La privacitat dels nostres telèfons mòbils

MaTriX
2020-2021

Resumen

Actualmente estamos en un mundo donde cada día la tecnología avanza y estamos más expuesta a ella. Por eso se han diseñado leyes que protegen a los usuarios para que sus derechos de seguridad y privacidad no sean vulnerados, pero alguna vez estas leyes sean infringidas.

Este trabajo de investigación tiene el objetivo de identificar cómo gestionan las empresas los datos de los usuarios, si se utilizan sin nuestro consentimiento y nos perjudica, si la información personal de los usuarios es un negocio y las medidas de seguridad que implantan, y referenciar los métodos recomendados para gestionar y mejorar nuestra privacidad en el teléfono móvil. Además de hacer entrevistas a personas cualificadas y expertas en el tema de privacidad y seguridad.

Abstract

We are currently in a world where technology is advancing every day and we are more exposed to it. That's why laws have been designed to protect users, so that their security and privacy rights are not violated, but sometimes these laws are broken.

This research work aims to identify how companies manage user data, if it is used without our consent and harms us, if a user's personal information is a business and the security measures they implement, and to reference the recommended methods for managing and improving our privacy on the mobile phone work. In addition to interviewing qualified individuals who are experts in the field of privacy and security.

ÍNDEX

1.Introducció

Avui en dia la informació és poder.
Cada persona que té un telèfon mòbil genera molta informació personal que pot interessar a les empreses i utilitzar-la per al seu propi benefici sense que els usuaris ho sàpiguen. Nosaltres acceptem els permisos que les aplicacions dels telèfons mòbils ens demanen o les condicions de privacitat, sense saber res del que posava en aquell contracte, però simplement ho acceptem i sense saber com utilitzaran els permisos de la càmera, contactes, micròfons, GPS, etc.

Amb la innovació de noves tecnologies, com la domòtica, ha començat l'inici de la utilització de les intel·ligències artificials, com els assistents virtuals: Alexa i l'Assistent de Google. Aquests aparells electrònics ens escolten, i poden utilitzar la informació que generem sense el nostre permís, perjudicant-nos i utilitzar-la per al benefici d'altres, com empreses i el mateix govern.
El govern deixa que empreses com Amazon, Microsoft, Apple i Facebook administrin la informació dels usuaris per vigilar-los, controlar-los i manipular-los. També amb el sorgiment de COVID-19, a Espanya la utilització de l'aplicació COVID afectarà la nostra privacitat.

Per això els objectius d'aquest treball és investigar i identificar com gestionen les empreses les dades dels usuaris, si s'utilitzen sense el nostre consentiment i ens perjudica, si la informació personal dels usuaris és un negoci i les mesures de seguretat que implanten, i referenciar els mètodes recomanats per gestionar i millorar la nostra privacitat al telèfon mòbil . A més es farà entrevistes a persones professionals amb coneixements de seguretat i privacitat.
També amb aquest treball pretenc demostrar si la meva hipòtesi és correcta: utilitzar el mòbil implica la teva vulnerabilitat de la privacitat.
Ja que la majoria de la població posseeix un telèfon mòbil i està exposada a Internet a cada moment, això significa l'exposició de la informació personal de tots aquests usuaris. També conscienciar a la població de com s'està utilitzant les nostres dades i com poder millorar la seguretat i privacitat.

1.1. Metodologia

Per fer el meu treball d'investigació, faré una recerca bibliogràfica en diferents articles, diaris, revistes i pàgines web. La majoria del meu treball és una recerca d'informació, qualitativa, de tipus avaluativa, semiestructurada i fent entrevistes semipresencials a personal professional amb coneixements de tema tractat.

La majoria de la informació del meu treball és la de pàgina web de *la Agencia Española de Protección de Datos* (AEPD). Gairebé tota la informació estreta ha estat en castellà, però hi ha hagut informació extreta d'anglès.

Per fer les entrevistes primer m'he hagut d'informar i desenvolupar el cos teòric, per arribar a buscar persones amb perfils que s'ajustaven a les preguntes desenvolupades durant el treball de recerca.

2. Com gestionar la nostra privacitat

2.1. Privacitat digital

Avui en dia les persones generem molta informació personal a Internet o les xarxes socials pel seu ús quotidià fem accions molt habituals com donar *like* a una fotografia o buscar pel navegador. Aquestes accions deixen rastre sobre nosaltres a la xarxa. Encara que algunes persones creuen que navegar per internet és anònim, en realitat tota l'activitat que es genera pot quedar arxivada.
Per això hem de saber què és la privacitat digital i com poder millorar i augmentar la seguretat de la nostra informació personal, ja que cada vegada les tecnologies es van desenvolupant més ràpidament i la gestió de la nostra privacitat és cada vegada més complexa.

La privacitat digital és el dret que tenen tots els usuaris d'internet a protegir i controlar les seves dades que circulen per la xarxa i si aquesta informació és visible, si poden accedir altres persones i limitar-la.

