets fonamentals, d'acord amb el principi de proporcionalitat. Aquest Reglament respecta tots els drets fonamentals i observa les llibertats i els principis reconeguts a la Carta conforme es consagren als Tractats, en particular el respecte de la vida privada i familiar, del domicili i de les comunicacions, la protecció de les dades de caràcter personal, la llibertat de pensament, de consciència i de religió, la llibertat d'expressió i d'informació, la llibertat d'empresa, el dret a la tutela judicial efectiva i a un judici just; i la diversitat cultural, religiosa i lingüística.

La ràpida evolució tecnològica i la globalització han plantejat nous reptes per a la protecció de les dades personals. La magnitud de la recollida i de l'intercanvi de dades personals ha augmentat de manera significativa. La tecnologia permet que tant les empreses privades com les autoritats públiques utilitzin dades personals en una escala sense precedents a l'hora de fer les seves activitats. Les persones físiques difonen un volum cada vegada més gran d'informació personal a escala mundial. La tecnologia ha transformat tant la economia com la vida social, i ha de facilitar encara més la lliure circulació de dades personals dins de la Unió i la transferència a tercers països i organitzacions internacionals, garantint alhora un elevat nivell de protecció de les dades personals.

D'altra banda, també es recull a l'article 8 de la Carta dels Drets Fonamentals de la Unió Europea i a l'article 16.1 del Tractat de Funcionament de la Unió Europea.

Anteriorment, a nivell europeu, s'havia adoptat la Directiva 95/46/CE citada, l'objecte de la qual era procurar que la garantia del dret a la protecció de dades personals no suposés un obstacle a la lliure circulació de les dades al si de la Unió, establint així un espai comú de garantia del dret que, alhora, assegurés que en cas de transferència internacional de les dades, el seu tractament al país de destinació estigués protegit per salvaguardes adequades a les previstes a la pròpia directiva.

3.3. ESTATS UNITS

A diferència d'Europa, els Estats Units no tenen un únic marc o directiva de privadesa de dades. Més aviat, la llei de protecció de dades dels Estats Units està formada per un mosaic de lleis i regulacions federals i estatals, que regeixen el tractament de les dades en diverses indústries i operacions empresarials. Per complir amb les lleis de privadesa de dades dels Estats Units, les organitzacions sense ànim de lucre que operen als Estats Units han de respectar i complir les lleis federals i estatals. En general, els estatuts federals regulen la recollida, l'emmagatzematge i l'ús d'informació personal no pública sensible. La legislació estatal, en canvi, generalment regula els requisits de divulgació després d'una violació de la seguretat de no públic es produeix informació personal.

Les lleis federals de protecció de dades als EUA es deuen principalment a la indústria i al tipus de dades. Amb un augment de l'atenció a la privadesa de dades i la protecció del consumidor en els darrers anys, és probable que les lleis de protecció de dades siguin aplicades de manera més estricta pels reguladors en un futur proper.

1) *Federal Trade Comission Act (FTCA):* va ser promulgada per prohibir els actes o pràctiques deslleials o enganyoses en el comerç. Una pràctica comercial és enganyosa si implica una representació, omissió o pràctica material que pot induir a error un consumidor que actua raonablement en les circumstàncies, en detriment del consumidor.

2) *Health Insurance Portability and Accountability Act (HIPAA):* Segons HIPAA, les entitats cobertes han de complir les normes de privadesa i seguretat. Segons la norma de privadesa, les entitats cobertes no poden utilitzar ni revelar la informació de salut protegida, excepte en circumstàncies específiques o quan ho autoritzi el pacient o el participant. D'acord amb la regla de seguretat, les entitats cobertes han de garantir la confidencialitat, la integritat i la disponibilitat de la informació de salut protegida electrònica que mantenen o transmeten, fent complir les garanties administratives, físiques i tècniques raonables i adequades. Una entitat coberta es defineix com un pla de salut, centre de compensació d'assistència sanitària o proveïdor d'atenció mèdica

que transmet qualsevol informació de salut en forma electrònica en relació amb una transacció coberta per la llei.

3) *Family Educational Rights and Privacy Act (FERPA):* protegeix les dades dels estudiants i s'aplica a totes les agències i institucions educatives que reben el finançament del Departament d'Educació dels EUA, incloses les organitzacions sense ànim de lucre.

4) *Non-Solicited Pornography and Marketing Act of 2023 (CAN_SPAM Act):* la Llei de màrqueting i pornografia no sol·licitada de 2003 regula els missatges de correu electrònic comercials. Els missatges de correu electrònic comercials es defineixen com qualsevol missatge de correu electrònic, la finalitat principal del qual és la publicitat comercial o la promoció d'un producte o servei comercial.

5) *Gramm-Leach-Bliley Act (GLBA):* exigeix que les institucions financeres respectin la privacitat dels seus clients i protegeixi la seguretat i privacitat d'aquests.

6) *Fair Credit Reporting Act (FCRA*): va ser creada per promoure la presentació d'informes de crèdit justos i precisos, i estableix procediments per a la recollida, l'ús i la protecció de la informació personal en poder de les agències d'informació del consumidor.

7) *Children's Online Privacy Protection Act (COPPA):* es va promulgar per protegir els nens menors de tretze anys en el seu ús d'Internet mitjançant la regulació de com els llocs *web* recullen, utilitzen, i revelen la informació personal dels nens. Segons la COPPA, abans que un "operador" de llocs *web* pugui recopilar informació personal d'un nen, ha de notificar als pares del nen les seves pràctiques de recollida de dades i ha d'obtenir el consentiment dels pares per recollir la informació. COPPA s'aplica als operadors de llocs web dirigits a nens i als llocs web de "públic general" si l'operador té coneixement real que el lloc web està recopilant informació personal dels nens.

Gairebé tots els estats han promulgat algun tipus de llei de privadesa de dades aplicable a la seva jurisdicció. És important tenir en compte que, tot i que s'apliquen les lleis estatals de privadesa de dades, els fiscals generals de l'estat respectius també poden demandar per violació de la llei federal. Per tant, les organitzacions sense ànim de lucre no haurien de veure els estatuts federals i estatals com a dues esferes jurisdiccionals separades, sinó com a conjunts de lleis que s'aplicarien conjuntament. En general, la llei de privadesa de dades a la majoria dels estats es centra en la notificació d'incompliments, amb les entitats obligades a notificar als consumidors la informació personal dels quals està compromesa. Les excepcions notables són Califòrnia i Massachusetts, que tenen lleis i regulacions més proactives i de més

abast. És important tenir en compte que Califòrnia i Massachusetts van promulgar lleis que s'apliquen a qualsevol entitat, a qualsevol lloc dels Estats Units, amb accés a informació no pública d'un dels seus residents.

IV. RESULTATS

Al principi del treball s'ha dit que es faria un anàlisi d'enquestes per contrastar i recolzar la teoria. A continuació es mostraran els resultats d'aquestes enquestes.

4.1. ENQUESTA D'ELABORACIÓ PRÒPIA

En l'enquesta d'elaboració pròpia per conèixer l'opinió dels usuaris d'Internet s'ha recollit una mostra de 95 persones, de grups d'edat diferent. Dels 95 participants, 1 era menor de 18 anys, 60 eren de entre 18 i 34 anys, 5 de entre 35 i 54, i 29 de més de 55 anys.

73 usuaris s'han sentit vigilats a través dels seus dispositius electrònics. Se'ls hi ha preguntat si els hi preocupa que les seves dades siguin utilitzades per altres persones o empreses. La gran majoria, de totes les franges d'edat, ha contestat que si els hi preocupa, amb 76 persones que sí els hi preocupa, 10 que no i 9 enquestats mai s'ho havien replantejat. (Taula 1).

Taula 1

		¿Te preocupa o alguna vez te ha preocupado que tus datos sean utilizados por otras personas o empresas?			Total
		Nunca lo había pensado	No, no me preocupa.	Si, me preocupa.	
¿Cuántos años tienes?	De 18 a 34	9	6	45	60
	De 35 a 54	0	2	3	5
	Más de 55	0	2	27	29
	Menos de 18	0	0	1	1
Total		9	10	76	95

Taula: Elaboració pròpia a partir de la nostra enquesta.

Quan se'ls hi va preguntar si els hi preocupava que les seves dades siguin accessibles i públiques, el número de persones que no els hi preocupa creix. Amb un total de 20 persones que no els hi preocupa, 70 que sí els hi preocupa i 5 que no s'ho havien replantejat mai (Taula 2). Destaca bastant aquest canvi de resultats en aquestes dues preguntes molt semblants, l'únic que canvia és que en la primera les teves dades són utilitzades i en la segona només són observades.