2.2. Identitat digital

És el rastre que diàriament deixem en la xarxa a través de les nostres accions, com consumir series, vídeos de YouTube, les teves compres *online,* etc. Creant un perfil teu a la xarxa. Cada vegada el teu perfil es va detallant més i més gràcies a les xarxes socials perquè és un mirall que reflecteix la teva personalitat, que defineix qui ets o proporciona dades personals.
A causa de la identitat digital persones desconegudes o empreses poden saber que t'agrada, els teus *hobbys,* la data del teu aniversari, etc. A vegades aquestes accions poden ser beneficioses per a tu però també et poden perjudicar i fins hi tot, et poden robar la teva identitat digital.

2.3. Drets digitals dels usuaris

Quan utilitzem els serveis i aplicacions per a mòbils, és habitual deixar la nostra empremta digital. Podem compartir excessiva informació personal *online* coneguda com a *oversharing,* sense saber les conseqüències que poden arribar a tenir per altres persones o per a nosaltres mateixos, que poden arribar a sancions administratives i fins i tot penals.
Això és pel desconeixement que tenim els usuaris a l'hora de gestionar les nostres dades, posant en risc la nostra privacitat i la de tercers.
Segons *La Agencia Española De Protección de Datos* quan accedim, sense autorització, a informació d'altres persones o la publiquem sabent que ha estat obtinguda de manera il·lícita, a part d'estar vulnerant la seva intimitat, poden estar cometent un delicte de descobriment i revelació de secrets.

Les accions tan habituals com pujar una foto o vídeo a Instagram apareixent una tercera persona sense la seva autorització o sense el seu coneixement, és un delicte. Accedir al compte de correu electrònic i telèfon mòbil d'una altra persona sense el seu consentiment per conèixer informació seva, conversacions i missatges de caràcter absolutament privat i particular, és un delicte o vulnerar la normativa que protegeix la utilització de les dades de caràcter personal, encara que no siguem conscients ni la gravetat que comporta.

Però també quan la informació s'obté de manera lícita, com quan pugem una fotografia, gravació o àudio, encara que les realitzem amb el seu coneixement i sense que ningú més estigués present, no tenim cap dret ni permís per a després difondre-les, o quan s'obtenen de la persona o d'altres, però sense cap permís d'aquells per divulgar-les. Això és conegut com a *sexting,* que pot arribar a conductes delictives com l'assetjament, amenaces i les coaccions o *cyberbullying*. Aquestes accions han de ser denunciades, ja que és un dret que ens pertany.

Per això hem de tenir consciència sobre les nostres accions a la xarxa, cal conèixer quins són els nostres drets i les nostres obligacions.

La Unió Europea va dissenyar (BOE, 2016) un reglament a la protecció de les persones físiques en el tractament de dades personals i a la lliure circulació d'aquestes dades.
També en la pàgina oficial de la ("Ejerce tus derechos | AEPD", 2020) *Agencia Española Protección Datos* on ensenyen els teus drets i que permeten exercir davant de les persones o empreses encarregades de la teva informació personal, com el dret de rectificació, d'oposició o de supressió ("a l'oblit").

2.4. Millorar la nostra seguretat a la xarxa

Com usuaris d'Internet estem preocupats per si la nostra informació personal està segura. També com podem millorar i augmentar la nostra seguretat a la xarxa, ja que ningú vol que les seves dades i la d'aquelles persones amb les quals ens comuniquem es perdin o estiguin en terceres mans.
D'aquestes inquietuds va sorgir la ciberseguretat un conjunt de mesures físiques, lògiques i administratives destinades a la protecció digital de les empreses, persones i sistemes davant d'atacs digitals que puguin comprometre la confidencialitat, disponibilitat o integritat.

2.4.1. Criptografia

La Criptografia és l'art d'escriure amb procediments o claus secretes o d'un mode enigmàtic, perquè estigui escrit sigui intel·ligible per les persones no desitjades que vulguin saber informació nostra. La criptografia és una part molt important en la ciberseguretat, són unes mides extres de seguretat que proporcionen i aporten beneficis.

El problema d'utilitzar aquest sistema avançat en la seguretat és la seva complexitat i has de tenir un alt nivell de coneixements sobre els conceptes de ciberseguretat.
Per això a l'estudi (Garrigues, Robles, Borrell, Navarro-Arribas, 2010) *Promoting the development of secure mobile agent applications* hi han desenvolupat una arquitectura de software i un entorn per desenvolupar la implementació d'aplicacions basades en agents mòbils segurs. Aquests són programes intel·ligents i autònoms que poden navegar en la xarxa, buscant serveis que l'usuari necessita i interactuant amb ells, amb la finalitat de facilitar i accelerar el procés d'implementació de protocols criptogràfics, i permetre la reutilització d'aquests protocols pel desenvolupament d'agents mòbils segurs. Com a resultat, l'ús de tecnologies d'agent mòbil per la implementació d'aplicacions distribuïdes segures.
Simplificant el funcionament de les aplicacions basades en els agents mòbils. Per aquest entorn hi han desenvolupat tres eines principals: Agent Builder, Itenerary Dsigning Toll i Agent Launcher. Aquestes eines permeten dividir les diferents etapes del desenvolupament dels components.
L'element principal d'aquest software es Agent Builder, que permet la definició de protocols de protecció d'agents utilitzant el llenguatge de protecció criptogràfic d'agents mòbils (MACLP), amb diversos beneficis:

- Aquest llenguatge no requereix un ampli coneixement de la programació d'aplicacions criptogràfiques.
- Proporcionen funcions criptogràfiques d'alt nivell que no disposen de cap algoritme o implementació, així es pot reutilitzar el codi.
- És independent de les altres eines en cada plataforma i l'entorn d'execució.

Aquests avantatges permeten als experts poder utilitzar diverses vegades els protocols dels programes dels agents. Això significa que expandeix els agents mòbils amb els mecanismes de seguretat requerits per les aplicacions del dia a dia.
La diferència entre utilitzar agents mòbils alhora d'altres aplicacions distribuïdes és perquè a diferència d'altres tipus d'aplicacions distribuïdes els agents mòbils es poden moure autònomament d'un ordinador a un altre mentre s'està executant.
Això proporciona una reducció de la càrrega de la xarxa. En lloc de transferir grans quantitats de dades a través d'internet, s'envia els agents mòbils per millorar el suport per als dispositius mòbils amb connexió intermitent.
Encara que hi ha altres investigacions que ja han utilitzat els agents mòbils per fins de seguretat en la xarxa, però aquestes propostes s'han originat en el món de la intel·ligència artificial i s'han centrat a permetre que els programes expressen les capacitats del seu coneixement i no els mecanismes criptogràfics necessaris per protegir l'itinerari o els resultats de l'agent.

Aquesta nova arquitectura de software d'agent mòbil està basada en la plataforma on es vol utilitzar l'agent, però aquesta mateixa plataforma ha d'admetre tots els protocols de seguretat i s'han d'actualitzar cada vegada que apareix un nou protocol o millora. La seva funcionalitat és proporcionar els agents un codi que gestiona la seva pròpia protecció i execució. Aquest codi es coneix com a control AI, l'agent gestiona totes les tasques de manera autònoma, sense la necessitat de què les plataformes sàpiguen com està estructurat internament. Proporciona un itinerari que emmagatzema el conjunt de plataformes que l'agent ha de visitar i les tasques que hi haurà d'executar en cada plataforma. L'itinerari està compost per diferents nodes. És un punt d'intersecció, connexió o unió de diversos elements que conflueixen en el mateix lloc, on cadascun representa una etapa en la ruta de l'agent. Cada un d'ells té una tasca local i una plataforma d'execució associada, cada feina assignada haurà de començar i finalitzar en la mateixa plataforma, llavors no pot canviar a cap altra plataforma.
Els avantatges d'aquesta nova arquitectura són:

1. Emmagatzemar l'itinerari en una estructura separada que permet la seva protecció a partir de criptografia.
2. El codi de control es pot reutilitzar fàcilment perquè no depèn de les tasques realitzades per l'agent.
3. Els agents poden tenir diferents requisits de seguretat i implementar diferents esquemes de protecció diferent.
4. Tenir diferents tipus de nodes permet un disseny més flexible d'itinerari d'agent.

Ara, el desenvolupament d'un agent mòbil segur s'utilitza l'eina de disseny d'itinerari, Agent Builder i Agent Launcher.
L'eina de disseny d'itinerari (IDT) és una eina gràfica que es pot utilitzar per dissenyar l'itinerari de l'agent. Aquesta eina proporciona un editor d'itinerari gràfic on el programador pot definir el conjunt de nodes que componen l'itinerari. Després, es pot assignar una tasca i una plataforma d'execució a cada node. Amb tota la informació proveïda pel programador, aquesta eina produeix una especificació XML, especificació per dissenyar llenguatges de marcat, que permet definir etiquetes personalitzades per descripció i organització de dades, de l'itinerari inicial, a continuació l'Agent Builder es pot utilitzar per generar l'agent final. Per poder

utilitzar-lo, els programadors han d'especificar quins mecanismes de protecció requereix la seva aplicació. Aquests mecanismes han de definir-se utilitzant el llenguatge de protecció criptogràfica de l'agent mòbil (MACPL).
Una vegada que s'obté l'agent, el Llançador d'agents (AL) s'utilitza per executar a l'agent a la primera plataforma de l'itinerari.
Primer, el programador agent, que dissenya l'itinerari explícit i genera l'especificació XML utilitzant l'IDT. Després, l'expert en seguretat, que implementa els protocols de protecció de l'agent utilitzant MACPL.
Finalment, l'usuari final, que executa l'agent i obté els seus resultats sense cap coneixement sobre seguretat o programació. La separació d'aquests tres rols mostra la flexibilitat i la facilitat de reutilització que l'entorn del desenvolupament proposat aporta a les implementacions. Per tant, el desenvolupament d'un sistema complet es divideix en components independents - especificacions XML i MACPL- i eines independents que poden ser
utilitzades persones diferents.