Taula 2

		¿Te preocupa o alguna vez te ha preocupado que tus datos y tus búsquedas sean accesibles para otras personas/empresas?			Total
		No, no me preocupa.	Nunca lo había pensado.	Si, me preocupa.	
¿Cuántos años tienes?	De 18 a 34	15	5	40	60
	De 35 a 54	2	0	3	5
	Más de 55	3	0	26	29
	Menos de 18	0	0	1	1
Total		20	5	70	95

Font: Elaboració pròpia a partir de la nostra enquesta.

La pregunta de si creuen que l'empremta digital és beneficiosa o perjudicial és una pregunta oberta. Hi han hagut respostes molt variades. Molt poca gent s'ha posicionat a una banda o a l'altre. La gran majoria ha optat per les dues opcions i els arguments que han donat han estat variats. Com a arguments en contra de l'empremta digital s'ha repetit molt la preocupació de la privadesa. Consideren que el fet que persones i empreses puguin veure la teva informació és una violació a la teva privacitat. Un argument en contra de l'empremta digital que s'ha repetit també, és el control que poden exercir les empreses sobre tu. És a dir, que les empreses poden conèixer les teves preferències i oferir-te productes que ells volen que compris. O el fet de que la gent que accedeix a les teves dades pot saber tot el que fas. Un tema que es repeteix és la preocupació per el futur. Les publicacions que penges, els missatges que envies i les pàgines que consultes queden registrades i no es poden esborrar. "*El que penges és permanent i por arruïnar la imatge d'una persona per quelcom que va publicar fa deu anys".* Aquesta és unaresposta d'un usuari a qui li preocupa que el que publiqui en el present, pugui afectar-li en un futur. *"Perjudicial perquè no s'esborra res i en el futur et pot perjudicar a nivell laboral o personal".* Un altre argument contra l'ús de l'empremta digital és que si recopilen dades teves de tot el que fas i de tot el que t'agrada, les empreses poden conèixer-te millor que tu a tu mateix.

Es menciona el bombardeig constant de noticies i d'informació que t'envien i l'intercanvi de les teves dades com un negoci. Un altre enquestat menciona el consum innecessari, argumentant que les empreses utilitzen les nostres dades per llençar millors campanyes de màrqueting per fomentar les compres.

Com a arguments a favor, també hi ha hagut de molt diferents. Molts afirmen que és beneficiosa per les empreses perquè poden conèixer millor al seu públic, i també per casos de desaparicions, accidents, etc. (a l'any 2009 la policia de Massachusetts va rescatar a unanena segrestada gràcies al GPS i Google Maps del mòbil; amb l'ajuda de la companyia del telèfon van trobar a la nena a un motel amb la segrestadora). Altres creuen que és molt beneficiosa si les dades es treballen d'una manera correcte (un usuari menciona les *"cookies"* i diu que gràcies a elles pot veure anuncis del seu interès i li faciliten les cerques a Internet). Un usuari menciona la cerca de persones a Internet i posa l'exemple d'una primera cita (la persona enquestada explica que si has de quedar amb algú per primer cop, pots cercar a aquesta persona a les xarxes socials i saber una mica més sobre ella). Un altre usuari destaca el fàcil accés als seus comptes, ja que les pàgines webs guarden les seves contrasenyes. S'han trobat dues respostes que afirmaven que l'empremta digital és beneficiosa, però *"veient el món en el que vivim i els valors de les persones segur que és més perjudicial".* Un enquestat pensa que l'empremta digital pot ajudar a resoldre casos criminals (al gener del 2019 uns fiscals d'Alemanya van presentar a un tribunal dades del iPhone de la víctima, que contradeien la versió del sospitós, que al·legava que la víctima pujava per les escales, quant en realitat estava sent arrossegat, ja que el iPhone no va detectar les seves passes).

4.2. FECYT

El FECYT és la Fundació Espanyola per la Ciència i la Tecnologia. És una fundació pública dependent del Ministeri de Ciència i innovació d'Espanya. D'aquesta fundació s'han utilitzat les enquestes de percepció social de la ciència i la tecnologia a Espanya de l'any 2022.

Les persones que s'informen sobre ciència i tecnologia a través d'Internet ho fan principalment a través de: vídeos (62,3%), xarxes socials (75,4%) i mitjans digitals generalistes (58,9%). Les xarxes socials i els vídeos són més utilitzats a mesura que baixa l'edat, sent els principals canals d'informació sobre ciència i tecnologia a Internet per a les persones de 15 a 34 anys.

S'ha consultat una enquesta on es demana l'opinió dels enquestats sobre si les noves tecnologies són beneficioses o no, i els resultats mostren que en relació a la intel·ligència artificial, l'experimentació animal amb finalitats mèdiques, la robotització del treball i el cultiu de plantes modificades genèticament el balanç és proper a zero, és a dir, que l'atribució

de riscos i beneficis és similar. Més o menys el mateix resultat obtingut a la nostra enquesta.

En relació amb l'ús de dades personals amb intel·ligència artificial, una mica més de dues terceres parts de la ciutadania (70,4%) es mostra d'acord que el risc de ser manipulats amb les nostres pròpies dades per empreses o governs és alt o molt alt, produint-se un lleuger increment respecte del 2020 (67,7%). Una mica més d'un terç (38,1%) creu que la intel·ligència artificial incidirà en la millora de la qualitat dels serveis públics i empreses.

4.3. EUROBARÒMETRE

A la European Comissions s'ha trobat un Eurobaròmetre sobre les actituds vers a l'impacte de la digitalització i automatització de la vida quotidiana. Es mostra que els enquestats estan molt més disposats a compartir les seves dades de salut i benestar amb els metges i professionals sanitaris (65%) que amb administracions públiques o empreses del sector públic (21%), o amb empreses del sector privat (14%), encara que siguin anònims i per a finalitats de recerca (Special Eurobarometer, pg. 99).

També ens mostra que la majoria d'usuaris d'Internet han pres mesures de seguretat i privacitat quan naveguen per la xarxa. Entre els usuaris d'Internet, les accions més habituals en els últims tres anys en resposta als problemesde privadesa i seguretat han estat instal·lar o canviat el seu programari antivirus (45%), mostrar-se menys propensos a donar informació personal als llocs web (39%), utilitzar només el seu ordinador (36%), o obrir correus electrònics només de persones i adreces que coneguin (35%).

La majoria diu que les funcions de seguretat i privadesa d'un producte informàtic tenen un paper important en la seva elecció. El 27% diu que tenen un paper important en la seva elecció i que estan disposats a pagar més per millorar característiques de seguretat i privadesa, mentre que el 34% afirma que no està disposat a pagar més, encara que aquests aspectes tenen algun paper en la seva elecció (Special Eurobarometer, pg. 109).

En l'àmbit cibernètic, la majoria dels usuaris d'Internet han pres accions com a resposta a les preocupacions privadesa i seguretat en línia, com, per exemple, instal·lar o canviar programari antivirus, ser més prudent amb la informació personal que donen als llocs web i amb els correus electrònics que obren, i utilitzar només els seus propis ordinadors. Tot i que les funcions de seguretat i privadesa juguen un paper important, la majoria de l'elecció de productes informàtics dels enquestats, no tothom està disposat a pagar més per millorar característiques de privadesa i seguretat.