2.4.2. Connexió gratuïta en espais públics

En algun moment de la teva vida t'haurà passat que no tens dades 4G per poder navegar per internet o enviar un missatge i has hagut de connectar-te a una xarxa pública. També has utilitzat la connexió Bluetooth per connectar-te a un altre dispositiu sense fil com uns auriculars. Aquest tipus de connexió de vegades poden ser molt perilloses perquè permeten l'intercanvi d'informació, sigui per wifi o Bluetooth, però aquestes dues connexions sense cables són diferents i tenen avantatges i inconvenients respectivament.

Riscos de connectar-se a una xarxa wifi pública

El wifi és un tipus de tecnologia que permet la connexió sense fil a Internet des de diferents dispositius.
Actualment podem trobar diferents punts per accedir a una xarxa wifi pública, normalment gratuïtes, en parcs, centres comercials, cinemes, etc. A vegades necessiten un registre previ.
Connectats en la xarxa pública deixem tota la nostra informació i l'activitat en terceres mans de qualsevol persona que sigui una mica hàbil en ciberdelinqüència.
Per això ara explicaré els diferents atacs i tècniques que poden utilitzar, i amb això et pensaràs dues vegades a connectar-te a una xarxa pública gratuïta:

- **"Man-in-the Middle"**: Aquesta tècnica és molt senzilla d'executar, simplement l'atacant s'ha de posar entre el dispositiu (objectiu) i la connexió wifi (font), passant totalment incògnit. Així aquesta persona pot veure tota la nostra informació i l'activitat en la xarxa.
- **"Xarxes Trampes"**: En aquest atac el ciberdelinqüent crea una xarxa wifi amb les mateixes característiques que l'original. Simplement el nostre dispositiu hauria d'accedir al senyal wifi i ja podria connectar-se el nostre dispositiu i controlar-lo.

Pot ser que de vegades no sapiguem com hem estat connectats aquest wifi maliciós, i és perquè en els nostres dispositius hi ha una opció de connectar-se automàticament a la xarxa wifi més pròxima, llavors això ens deixa més vulnerables l'atacant.
La millor manera perquè no passin aquestes coses és NO connectar-se a una xarxa wifi pública. Encara que sigui una excepció molt important, hem d'intentar no donar accés a les nostres dades o credencials de serveis crítics ni transaccions bancàries.

Riscos de connectar-se a una connexió Bluetooth

El principal problema del Bluetooth és mantenir-lo actiu sempre en el nostre dispositiu, encara que no ho estiguem utilitzant. Pot semblar que això no sigui una amenaça, però és una exposició als ciberdelinqüents i vulnera la nostra seguretat i privacitat.
Si tenim la connexió Bluetooth activada tota l'estona, s'estarà enviant simultàniament i continuada informació, encara que no estigui sincronitzada a un altre dispositiu. Això significa que durant un període de temps s'està enviant un senyal per intentar connectar-se al dispositiu, on els atacants podran localitzar la ubicació.
També es pot realitzar la tècnica del **"Man-in-the-Middle"** deixant el nostre dispositiu vulnerable i permeten la intercepció de tota la informació i activitat que s'estigui enviant.

Ara els usuaris que tenen *wearables*, rellotges intel·ligents, sabatilles d'esport amb GPS incorporat o polseres que controlen el nostre estat de salut, s'estan qüestionant si estan indefensos per tota la informació personal que crea sobre el nostre estat físic, anímic, hàbits, hora d'anar a dormir, edat, en què lloc està, etc. Vinculat a una aplicació en el nostre dispositiu mòbil. Aquí el problema més gran és si la nostra informació està segura, tota la informació registrada la pot veure qualsevol persona o si el fabricant l'està usant per a seu propi benefici.
Per això abans d'adquirir un *wearable* has de preguntar si aquest dispositiu té un mecanisme de xifrat que garanteix la confidencialitat de la teva informació, qui té accés a la informació personal, què permisos necessita l'aplicació, és guarda la informació al núvol, etc.
Recerca la millor garantia de seguretat i privacitat per l'ús de la teva informació personal, revisa les opcions de privacitat i seguretat de les configuracions que incorpora el dispositiu i configurar els mecanismes de protecció que porta l'aplicació amb la qual es gestiona el *wearable*.

Per protegir-nos i millorar la nostra seguretat en les connexions hauries de:

1. Connexions xifrades:
    - Bluetooth: tenir l'última versió, perquè a partir de la versió 4.0 totes les connexions entre dispositius venen xifrades per defecte.
    - Wifi: utilitzar pàgines segures i xifrades.
2. Utilitza antivirus que et protegeix al connectar-te a les xarxes sense fils.
3. Eliminar les xarxes wifi i dispositius Bluetooth als quals t'has connectat prèviament perquè poden revelar la teva ubicació anterior.
4. Desactivar les connexions Bluetooth i wifi si no les estàs utilitzant.

5. Fer servir xarxes VPN (xarxa privada virtual): permet xifrar tota la informació que es transmet des dels teus dispositius en el moment de connectar-se a una xarxa wifi.

2.4.4. Mode incògnit

Quan naveguem per Internet, per defecte tota l'activitat que hem realitzat amb el navegador directament s'emmagatzema en la memòria del dispositiu i no desapareix, això significa que es pot conèixer la teva empremta digital per Internet. Per poder evitar això els navegadors proporcionen als usuaris un de navegació privat o majorment conegut mode incògnit, especialment si utilitzes dispositius públics o compartits amb altres persones.

La funció d'un navegador incògnit és la següent:

- ❑ Elimina les *cookies* i borra la memòria després de sortir del navegador.
- ❑ No guarden les pàgines visitades en l'historial ni mostren els arxius descarregats.
- ❑ No guarden les contrasenyes ni permet l'autocompletat de formularis.

Però aquest mode no proporciona l'anonimat:

- ❑ No oculta l'adreça IP.
- ❑ No estableix connexions segures i/o xifrades.
- ❑ Les pàgines emmagatzemen la informació sobre la teva visita a la web.
- ❑ Els administradors de la xarxa poden veure les pàgines visitades.
- ❑ No proporciona privacitat total.

És important conèixer la informació que emmagatzema els navegadors sobre nosaltres i què configuracions poden tenir per la seva utilització, per poder evitar els riscos com que tota la teva informació en Internet està a la vista de qualsevol persona que tingui accés al navegador, donant informació de les teves preferències en Internet i que la teva sessió en una pàgina web quedi oberta en el navegador, i et suplantin la identitat.
Per poder evitar aquestes coses és necessari adaptar una sèrie de mides per disminuir els riscos en qualsevol navegador que utilitzis:

- Sempre tenir l'última versió del navegador.
- Revisar les opcions de configuració del navegador i adaptar-les per protegir la teva seguretat i privacitat.
- Borra l'historial de navegació quan no ho necessites.
- Elimina les *cookies*.
- Utilitza gestor de contrasenyes perquè no sigui el teu navegador qui les gestioni.
- Tanca **sempre** la sessió quan surtis d'una pàgina web, així evites que si una persona utilitza el teu dispositiu, no accedeixi a la informació personal amb la teva sessió iniciada.

2.4.5. La importància de les contrasenyes

La contrasenya és una de les primeres barreres de seguretat que té cada dispositiu mòbil. La majoria sabem que les contrasenyes són importants el problema és que no estem preparats per tenir diverses contrasenyes per a cada sessió que iniciem així que utilitzem una o a vegades dos per accedir als diferents serveis. Tampoc tenir una contrasenya de més de 10 caràcters i diferents entre ells, però és important perquè és la clau als teus serveis i per tant a la teva informació personal.

Per això hi ha una sèrie de recomanacions i consells per poder millorar la teva contrasenya i així la teva seguretat i privacitat:

- **Gestor de contrasenyes**: per la gent oblidadissa i mandrosa aquesta és una de les millors opcions. És un programa que permet emmagatzemar de forma segura les teves claus i accedir als diferents serveis.
- **No utilitzar contrasenyes per defecte**: s'ha d'evitar la utilització d'aquestes contrasenyes per defecte i canviar-les. Amb aquesta mesura evitem l'accés no permès, ja que si deixem les contrasenyes per defecte, poden trobar-les i ser utilitzades amb diferents usuaris.
- **No compartir les contrasenyes amb ningú, no hem d'apuntar-les en cap lloc ni escriure-les en correu ni formularis web on el seu origen no sigui segur** perquè si o fas ja no serien secretes, perdrien la seva utilitat i estaràs dóna-li a una altra persona la teva privacitat.
- **Contrasenyes robustes** perquè siguin fortes, difícils d'endevinar s'ha de complir uns requisits:
    - ❑ Han de tenir com a **mínim** 8 caràcters amb majúscules, minúscules, nombres i caràcters especials.
    - ❑ No han de tenir paraules senzilles en qualsevol idioma, nombre propis, dates, llocs o dates de caràcter personal ni paraules curtes.
    - ❑ Tampoc claus formades únicament per elements o paraules que poden ser públiques o fàcilment endevinables, com per exemple només data de naixement.
- **No utilitzar la mateixa contrasenya per a diferents serveis**.
- **Canviar les contrasenyes periòdicament**: garantir la confidencialitat de les contrasenyes, ja que amb el pas el temps es pot veure compromeses.
- **No utilitzar el recordatori de contrasenyes** perquè facilita l'accés a persones no autoritzades.

Amb aquests consells es pot millorar la teva seguretat i no accediran amb facilitat a la teva informació personal ni els serveis utilitzats, però si encara no estàs segur o segura sempre està l'opció de la **verificació en dos passos** que afegeix una capa de seguretat extra que consisteix que en el procés on has de posar el teu nom d'usuari, contrasenya i després incorpora un codi que solament tu coneixeràs i que generalment s'obté a través del telèfon mòbil. Gràcies amb aquesta opció extra l'accés serà més complicat per a terceres persones als teus serveis *online*.

2.4.6. Cal donar tanta informació personal?

En aquesta era digital la nostra informació és molt important, ja que proporciona una part de la teva identitat digital que pot ser exposada en qualsevol part d'Internet.
Per això abans de facilitar dades personals hem d'analitzar la informació que t'estan demanant, per què volen la teva informació i si és necessària proporcionar-la, perquè no és el mateix contractar un segur del teu vehicle que subscriure's a Netflix. En la primera opció segurament serà necessari proporcionar més informació personal, mentre que en la segona opció solament serà aquelles dades sobre el pagament online i correu electrònic.