4.4. VODAFONE INSTITUTE FOR SOCIETY AND COMUNICATIONS

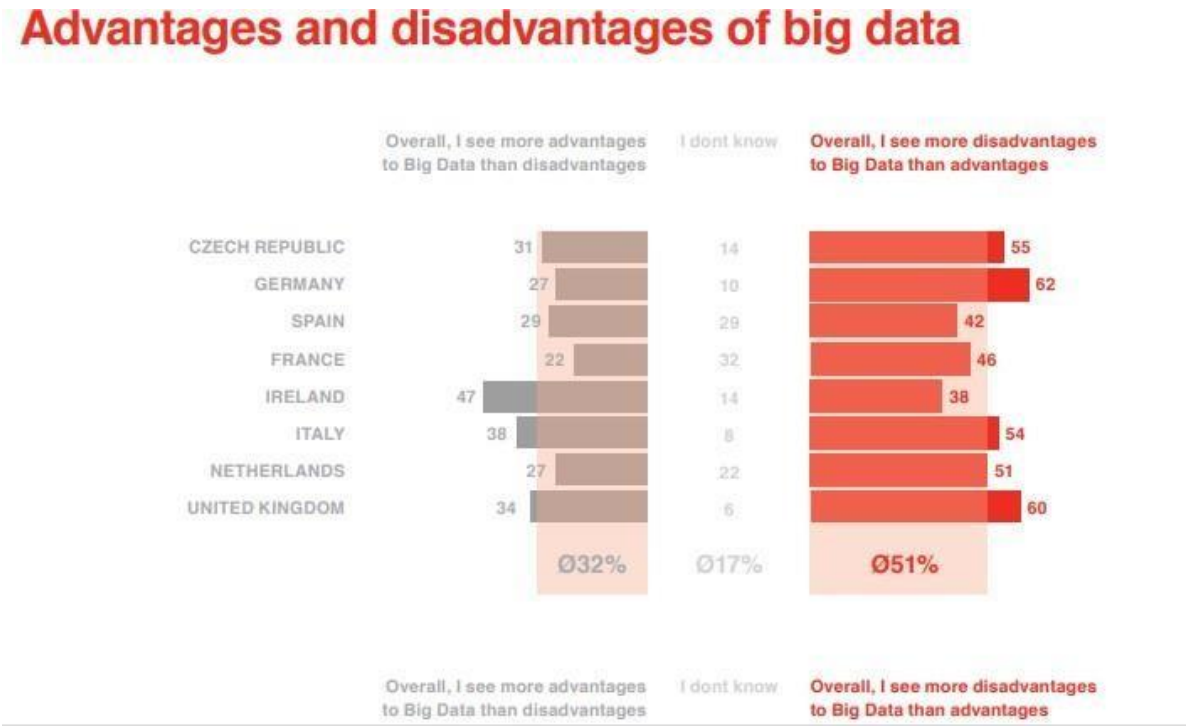
Per últim s'ha trobat una enquesta a nivell europeu realitzada per la companyia Vodafone per il·lustrar com els europeus perceben el maneig de les seves dades personals i valoren qüestionsde privadesa. El Vodafone Institute for Society and Communications va iniciar una enquesta anomenada "Big Data - Oportunitats i Riscos" a vuit països europeus. L'enquesta aborda situacions quotidianes en què els consumidors, conscient o inconscientment, revelen que les seves dades personals són recollides per empreses privades o institucions públiques per habilitar productes personalitzats, serveis i experiències. L'enquesta mostra que només el 12% de les persones llegeix les polítiques de termes i condicions sobre la recopilació i ús de les dades. Això mostra que molt poca gent sap el que passa amb les seves dades.

Se'ls hi pregunta sobre el grau de confiança respecte a l'ús de les seves dades. Un gran percentatge (43%) confia molt en les institucions sanitàries; per contra, la confiança es redueix considerablement quan es tracta de companyes de xarxes socials.
L'enquesta mostra que la majoria de la gent no se sent ben informada sobre les pràctiques actuals de recollida de dades. Es va preguntar als enquestats què en saben sobre la recollida i l'ús de dades per part de diferents organitzacions. L'enquesta ens mostra que una manera de que la població guanyi confiança respecte a la recollida de dades és utilitzar un llenguatge clar i concís, amb termes simples.

La meitat de les persones enquestades (55%) dels vuit països on es va realitzar l'enquesta van estar d'acord amb l'afirmació de que el govern hauria de tenir accés a dades personals per tal de mantenir la seguretat al seu propi país. D'altra banda, una quarta part (25%) està en contra d'aquest afirmació, mentre que el 19% s'abstenen i no estan d'acord ni discrepen. Hi ha moltes maneres possibles de protegir les nostres dades.

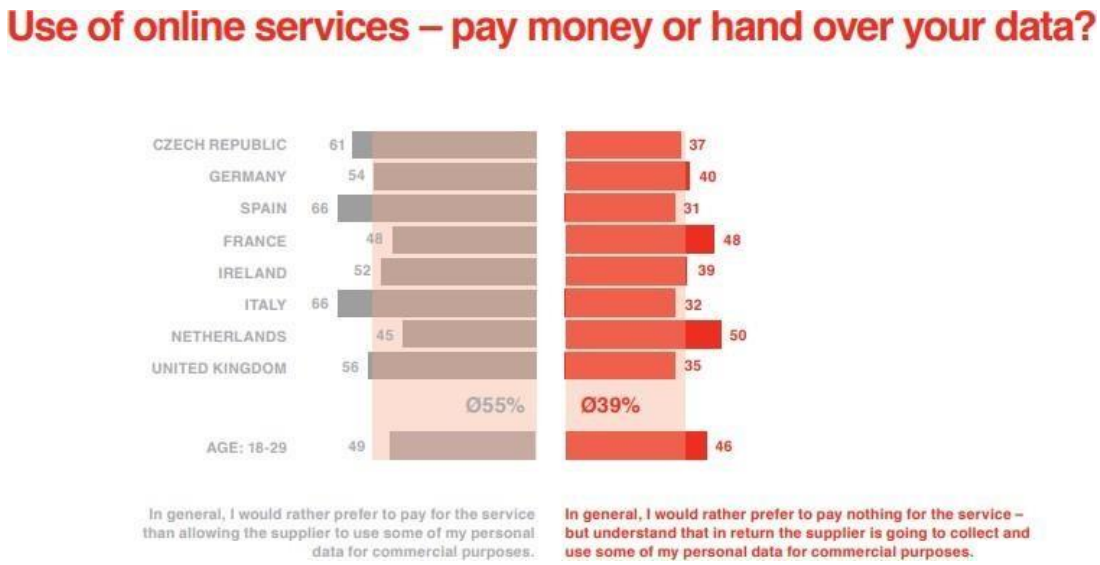
Font: captura de pantalla de l'enquesta de Vodafone Institute for Society and Communications

La mesura més esmentada pels europeus enquestats (44%) és eliminar o bloquejar les *"cookies"*. Una altre mesura de seguretat que prenen (41%) és aturar una descàrrega quan se'ls demana que introdueixin les seves dades personals. En qualsevol cas, gairebé un terç (31%) dels enquestats de tots aquests països no donen el seu nom real ni altres dades personals. També es veu que un 51% de la població creu que el *Big Data* porta desavantatges, mentre que el 32% opina que aporta avantatges.



Font: captura de pantalla de l'enquesta de Vodafone Institute for Society and Communications

Més de la meitat de tots els europeus enquestats (55%) diuen preferir pagar al proveïdor de serveis per utilitzar un servei a permetre que les seves dades siguin recopilades i utilitzades per aquest. En canvi, les persones més joves solen no tenir una aversió tan forta al fet de que les seves pròpies dades siguin utilitzades pel proveïdor de serveis. Tanmateix, en el grup d'edat de 18 a 29 anys, un nombre aproximadament igual prefereix pagar a lliurar les seves dades.



Font: captura de pantalla de l'enquesta de Vodafone Institute for Society and Communications

Una dada curiosa que s'ha vist a l'enquesta de Vodafone és que una manera de guanyar confiança vers els governs és a través de l'apoderament dels usuaris. És a dir, més de la meitat dels enquestats (51%) associen la confiança en les institucions amb el potencial d'influir personalment en la seva configuració de privadesa personal, la qual cosa podria ser una solució a la sensació d'invasió de privadesa que molts usuaris pateixen.

En aquests sentit, un exemple seria la nova proposta de Telefónica: la quarta plataforma. És tracta d'un projecte en desenvolupament que persegueix donar als usuaris el control de les dades generades pel consum que fan dels seus productes i serveis, així com de les generades quan naveguen per les seves xarxes. D'aquesta manera, Telefónica pretén generar confiança entre els seus clients a l`hora d'utilitzar Internet. Així, Telefónica posarà les capacitats de les seves plataformes al servei dels seus usuaris perquè les dades d'aquests no arribin a mans de tercers sense el seu consentiment exprés i informació clara. El president de Telefónica, a la seva intervenció a Santander, va deixar clar que es tracta d'un projecte en marxa que busca la solució més senzilla i transparent perquè l'usuari sigui el veritable sobirà de les dades.

V. DISCUSSIÓ

5.1. CONTROL O SEGURETAT?

Hi ha moltes implicacions ètiques i polítiques importants en relació amb l'ús de l'empremta digital. Els termes "bones dades" i "males dades" ara s'utilitzen de vegades per descriure les implicacions de l'ús de grans dades per part de les corporacions i les agències governamentals. Per exemple,les "bones dades" ofereixen beneficis per a les empreses comercials i les agències governamentals, contribueixen a investigacions importants (com ara la de temes mèdics) i ajuden a les mesures de seguretat sense perjudicar els consumidors i els ciutadans ni infringir la seva privadesa o llibertats civils (Lupton, 2015).

Ara bé, què passaria si la novel·la "1984" de George Orwell es fes realitat? *The Guardian* va revelar que Raytheon (un contractista de defensa nord-americà) va desenvolupar el programa *Rapid Information Overlay Technology* (RIOT), que utilitza dades de lliure accés de xarxes socials i dades associades a una adreça IP, etc, per perfilar una persona i fer les seves accions quotidianes completament transparents.

Empreses com Netflix o Amazon aprofiten el seu emmagatzematge del *Big Data* per predir el comportament dels consumidors i actuar en conseqüència. La majoria dels governs i bancs centrals mai no ho havien fet, però ara sembla que sí. S'estan donant compte a poc a poc que amb l'ús del *Big Data* poden reaccionar molt més ràpid davant de les crisis econòmiques identificant els comportaments de productors i consumidors. Durant molts anys hi ha hagut un debat constant sobre si l'activitat a Internet hauria de ser supervisada legalment pels proveïdors de serveis d'Internet o pel govern. Hi ha molts pros i contres a ambdues parts d'aquest problema. No només hi ha una necessitat vàlida de monitorització d'Internet de les xarxes privades a més dels sistemes governamentals, sinó que també hi ha una preocupació vàlida per la privadesa dels ciutadans del nostre país.

Aquesta informació recollida a partir de dades estadístiques i cada cop més del *Big Data* es pot utilitzar de manera específica per aconseguir que la gent consumeixi o es comporti d'una determinada manera, mitjançant màrqueting específic. A més, si es coneixen diferents aspectes sobre les preferències i condicions d'un grup concret, aquests es poden utilitzar per emprar incentius per fomentar o desanimar un determinat comportament (Zwitter, 2014). Es donarà un exemple molt simple per entendre-ho millor. S'ha descobert a partir de recopilar informació que a un grup de persones els hi agrada la xocolata. I resulta que una gran part d'aquest mateix grup es troba en una situació de que no saben quin partit polític votar entre el partit A o el B. El que pot fer el partit B és oferir xocolata si el voten. D'aquesta manera el *Big Data* augmenta la capacitat de descobrir correlacions ocultes, la qual cosa augmenta la capacitat de crear incentius, els propòsits dels quals són menys transparents.

D'una banda, Facebook és el sospitós habitual a esmentar quan es tracta de qüestions de privadesa. Al mateix temps, aquesta discussió amaga el fet que molta informació no personal també pot revelar molt sobre grups molt específics en relacions geogràfiques molt específiques. En altres paraules, la informació individual pot ser interessant per a finalitats d'investigació de les agències d'intel·ligència, però la informació realment valuosa per a les empreses no requereix l'etiqueta individual. Per exemple, la "policia predictiva" ja és un fet a grans ciutats, on l'anàlisi del *Big Data* apunten a determinats carrers, bandes o grups d'individus, que tenen més probabilitats de cometre un delicte, per tal de sotmetre'ls a una major vigilància. Què passa si l'anàlisi del *Big Data* prediu que una determinada persona (per exemple, una mare que viu en un barri determinat, sense feina, sense relació estable, etc.) té una probabilitat del 95% de patir violència domèstica? Cap organització de benestar social que tingui aquesta informació podria actuar políticament sobre aquesta informació. L'enviament de treballadors socials a casa de la persona pot ser tan invasiu com empresonar persones abans de l'acte, i viola la presumpció d'innocència. Tanmateix, això pot provocar un estigma a la persona, la família i els amics. Fins i tot si les dades recollides mitjançant la vigilància governamental creen una sospita raonable de conducta per a la persona objectiu, pot ser que no hi hagi cap garantia que l'individu sigui culpable.

Quan augmentem la quantitat de cobertura disponible a la societat, comencem a restringir els drets d'aquells que no mereixen intervencions de seguretat. La vigilància és perjudicial perquè pot frenar l'exercici de les nostres llibertats civils. Amb respecte a les llibertats civils, es considera la vigilància de les persones quan pensen, llegeixen i es comuniquen amb els altres per tal de crear la seva opinió sobre qüestions polítiques i socials. Aquesta vigilància intel·lectual és especialment perillosa perquè pot provocar que la gent no experimenti amb idees noves, controvertides o desviades. A més, això planteja preguntes sobre el paper ètic dels qui estableixen el llindar d'intervenció i dels científics de dades que escriuen l'algoritme que calcula l'atzar en funció de determinades variables disponibles al conjunt del *Big Data.*

"Si no has fet res malament, no tens res a témer"

Aquest és un argument típic utilitzat pels governs i altres grups per justificar les seves activitats d'espionatge. Sembla que té sentit, ja que la majoria de les persones són ciutadans respectuosos, la majoria no seran objecte de vigilància i no afectarà les seves vides, sinó que les farà més còmodes i segures mitjançant l'eliminació dels delinqüents. Per tant, l'ús per part del govern de càmeres de circuit tancat a l'espai públic, les escoltes telefòniques sense mandat i les comprovacions dels registres de la biblioteca tenen el potencial de salvar vides de delinqüents i terroristes amb una invasió mínima de la privadesa dels seus ciutadans.

En primer lloc, s'ha de pensar que aquests arguments es podrien aplicar fàcilment demanant a tots els ciutadans que portin dispositius de seguiment lligats al peu; faria molt més fàcil el rastreig d'actes delictius, i es podria argumentar que les persones que es neguen a portar aquests dispositius només ho fan perquè tenen alguna cosa a amagar. Considero evident que

la majoria de la gent de la nostra societat s'oposaria a aquesta solució, no perquè vulguin cometre cap delicte, sinó perquè és invasiva. S'ha de tenir en compte que, donada la tecnologia actual, el govern ja té la capacitat de fer un seguiment dels moviments d'un objectiu conegut fins a un grau raonable i té fàcil accés a informació com ara els hàbits de compra, les activitats en línia, les converses telefòniques i el correu. Tot i que la implementació de dispositius de seguiment d'ubicació obligatoris per a tota la població és sens dubte més invasiva que l'anterior, diria que les pràctiques actuals són igual d'invasives.

A continuació, aquest argument no té en compte una sèrie de qüestions importants a l'hora de recopilar dades o enregistraments d'identificació personal; en primer lloc, que aquestes pràctiques creen un arxiu d'informació que és vulnerable a l'abús per part de persones privilegiades de confiança. A més, permetre la vigilància anima el govern a ampliar aquests programes de vigilància en el futur. El European Data Protection Supervisor ha reconegut que fins i tot quan es creen dues bases de dades d'informació amb finalitats específiques i diferents, es podrien combinar entre si per formar un tercer amb un propòsit per al qual els dos primers no es van construir. Aquesta no singularitat i immutabilitat de la informació ofereix un gran potencial d'abús per part de persones i institucions.

Al inici del treball, a l'apartat Metodologia, s'ha mencionat que es faria una aproximació a l'opinió pública fent cerques a les xarxes socials. La gran majoria de publicacions i fòrums que parlen de l'empremta digital o del *Big Data* no són favorables als seus usos, ja que comporten un perill inherent de vigilància i control, i fins i tot d'espionatge.

A Twitter s'ha fet una cerca amb el *#bigdata*, on s'han trobat comentaris i publicacions amb opinions bastant iguals. "*Big Data, Big Shit"* és el missatge que un usuari va publicar, donant la seva opinió. Una noia va publicar un missatge relacionat amb la vigilància i el control: *"Alguien más habla lejos de su movil para que no les escuchen?"* o "*No solo por los teléfonos nos espían. Cuidado con lo que digan o hagan"* donant a entendre que hi ha una "cosa" que ens escolta a totes hores. També s'han trobat publicacions en les que es mostren bastant enfadats, com l'usuari PATGON78 qui afirma que *"Cada día estoy más convencido de que nos espían por todos lados. Ayer estuve en un local donde se juega a dardos y, qué casualidad, hoy me salen anuncios de accesorios para dardos de todo tipo !!!!"*.

Les poques publicacions que s'han trobat a favor de l'ús de l'empremta digital han sigut de comptes d'hotels, que trobaven favorable l'ús per augmentar el turisme. Un exemple és el cas de Airbnb quan, després d'una caiguda del 70% de les reserves a causa de la pandèmia, l'empresa va canviar l'enfocament a l'hora d'oferir recomanacions. La companyia es va centrar en la idea de que viatjar en aquests temps es tracta més de viure còmodament i de manera segura, que de fer turisme. Per això, van ajustar l'algoritme i van començar a recomanar allotjaments allunyats de les grans ciutats.