Perquè donar més informació de la necessària por arriba a:

- Rebre missatges spam.
- La teva identitat digital i privacitat estiguin exposades.
- Ser víctima d'una estafa, extorsió o xantatge.
- Si dones dades de terceres persones sense el seu consentiment, et poden denunciar.

Per poder evitar això, tu has de decidir que informació teva donar. On tens la capacitat de tenir, decidir i conèixer sobre el teu dret a la protecció de les teves dades personals en el (BOE, 2016) Reglament (UE) 2016/679 General de Protecció de Dades (RGPD).
Abans de donar cap informació has de tenir en compte:

- ➔ Quina és la finalitat? Per què les volen utilitzar?
- ➔ Com la gestionaran?
- ➔ Com exercir els teus drets: Accés, Rectificació, Supressió, Oposició, Limitació del tractament i Portabilitat.
- ➔ El temps que conserven la informació.
- ➔ Mai facilitar informació personal de terceres persones sense el seu consentiment perquè no tens dret a proporcionar dades.
- ➔ No facilitis més dades personals que les estrictament necessàries.

2.4.7. Seguretat al núvol

El núvol és un dels serveis que et proporciona accedir als teus fitxers des de qualsevol lloc i dispositiu, organitzant informació i compartint-la. Això també permet la sincronització automàtica del núvol amb el dispositiu fent una còpia de seguretat amb l'avantatge de tenir la teva informació sempre accessible, no tenir el problema de perdre tots els teus arxius i informació quan perds o et roben el dispositiu perquè s'emmagatzemen en el núvol facilitant compartir informació i la sincronització dels teus dispositius.

No obstant això, no posis en perill la teva informació. Per això has de saber com protegir-te per qualsevol problema que pugui haver-hi:

- Ajustar les opcions de privacitat i seguretat del servei (núvol) a les teves necessitats.

- El servei que utilitzis sempre ha de comptar amb xifrat https i el seu propi certificat de seguretat.
- Si utilitzes el núvol com a còpia de seguretat utilitza un altre suport com un disc dur.
- Utilitza una contrasenya forta, tancar sessió després d'utilitzar-la. Si et proporciona la verificació en dos passos, utilitza-la.
- Verifica que si comparteixes arxius que la persona sigui la indicada.

3. Com gestionen la nostra informació

3.1. Reglament General de Protecció de Dades

El Reglament General de Protecció de Dades és un reglament Europeu que protegeix a les persones respecta el seu tractament de la informació personal i la lliure circulació d'aquesta. Va dirigit principalment a les empreses, les organitzacions, organismes i institucions en la Unió Europea o empreses que negocien amb ella. Aquest reglament conté unes lleis que protegeixen a la ciutadania i donen a conèixer els drets que tenen.

Obligacions de les empreses en el tractament de la informació personal dels usuaris

Les empreses, administracions o altres entitats tenen la responsabilitat de complir uns principis i obligacions que s'implanta en el Reglament General de Protecció de Dades.
Els principis són:

- **Principi de licitud, lleialtat i transparència**: Aquest principi consisteix en el fet que les dades de caràcter personal han de ser tractades de manera lícita, lleial i transparent. Això significa que la informació personal ha de complir les bases jurídiques que compleix el RGPD. El principi no inclou que les teves dades siguin tractades de forma deslleial o sense proporcionar-te tota la informació necessària sobre l'objecte i fins de tractament, les seves conseqüències i possibles riscos, obliguen als responsables que tracten les teves dades personals que proporcionin la major transparència possible.
- **Principi de limitació de la finalitat**: La teva informació personal serà utilitzada per a un propòsit determinat, explícit i legítim, i mai serà tractat de manera incompatible amb altres propòsits.
  La seva finalitat per la qual les teves dades seran utilitzades ha d'estar molt clara i definida, per l'ordenament jurídic. No es podrà gestionar les dades per a una finalitat no determinada ni definida.
- **Principi de minimització de dades**: Les dades personals seran convenients, pertinents i amb límits necessaris relacionats amb els fins tractats.

No serà possible obtenir informació ni utilitzar-la si en qualsevol moment poden ser útils o simplement per tenir-les.