Reddit és una col·lecció massiva de fòrums on la gent pot compartir notícies i contingut, a més de comentar les publicacions d'altres persones. En aquest cas s'ha cercat el concepte *Big Data* a la seva pàgina web. S`han trobat diversos comentaris, però s'ha volgut aprofundir i s'ha cercat el terme "espionatge", i s'han obtingut molts més resultats.

"The FBI is the same as they always were, above the law and having no respect for the citizens constitutional rights. They have done this since their inception.". Aquest és un comentari extret de Reddit on un usuari expressava la seva frustració cap al FBI per no respectar els seus drets. És un comentari fet a una comunitat on s'estava parlant de la violació de privadesa i de l'espionatge que fa el govern nord-americà als seus ciutadans. *"F*ck government. I won't give them honest information"*. En aquest cas, aquest és un comentari fet a una publicació que es queixava de que el govern els estava espiant un altre cop. L'usuari que ha comentat això bàsicament diu que no pensa donar informació honesta, justament perquè el govern no el tingui controlat. Igual que a Twitter, aquí també han aparegut comentaris dient que les mòbils els espien i molts comentaris compartint les seves experiències de com els espien. Per exemple, una noia explica que va trencar amb la seva parella, i dos hores després li va sortit un anunci d'una aplicació de cites.

Discord és una plataforma on pots crear comunitats i parlar en línia amb gent de tot el món. Per aquesta aplicació es va crear un compte i es va parlar en temps real amb usuaris. Se'ls hi va preguntar l'opinió sobre l'empremta digital i els seus usos, si estaven d'acord o no. La gran majoria estava en contra i uns pocs consideraven que era una bona eina per "*tenir-nos a tots controlats".* En totes les tres aplicacions, els usuaris tenen opinions semblants i la majoria no són opinions positives. Això recolza l'argument de que encara que no hagi d'amagar res, la població no se sent còmoda sabent que és vigilada a través dels seus dispositius electrònics.

5.2. A QUI PERTANYEN LES TEVES DADES?

A l'any 2010 Eric Schmidt, aleshores conseller delegat de Google, va declarar que un dia, en el curs d'una conversa, es van adonar que es podrien utilitzar les dades que té Google dels seus usuaris per predir l'evolució del mercat borsari. Però van decidir que això era il·legal. Així que van deixar de fer-ho.

Moltes vegades, quan accedim a qualsevol servei, com ara una xarxa social, ens sentim bé perquè l'accés és gratuït. Podem compartir amb amics o família les nostres fotos, els llocs que visitem o, quan marxem de vacances, els fem reviure amb nosaltres aquests moments especials i les anècdotes divertides que ens succeeixen. En altres casos, també podem expressar les nostres opinions o comentar situacions que ens importen i compartir-les lliurement. Tot i això, no som conscients que estem cedint, gratuïtament, les nostres dades personals. I n'hi ha una màxima que gairebé sempre es compleix: " si un servei és gratuït, el producte ets tu". Aquí tenim la primera i fonamental raó per la qual no hem de pagar: Facebook viu de la publicitat que contracten les empreses. Facebook els facilita estadístiques

basades en totes les dades que recopilen, perquè les campanyes publicitàries es dirigeixin amb la màxima precisió possible a tots els potencials clients que podrien estar interessats en els seus productes. Si baixem l'arxiu de les dades que Facebook emmagatzema sobre nosaltres, ens sorprendrà la quantitat d'informació que tenen sobre nosaltres: l'agenda del nostre telèfon, la cronologia de la nostra vida, les localitzacions, etc.

Aquestes dades brinden a les empreses un enorme poder per conèixer el món. Considerem els exemples següents: Mark Zuckerberg, conseller delegat de Facebook, ha utilitzat dades personals per predir quins usuaris de Facebook iniciaran relacions sentimentals; analistes de mercat han fet servir dades de Twitter per calcular els ingressos de taquilla de les pel·lícules; i Google ha utilitzat criteris de cerca per detectar brots de grip a tot el món (Nielsen, 2013). Avui dia donem per fet que només un grapat de grans companyies amb ànim de lucre i agències secretes d'intel·ligència, com ara la NSA, tenen accés a una infraestructura de dades potent. Però hi ha possibilitats de crear una infraestructura pública de dades igual de poderosa, una infraestructura que la pot utilitzar qualsevol des de qualsevol part del món. Es tracta de portar el *Big Data* a les masses.

5.3. QUI GUANYA I QUÈ GUANYEN?

S'han mencionat els beneficis i els perjudicis de l'ús de l'empremta digital. A les enquestes s'han vist les preocupacions de la població i les diferents opinions sobre el tema. La pregunta aquí és, qui guanya amb l'ús del *Big Data* i l'empremta digital?

Al món real no hi ha un sol vigilant com a la novel·la d'Orwell, sinó que les dades passen per moltes mans. Neix així una nova professió, la del *Data Broker*, que a diferència del broker de borsa, és intermediari en operacions de compravenda de dades personals (Sedano, 2017). Però per sort, a Espanya gràcies a la Llei Orgànica de Protecció de Dades de Caràcter Personal (LOPD), que va entrar en vigor el 13 de desembre del 1999 i que es va modificar finalment el 2011, els usuaris estan més protegits que en altres països. El nostre país no permet l'exercici dels *Data Brokers* sense el consentiment de l'usuari. Però, el problema aquí és que molt poca gent llegeix totes les condicions d'una aplicació abans d'acceptar-les. A l'actualitat, obtenir el consentiment quan els usuaris estan acostumats a donar-lo a "Acceptar" sense problemes, és la cosa més senzilla del món, per la qual cosa a la pràctica moltes vegades estem donant l'autorització perquè s'explotin les nostres dades amb fins comercials, a través d'interminables polítiques de privadesa, sense ni tan sols ser-ne conscients. La legislació espanyola no permet la venda de dades personals entre empreses, per la qual cosa moltes es fan amb elles de dues maneres. La primera és mitjançant una aliança d'empreses en què una empresa paga a una altra perquè enviï publicitat d'aquesta als seus usuaris registrats. La segona és quan una companyia se'n fa amb una altra per quedar-se amb els usuaris sense ànim de seguir amb el desenvolupament de l'activitat.

I com els governs segueixen les activitats en línia dels ciutadans? Doncs a través de proveïdors d'Internet, xarxes socials, malware i sistemes automatitzats. És important subratllar que els governs sovint tenen poders limitats per supervisar les activitats en línia dels ciutadans i que aquests poders sovint es basen en lleis i reglaments. Els governs han de complir la legislació de privadesa i només poden supervisar les activitats en línia dels ciutadans si estan autoritzats legalment per fer-ho.

Aquest control de dades per part dels governs té avantatges. En els darrers vint anys, les tecnologies de la informació i la comunicació (TIC) han prevalgut a les ciutats, transformant-les en "ciutats intel·ligents". Grans empreses, com IBM, Oracle, Siemens i Microsoft, han fomentat el desenvolupament d'aquestes ciutats. ja que afavoriria l'ús dels seus productes. A més, els governs veuen aquestes "ciutats intel·ligents" com a progressistes, ja que hipotèticament són més segures, funcionals i sostenibles. Per exemple, Filadèlfia calcula que està estalviant un milió de dòlars cada any amb sensors a les papereres que poden indicar quan el contenidor està ple i, per tant, reduir el nombre de recollides innecessàries. Per mantenir aquest urbanisme intel·ligent, els governs i les empreses han de recollir masses de dades sobre els seus ciutadans. O Songdo, Corea del Sud, és una ciutat dissenyada amb sensors per controlar la temperatura, l'ús d'energia i el trànsit de tota mena, també disposa d'un sistema d'absorció dels residus sòlids que automàticament els condueix a grans túnels que els porten al dipòsit final. A més, les interconnexions entre els sensors instal·lats als carrers i els dispositius electrònics personals poden arribar a permetre que l'usuari rebi avís automàticament quan és a prop el seu autobús. Així, pel bé de la societat, els ciutadans renuncien a part de la seva privadesa: hi ha una compensació.

A més, els governs també poden utilitzar el *Big Data* per entendre com es comporten els ciutadans davant de noves polítiques i serveis. De fet, a través de les xarxes socials, per exemple, els governs poden recopilar informació i millorar les seves polítiques per adaptar-les a les necessitats i preferències dels ciutadans. Les dades governamentals tenen molts propòsits i usos diferents: mesurar els resultats del govern, millorar resultats i qualitat operativa, prendre decisions de planificació i ampliar la consciència general i comprensió dels serveis i resultats del govern. Les dades s'utilitzen en cada fase de l'elaboració de polítiques i el procés d'implementació de polítiques, inclosa la planificació de programes, la gestió de les operacions diàries, realitzar revisions de seguiment o posteriors a l'acció, preparar informes estadístics i realitzar investigacions i avaluacions. Un exemple és quan algun polític llança un globus sonda, la població dóna una resposta, ja sigui positiva o negativa, a les seves xarxes de la proposta.

A continuació es mostren les àrees on la recopilació de dades por ajudar als governs:

1) Ciutats i governs regionals: Ajuda a gestionar els costos, optimitzar els serveis, gestionar les infraestructures de manera intel·ligent i crear marcs de gestió del rendiment que mostrin valor a totes les parts interessades.

2) Impostos i assistència social: Combinant aquestes eines amb anàlisis predictives, es detecten fraus i maximitza la recaptació mitjançant programes de contacte amb el client optimitzats i rendibles.

3) Seguretat: Responen les amenaces a la seguretat, tant interns com externes, supervisant de manera visual els esdeveniments d'un país, frustrant activitats delictives a través de patrons mòbils, també protegeix la nació contra les amenaces externes, tant digitals com físiques.

4) Defensa: Ofereix un sentit al complex seguiment de la informació logística i la seguretat de les dades.

5) Educació: Ajuda a optimitzar els plans d'estudi i el rendiment dels cursos per obtenir el màxim valor dels recursos disponibles.

6) Salut: A través de dades històriques, juntament amb els patrons de mobilitat actuals, els governs poden entendre un brot de malaltia i prendre mesures per controlar-lo, alhora que poden iniciar programes de benestar dirigits a cohorts específiques del país, dirigint programes preventius de atenció sanitària.

7) Reduir els fraus financers: A través de sofisticats algorismes, es rastregen immediatament les transaccions dubtoses, proporcionant informació sobre el comportament dels ciutadans i mitigant els fraus financers.

8) Millors iniciatives de benestar: Mitjançant l'anàlisi dels sentiments és possible fer un seguiment dels sentiments nacionals i desenvolupar nous serveis i iniciatives d'acord amb les necessitats dels ciutadans. Les dades governamentals tenen molts propòsits i usos diferents: mesurar els resultats del govern, millorar resultats i qualitat operativa, prendre decisions de planificació i ampliar la consciència general i comprensió dels serveis i resultats del govern. Les dades s'utilitzen en cada fase de l'elaboració de polítiques i el procés d'implementació de polítiques, inclosa la planificació de programes, la gestió de les operacions diàries, realitzar revisions de seguiment o posteriors a l'acció, preparar informes estadístics i realitzar investigacions i

avaluacions. Els mitjans de comunicació i el públic també utilitzen les dades governamentals per a informació general i per fer diferents decisions personals.

En el cas de les empreses és diferent. Les empreses creen sistemes de captació de dades per mantenir els seus clients con són regals, subscripcions a ofertes, etc. Les dades són necessàries per mantenir una comunicació activa amb els clients. En ocasions el client no sap que està donant el consentiment per l'ús de les seves dades. Les lleis espanyoles i europees sobre protecció de dades impedeixen que les empreses comprin les bases de dades pròpies a altres empreses. En canvi sí que es poden adquirir legalment mitjançant servidors que busquen a Internet noms, direccions de correu electrònic o números de telèfon sempre que estiguin publicats, de forma similar a com funciona un buscador d'Internet.

5.4. ALTERNATIVES AL BIG DATA

Al llarg del treball s'ha vist, sobretot amb les enquestes i la opinió pública, que l'ús del *Big Data* i l'empremta digital no són ben rebuts. Encara que pel que s'ha vist, aquest ús és molt ampli i bastant útil. És un fenomen que molt difícilment marxarà. És molt poc probable que es deixin d'utilitzar les dades personals com una eina empresarial o governamental. És per aquest motiu que durant la realització del treball s'han plantejat altres opcions no tan intrusives, però que segueixin fent ús de les dades personals.

5.4.1. VENDA DE DADES

Federico Zannier és un jove nord-americà que es va oferir a lliurar la seva empremta digital d'un dia per només 2 dòlars. Diu que va violar la seva pròpia privadesa a partir del febrer durant uns 50 dies seguits, gravant captures de pantalla i càmeres fotogràfiques de sí mateix cada 30 segons i fent un seguiment de tots els seus passos mitjançant la tecnologia GPS. Va registrar l'adreça de cada pàgina web que va visitar (emmagatzemar uns 3 milions de línies de text) i va acumular 21.124 fotos de càmera web i 19.920 captures de pantalla. L'objectiu de Zannier, una mica paradoxalment, era apropiar-se de les seves dades venent-les. Assenyalava que sovint cedim les nostres dades privades sense voler-ho, atès que poca gent es dedica a llegir els termes i condicions de les aplicacions i serveis en línia. Les empreses recapten milions de dòlars venent la nostra informació a empreses de màrqueting mentre rebem poc a canvi. Però Zannier no només vol fer una declaració sobre la privadesa en línia, sinó que té previst utilitzar els fons per crear una extensió del navegador i una aplicació per a telèfons intel·ligents que, segons ell, ajudarà els altres a vendre les seves pròpies dades. El resultat ha estat que 213 usuaris han comprat les seves dades mitjançant mecenatge a

Kickstarter. En total les dades de Zannier van tenir un valor de 2733 dòlars. A Espanya per exemple, Movistar va comprar Tuenti en 2010 pagant 9,62 euros per usuari. Una xifra que de forma individual no és molt alta, però si es multiplica pels casi 8 milions d'usuaris que tenia la xarxa social, fa una quantitat considerable: 70 milions de euros (Sedano, 2017). Aquest experiment que va realitzar obre portes a noves solucions per tenir control sobre les teves dades. Quan s'accedeix a una pàgina *web,* un percentatge molt baix llegeix les condicions de privacitat (12% a Europa segons l'enquesta de Vodafone), per tant una gran majoria de la població no sap el que passa amb les seves dades. Una forma de saber-ho seria venent les teves dades a empreses. D'aquesta manera els usuaris podrien decidir quina informació donen i quina no, a quines empreses els hi donen i a quines no, i decidir què fan amb elles. Tant a Espanya com a Europa està prohibida la venta de dades, per tant aquesta solució no seria possible a nivell nacional o europeu.

Però imaginem un escenari en el que sí fos legal vendre les teves dades. No per empreses, sinó pels propis usuaris. Fer el que va fer Zannier. A l'enquesta de Vodafone, el 55% de la població preferia pagar per l'ús d'aplicacions que donar les seves dades. Què passaria si fos al reves? Que les empreses haguessin de pagar per tal d'accedir a les nostres dades. Guanyaríem control sobre la informació que donem a les empreses. Facebook, per exemple hauria de pagar als seus usuaris per aconseguir les seves dades. Però aquesta idea tan idíl·lica comporta alguns reptes. És poc probable que el preu sigui tan just. No és fàcil determinar quin és el valor de mercat de les nostres dades, de manera que és probable que acceptem el que els altres pensen que acceptarà el mercat massiu. Per exemple, quin és el valor de les fotos que comparteixes a les xarxes socials en un any? Depèn de qui ets i de quant saps sobre el potencial de les teves dades. I iniciar un model com aquest és pràcticament impossible. Cap empresa acceptaria pagar per informació que aconseguien de manera gratuïta.

5.4.2. OPEN DATA

L'*Open Data* són dades públiques a les que qualsevol pot accedir, i que persones, empreses i organitzacions poden fer servir per analitzar patrons i tendències, prendre decisions basades en dades i resoldre problemes complexos (secció 5 del diagrama). Totes les definicions de l'*Open Data* inclou dues característiques bàsiques: les dades han d'estar públicament disponibles perquè qualsevol les utilitzi i han d'estar organitzades d'una manera que en permet la reutilització. L'*Open Data* també ha de ser relativament fàcil d'utilitzar i ha d'estar disponibles gratuïtament o a un cost mínim. Aquest aporta una perspectiva que pot fer que el *Big Data* sigui més útil, més democràtic i menys amenaçador. Mentre que el *Big Data* es defineix per la mida, l'*Open Data* es defineix pel seu ús.