- **Principi d'exactitud**: Les dades seran exactes i en el cas d'haver d'actualitzar-les s'haurà d'adaptar a les mesures perquè es corregeixin o eliminin segons els fins que s'han tractat.
- **Principi del termini de conservació**: Les dades personals seran mantingudes de forma que permetin la identificació de les persones interessades per un període de temps mai superior als fins tractats.
  Després que les dades hagin estat utilitzades per al seu fi, a continuació s'hauran d'eliminar o que no es pugui identificar les dades personals de les persones interessades.
- **Principi d'integritat i seguretat**: Les dades personals seran tractades de manera que s'asseguri la seva seguretat, com la protecció contra la utilització no autoritzada o il·lícita i contra la seva pèrdua, destrucció o dany accidental, aplicant les mesures tècniques i organització apropiades.
  Això significa que el principal objectiu serà la protecció contra qualsevol risc que amenaci la seguretat de la informació personal de l'usuari.
- **Principi de responsabilitat proactiva**: En el tractament s'ha de complir aquest principi de responsabilitat on ha de demostrar el seu compliment.
  El responsable pot realitzar el tractament de les teves dades de caràcter personal si es dóna alguns d'aquests casos:
  - ❑ Has prestat el teu consentiment per una o diversos fins específics, com quan et subscrius a un servei *online*.
  - ❑ El tractament és necessari per a l'execució d'un contracte en el qual és part o per l'aplicació a peticions de les teves de mesures, com el tractament de dades de nom, cognoms i fotografia d'un treballador per la targeta d'identificació de l'empresa.
  - ❑ Si el tractament és necessari per satisfer els interessos legítims del responsable o per un tercer, sempre que no domini els interessos o drets del titular de les dades, com l'accés a les imatges de videovigilància d'un aparcament per identificar qui n'hi ha colpejat el cotxe.
  - ❑ El tractament és necessari per al compliment d'una obligació legal aplicable al responsable del tractament, com l'obligació de facilitar informació de caràcter tributari a l'AEAT.
  - ❑ El tractament és necessari per al compliment d'una missió d'interès públic o en l'execució de poders públics conferida al responsable del tractament, com del suposat principal que empara els tractaments per les Administracions Públiques, quan existeix una competència atribuïda per Llei.
  - ❑ El tractament és necessari per protegir interessos vitals de l'interessat o d'una altra persona.

Seguretat

El responsable que s'encarrega d'obtenir i utilitzar les teves dades personals ha de complir uns mesures de seguretat tècniques i organitzatives per protegir la teva informació:

- Evitar accessos no autoritzats.
- Realitzar còpies de seguretat.
- L'anonimat i el xifrat de dades.
- Realitzar un control de l'emmagatzematge, dels usuaris, dels suports i de l'accés a les dades.

També, tots aquells que vulguin intervenir en la gestió o tractament de les dades siguin amb el deure secret, i amb l'aplicació del RGPD:

- Els tractadors de la teva informació personal hi han d'avaluar els riscos per garantir un nivell de seguretat abans d'implementar cap mesura de seguretat.
- Si es produeix alguna fissura de seguretat, els responsables hauran d'avisar-te.
- Si alguna persona té les teves dades personals i vol tractar amb elles, i pot suposar un risc de seguretat, prèviament haurà d'avaluar quines conseqüències tindrà.
- Qualsevol persona que tracta amb les teves dades personals haurà de tenir en compte la 'Privacitat per disseny' i 'Privacitat per defecte'.

Transparència de la teva informació

El responsable que adquireix les teves dades personals ha de facilitar-te d'on ha obtingut aquesta informació, el tractament de les dades i determinada informació.
El RGPD implementa aquest dret, diferenciant entre la informació que s'ha de facilitar depenent de si les dades personals s'han obtingut directament o no.

Primer, la informació s'ha de facilitar prèviament a la recollida o registre.
Segon, quan es tingui la informació el responsable ha d'informar dins d'un període de temps responsable:

- Abans d'un mes a partir de l'obtenció de les dades personals.
- Abans o en la primera comunicació amb l'interessant.
- Abans que les dades s'hagin comunicat amb altres destinataris.

Això és una obligació que ha de complir el responsable.

El RGPD també regula una sèrie d'hipòtesis on serà necessari complir amb el dret d'informar:

- Quan l'interessat ja disposa de la informació.
- Si les dades no són de l'interessat, quan la comunicació sigui impossible, el registre o la comunicació està establerta pel Dret de la Unió o dels Estats membres, o quan les dades segueixin sent confidencials per un deure legal de secret.

3.2. Política de privacitat

La política de privacitat és un document legal establert en el Reglament General de protecció de dades (RGPD), on s'organitza i es tracta les dades de caràcter personal de les persones

implicades (clients). Aquesta política implica l'obligació que té el responsable del tractament de les dades a la transparència i facilitar-te la informació necessària i requerida. Un document que consta que les teves dades personals seran de caràcter privat i secret.

La finalitat de la política de privacitat és informar els usuaris sobre com s'està gestionen les seves dades amb una accessibilitat i disponibilitat en un llenguatge simple i fàcil d'entendre. L'usuari tindrà el control sobre totes les seves dades i podrà accedir a elles en qualsevol moment per modificar o sol·licitar la baixa del seu ús.

Avui en dia aquesta política és necessària, ja que qualsevol pàgina web, xarxa social o aplicació pot recollir les teves dades personals i de vegades sense que tu ho sàpigues, amb les nomenades *cookies*.
La política de privacitat recull una sèrie d'apartats, dels quals són articles del RGPD, com:

- Identificació del responsable del tractament de les dades de caràcter personal.
- Finalitat del tractament de dades.
- Termini de conservació de les dades.
- Base de legitimació per al tractament de les dades.
- Destinataris de les dades.
- Drets dels interessats.
- Dret a retirar el consentiment.
- Possibilitat de reclamar davant l'autoritat de control (AEPD).
- Seguretat i confidencialitat de les dades.
- Identificació del delegat de protecció de dades.
- Especificació dels interessos legítims del responsable del tractament.
- Transferències internacionals de dades.
- Elaboració de perfils, així com l'existència de decisions automatitzades.
- Finalitat secundària del tractament.