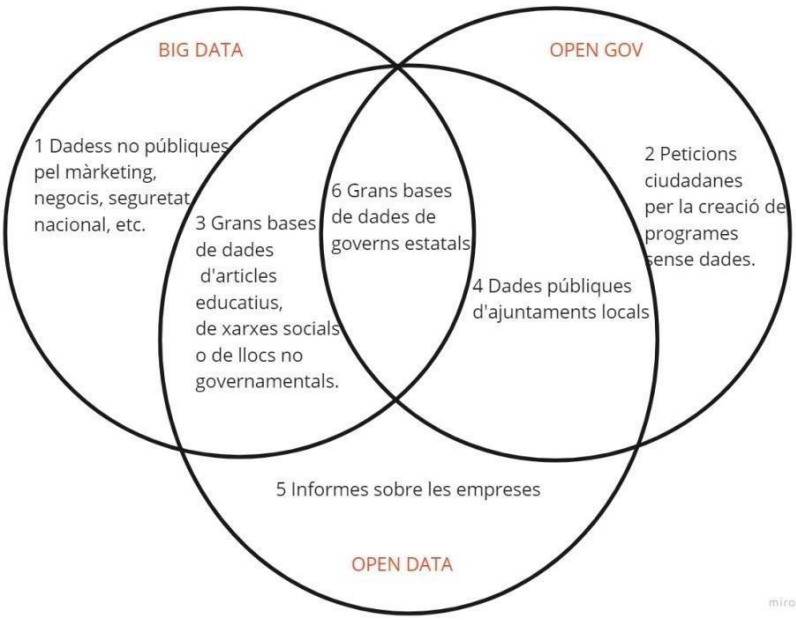
El *Big Data*, si no és obert al públic, no és gens democràtic. La secció 1 del diagrama inclou totes les dades on el públic no pot accedir: és el tipus d'informació que dóna avantatges a la gent que la controla però treu poder a aquells que no la tenen.

L'*Open Data* no ha de ser una base de dades enorme, quantitats modestes de dades poden tenir un gran impacte quan es fan públiques. Les dades dels governs locals (secció 4) per exemple, poden ajudar els ciutadans a participar amb el pressupost local, triar l'atenció mèdica, analitzar la qualitat dels serveis locals o crear aplicacions que ajudin les persones a navegar pel transport públic.

L'*Open Data* no ha de venir només de les administracions públiques, cada cop més científics estan compartint les seves investigacions en astronomia i altres àrees en un nou model col·laboratiu de recerca (secció 3). Altres investigadors utilitzen dades importants recopilades en mitjans socials, la majoria de les quals estan obertes al públic, per analitzar l'opinió pública i les tendències del mercat. Però quan el Govern converteix el *Big Da*ta en l'*Open Data*, és especialment poderós: les agències governamentals tenen la capacitat i els recursos per recopilar grans quantitats de dades, i l'obertura d'aquests conjunts de dades pot tenir grans beneficis econòmics.

I si fos el Govern qui proporcionés la infraestructura pública de dades? Això, de fet, ja passa quan es tracta de dades directament relacionades amb el Govern, a través d'iniciatives com Data.gov, el portal del Govern dels Estats Units per a les dades locals. La secció 6 mostra el resultat d'una bona combinació entre el *Big Data*, un govern obert i *l'Open Data*: una base de dades extensa amb tota la informació d'empreses i governs a l'abast de tothom. Però resulta difícil creure que seria una bona idea deixar que sigui el Govern qui subministri una infraestructura pública de dades de més abast. La innovació tecnològica requereix que molts grups de persones exposin i sotmetin a prova les idees d'altres grups diferents. Seria necessari crear una organització sense ànim de lucre que es dediqués a controlar la base de dades pública. Això implica una gran confiança per part dels ciutadans en aquesta organització, i un compromís de la organització en fer un bon ús de les dades i no deixar que cap empresa o govern intenti comprar les dades per usos privats. És un escenari poc probable, requereix molt esforç i els governs i empreses s'oposarien. Dit això, iniciatives com Data.gov seran una contribució important a la infraestructura pública de dades, però no poden constituir el nucli d'una potent infraestructura pública de dades d'ampli abast.

Figura 1:



Font: imatge recreada a partir de la imatge de Gurin (Gurin, 2014)

5.4.3. THICK DATA

El *Thick Data* fa referència a un complex ventall d'estratègies de recerca primària i secundària, incloses enquestes, qüestionaris, grups focals, entrevistes, revistes, vídeos, etc. És el resultat de la col·laboració entre científics de dades i antropòlegs per donar sentit a grans quantitats de dades. Junts, analitzen sèries de dades per extreure informació qualitativa com a coneixements, preferències, motivacions i raons dels comportaments. En essència, el terme *Thick Data* fa referència a sèries de dades qualitatives (observacions, sentiments, reaccions) que ofereixen informació sobre la vida emocional quotidiana dels consumidors. El *Thick Data* se centra a identificar emocions, històries i models al món on viuen les persones, per la qual cosa els seus resultats poden ser difícils de quantificar. Es pot confondre amb el *Big Data* però tenen les seves diferències.

1) El *Big Data* és quantitatiu, mentre que el *Thick Data* és qualitatiu.
2) El *Big Data* genera tanta informació que necessita alguna cosa més per tancar i/o revelar els buits de coneixement. El *Thick Data* descobreix el significat després de les visualitzacions i anàlisis del *Big Data*.
3) El *Big Data* revela informació a partir d'un rang determinat de punts de dades. El *Thick Data* revela el context social i les connexions entre els punts de dades.

4) El *Big Data* ofereix números. El *Thick Data* revela històries.
5) El *Big data* depèn de les tecnologies de d'Intel·ligència Artificial i l'aprenentatge de màquina, mentre que el *Thick Data* depèn de l'aprenentatge humà.

Si les grans tecnològiques de Silicon Valley aspiren realment a entendre el món, han de capturar tant les seves quantitats (*Big Data*) com les seves qualitats (*Thick Data*). El procés de recol·lecció de dades dut a terme pel *Big Data* requereix una estandardització i un agrupament que desposseeix de context els resultats obtinguts. La immensa mida de les mostres fa impossible centrar-se en les històries particulars, històries plenes d'emocions que resulten fonamentals per entendre la relació entre el consumidor i el producte. El *Thick Data* no es mostra com a antagònic al *Big Data*, sinó com a complementari. No es tracta de la clàssica i maniquea oposició entre quantitatiu i qualitatiu, sinó més aviat d'entendre que les dues tècniques són igualment valuoses per obtenir un prisma general de la situació que estem analitzant. Mentre que el *Thick Data* perd escala, el *Big Data* perd resolució. Mentre que el *Big Data* aïlla variables per identificar patrons, el *Thick Data* assumeix la complexitat humana. Dues cares de la mateixa moneda.

Per entendre les persones, cal entendre'n el context. La major part del món és coneixement de fons. Més enllà de tractar d'entendre'ns atenent exclusivament allò que fem, el *Thick Data* cerca entendre com ens relacionem amb els diferents mons que habitem. Mentre que el *Big Data* requereix un procés algorítmic generalment dut a terme per estadistes i matemàtics, el *Thick Data* és terreny d'antropòlegs, sociòlegs i científics socials.

Hi ha una tecnologia que permet combinar les dues coses. Es tracta de la computació afectiva.

La computació afectiva és l'estudi i el desenvolupament de sistemes i dispositius capaços de reconèixer, interpretar, processar i simular els afectes humans. Sembla de pel·lícula de ciència ficció en les que apareixen robots i intel·ligències artificials amb emocions, com per exemple 'I Robot', '2001', 'WallE', o 'Eva'. Algunes vegades, aquests robots emocionals generen problemes inesperats pel seu comportament que, en certes circumstàncies, és menys predicible del que seria el comportament d'una màquina purament racional. En altres ocasions, però, és el fet de tenir un components emocional el que permet als robots actuar de forma raonable, entendre als humans i respectar les decisions que prenem encara que racionalment pareix que no són bones per a nosaltres.

Es tracta d'un camp interdisciplinari on es donen la mà la informàtica, la psicologia i les ciències cognitives. L'origen d'aquesta branca de la ciència informàtica, la més moderna, es remunta a la publicació el 1997 del treball de Rosalind Picard sobre Computació afectiva (Lapedriza, 2019). Un dels objectius d'aquest estudi era la capacitat de simular empatia. Això exigiria als equips informàtics interpretar l'estat emocional dels humans i adaptar-ne el comportament a ells, oferint respostes adequada a aquestes emocions. Per fer això es necessita un sistema de reconeixement d'emocions es basa en captar, amb sensors, senyals relacionats

amb les nostres emocions. Per exemple fer servir càmeres per capturar imatges o vídeos de les persones, per observar els moviments facials, els gestos o la situació en què es troba una persona. També podem fer servir sensors integrats al cos per capturar senyals fisiològiques com el ritme cardíac o la respiració, o fer servir micròfons per captar la veu i els canvis d'entonació quan algú està parlant. Per tant, mirant la càmera web a la seva pantalla, els investigadors de mercat ho prenen i diuen "aquesta persona sembla que no està interessada" i estan fent una inferència sobre el que signifiquen les seves expressions facials. Estan descobrint si els seus anuncis són avorrits i haurien de deixar de publicar-los. Tota aquesta informació conté senyals sobre l'estat emocional d'una persona. De fet nosaltres mateixos fem servir aquest tipus d'informació per intentar reconèixer les emocions d'altres persones. Un cop capturats aquests senyals es poden fer servir tècniques d'aprenentatge automàtic per aprendre, a partir de moltes dades, patrons en els senyals que són informatius sobre l'estat emocional d'una persona.

Actualment no hi ha cap sistema automàtic que pugui reconèixer i entendre perfectament les emocions d'una persona. Tot i això, aquest tipus de tècniques sí que s'apliquen ja per a problemes i casos concrets. L'anàlisi dels moviments i gestos de la cara i la seva relació amb l'estat emocional és una de les línies de recerca que ha estat més activa dins de la Computació Afectiva, i ja hi ha programari comercial que analitza els moviments de la cara per reconèixer emocions. A més, actualment s'està estudiant com fer servir aquestes tècniques en diferents aplicacions, com per exemple al camp de la conducció assistida.

Per últim, i com un extra que semblava interessant, l'empremta digital i el *Big Data* es poden relacionar amb la intel·ligència artificial. És per això que se li ha preguntat a una IA solucions per protegir les nostres dades. S'ha utilitat el ChatGPT i ha donat aquesta resposta:

1) Utilitza cercadors per comprovar la teva petjada digital.
2) Limita el que comparteixes.
3) Verifica la teva configuració de privadesa.
4) No comparteixis en excés la teva vida personal a les xarxes socials.
5) Evita els llocs web insegurs.
6) No divulguis dades privades en xarxes Wi-Fi públiques.
7) Crea contrasenyes segures i utilitza un administrador de contrasenyes.

Aquestes alternatives al *Big Data* són recents i poc explorades. Són teories i esborranys de propostes que, en un futur, poden tenir un gran impacte. El que ha resultat curiós és que una Intel·ligència Artificial com ho és el ChatGPT hagi donat una resposta per "protegir" les nostres dades, saben perfectament que aquesta cerca ha sigut emmagatzemada i ja forma part de la meva empremta digital.

VI. CONCLUSIONS

L'anàlisi del *Big Data* i l'ús de l'empremta digital són unes noves tendències en l'ús de la informació que pot generar beneficis tant a les empreses com a tota la societat donat l'ampli univers de les aplicacions pràctiques que se li pot donar. No obstant això, els reptes tècnics que planteja no són senzills i requereixen molta inversió, cosa que pot provocar que els beneficis no arribin. Per una part, hi ha arguments que defensen la vigilància, però que ha d'existir registres raonables i accessibles al públic i responsabilitat per als qui aproven i realitzen la vigilància en qüestió. Per una altre part, hi ha arguments que defensen que aquesta vigilància recorda a lògica penitenciària moderna, el panòptic. Consisteix en que el presoner és observat sense que aquest pugui veure el seu observador. L'altíssima concentració i la centralització de la informació sembla aleshores conduir-nos de manera inexorable que el 99%-1% sigui també una realitat no només en la riquesa material sinó també en el coneixement de l'altre. En aquest cas, 1% coneix i anticipa els moviments i els sentiments del 99% restant, sense que aquest ho percebi, i menys que tingui accés al que aquest 1% predisposa per a la totalitat.

Quan es va realitzar la investigació de l'opinió pública a les xarxes socials, una cosa que s'ha trobat a faltar és la justificació de les opinions. O proves verídiques que sustentin les seves creences de que ens espien. També s'ha de considerar que justament aquesta és la gràcia de les xarxes socials. Dones la teva opinió en un fet, real o no, i la gent t'escolta i es posa d'acord amb tu, o al contrari. Ets "lliure" d'expressar les teves opinions sense haver de justificar-te a ningú. S'han trobat alternatives més "transparents" per l'ús de les dades, però per desgràcia no són molt utilitzades. Qui sap si en uns anys les empreses i governs les posin en pràctica; o que la població sigui conscient d'aquestes alternatives i demanin l'aplicació d'aquestes.

En el procés de fer aquest treball, la idea era simple: saber si la gent era conscient de que les seves dades eren utilitzades. A mida que s'ha anat investigant s'han anat descobrint nous temes de discussió, s'han descobert usos de les dades que no es sabien, com per exemple la importància de l'ús de les teves dades en campanyes polítiques. S'han detectat dos grups amb idees bastant polaritzades; per una part les empreses i els governs que estan a favor de l'ús de l'empremta digital, i per l'altre banda estan la gran majoria d'usuaris que consideren que l'ús de les seves dades és una violació de la seva privacitat.

Com s'ha dit anteriorment, s'han trobat alternatives que no violen la privacitat de les persones i, fins i tot, una IA ens ha donat solucions per protegir la nostra empremta digital. El que ha quedat clar és que l'ús de les dades no és una pràctica que vagi a desaparèixer. I és molt difícil lluitar contra això. Per tant, el millor que es pot fer és fer el possible per anar cap a una societat on aquestes pràctiques no suposin una violació dels teus drets.

VII. BIBLIOGRAFIA

Capote, R. A. (2020). El Big Data y la ciencia de la manipulación de las masas. *Granma* .

Consejo, P. E. (2016). *Reglamentos.* DIario Oficial de la Unión Europea.

Crawford, D. B. (21 / Septiembre / 2011). Six Provocatios for Big Data. *Oxford Internet Institute* , 17.

Deissner, D. (2016). *A European Survey on the Opportunities and Risks of Data Analytics.* Berlín: Vodafone Institute for Society and Communications.

Delgado, I. (2012). Big data: retos, posibilidades y aprovechamiento. *OpenMInd BBVA* .

DiPersio, D. (2022). *Data Protection, Privacy and US Regulation.* Marseille: European Language Resources Association.

Estado, J. d. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.* Boletín Oficial del Estado.

Big Data ethics, B. D. (2014). *Andrej Zwitter.* SAGE journals.

European Commission, Directorate-General for Communications Networks, Content and Technology, (2017). *Attitudes towards the impact of digitisation and automation on daily life – Report*, European Commission.

F. Paul Pittman, K. L. (8 / July / 2022). *ICLG.com*. Recollit de https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Gallagher, R. (13 / MAYO / 2013). *SLATE.* Recollit de SLATE.

Guerrero, L. D. (2018). *Control de nuestros datos personales en la era del big data: el caso del rastreo web de terceros.* Estudios Socio.Jurídicos.

Gurin, J. *Big Data and Open Data: How Open Will the Future Be?* CORE.

Gurin, J. (2014). Big data and open data: what's what and why does it matter? *The Guardian* .

IGN, G. (2017). Historia del Big Data. *IGN* .

Ikerfel. (2022). *Encuesta de Percepción Social de la Ciencia y la Tecnologia.* FECYT.

José Manuel Robles, J. T. (2020). *Big data para científicos sociales. Una introducción.* Madrid: Centro de Investigaciones Sociológicas.

Laney, D. (2001). *3D Data Management: Controlling Data Volume, Velocity, and Variety.* META Group.

Lapedriza, À. (1 / Abril / 2019). *Tecnología ++*.

Lucas, M. Á. (sense data). *MiBloguel.*

Lupton, D. (2015). *Digital Sociology.* Abingdon: Routledge.

Marr, B. (2014). Big Data: The 5 Vs Everyone Must Know. *Linkedin* .

Mohr, J. W. (2015). *Big Data/Big Theory - Part II.* Note from the Chair.

Nielsen, M. (2013). Big Data: ¿a quién pertenece? A *C@mbio: 19 ensayos clave sobre cómo Internet está cambiando nuestras vidas.* Madrid: OpenMind BBVA.

Picard, R. (12 / December / 2014). An Interview with Rosalind W. Picard: Adding Emotion to Computing. (H. Thorstensen, Entrevistador)

Richards, N. M. (2013). *The dangers of surveillance.* Harvard Law Review.

Robert Hasty, T. W. (2013). *Data Protection Law in the USA.* Advocates for International Development.

Sanabria, Á. (sense data). Big data y control social. *desde abajo* .

Sedano, J. A. (29 / Enero / 2017). *Diario Sur*.

Shelly Metzenbaum, B. K. (2022). *Government Decisions and Issues about Collecting and Using Data.* Urban Institute.

Telefónica. (10 / Mayo / 2023). *Telefónica*. Recollit de ¿A quién pertenecen los datos?