3.3. Permisos

Quan ens descarreguem una aplicació, sigui la que sigui, sempre ens diran que donem permís per poder accedir a la càmera, micròfon, àudio, emmagatzema, etc. Per què és necessari per poder utilitzar aquella aplicació i els seus serveis, però alguna vegada t'hauràs preguntat per què necessita la llanterna del mòbil accedir a la ubicació d'un usuari? I una aplicació de retoc fotogràfic al micròfon? O una gravadora als contactes? Per què tants permisos? Ja que aquestes aplicacions no necessiten aquests permisos per funcionar.
No obstant això, a vegades no són obligatoris els permisos i els desenvolupadors busquen extreure informació de l'usuari, sense el seu consentiment, per fins lucratius. A més si és una aplicació maliciosa obtenir informació personal teva i robar-la.

La primera cosa que fem quan ens descarreguem una aplicació és donar els permisos sense pensar si són necessaris i vitals perquè l'aplicació funcioni correctament. Algunes poden ser molt transparent, però altres no tant i un estudi (Otero, 2018) de la Universitat de la Northeastern va demostrar que poden activar la càmera, fer fotografies, gravar vídeos i fins i tot activar la ubicació i saber on estàs. Durant un any va estar comprovant al voltant d'unes 17.000 aplicacions més populars d'Android. El resultat va ser preocupant, però hi va haver una part positiva. La investigació va comprovar que no utilitzen el micròfon per "espiar-nos". Encara que si feia fotografies i vídeos sense el permís de cap usuari.
Entre les aplicacions implicades unes 8.000 eren propietat de Facebook que poden enviar informació a la xarxa social, i més del 50% demanaven permís per accedir a la càmera i al micròfon, suposant un risc pels usuaris de la seva privacitat.
Per demostrar els resultats les persones implicades a la investigació van utilitzar un programa automàtic com mètode per interactuar amb l'aplicació, l'anàlisi va demostrar que els arxius d'àudio no s'enviaven a tercers, però algunes aplicacions havien gravat vídeos i fent captures de pantalla del que estaven fent en el telèfon mòbil. Unes conclusions inquietants.

Com aquesta investigació hi ha moltes que demostren que les aplicacions i grans empreses violen els permisos dels usuaris per recopilar informació i utilitzar-lo per a fins lucratius sense el consentiment de cap usuari. Una investigació (Business insider España, 2019) realitzada per l'Institut Internacional de Ciències de la Computació en col·laboració amb la IMDEA i l'Institut Madrileny d'Estudis Avançats van descobrir que més de 88.000 aplicacions analitzades, 1.325 infringeixen la denegació de permisos. I et preguntaràs com ho feien si no li donaven els permisos. Doncs si navegues, a donar el permís de la ubicació utilitzaven les metadades de les teves fotografies o les teves connexions a xarxes wifi per esbrinar igualment on ets.

La vulnerabilitat de la nostra privacitat és una realitat i encara que hi hagi estudis i investigacions que ho certifiquin, els usuaris continuen donant el seu permís per poder utilitzar aquelles aplicacions i fins i tot el telèfon mòbil.

Per poder estar més conscienciat i estar més segurs quan ens descarreguem les aplicacions hi ha una sèrie de consells:

- Fonts fiables: descarregar solament les aplicacions en botigues oficials com Google Play o Apple Store.
- Comprovar qui és el desenvolupador: hi ha moltes aplicacions malicioses que es volen passar per l'original i poden tenir problemes.
- Nombre de descàrregues: aquest nombre de descàrregues és un bon senyal per veure si és de fiar o no.
- Permisos: revisar els permisos que ens demanen les aplicacions és una cosa essencial.
- Aplicacions imprescindibles: instal·la aplicacions que vagis a utilitzar i de tant en tant revisar i fer una neteja per eliminar aquelles que no utilitzis.
- Bloqueja els serveis "Premium" o de "tarifa especial".

4. El nostre rastre per internet

4.1.Empremta digital

L'empremta digital és la marca que deixem navegant per Internet, captan tots els registres i rastres. Deixa constància de com ens comportem, parlem, comentem, on i quan en la xarxa. Tota la informació que recopila pot ser beneficiosa per nosaltres, però de vegades pot ser utilitzada per a tercers per obtenir beneficis a la nostra costa.
Això preocupa als usuaris perquè és un risc directe a la nostra seguretat i privacitat.
Aquesta empremta digital crea un perfil complet al navegador.

L'obtenció de la nostra informació a través d'Internet són les *cookies* que guarden aquesta informació, recopilen dades personals i la nostra activitat en una pàgina web. Amb aquesta informació van generant el concepte que coneixem com Big Data, generant perfils dels usuaris amb tota la seva informació que pot arribar a mans equivocades.

4.2. *Cookies*: rastrejadores innates

Actualment la majoria de les persones coneixen l'existència de les *cookies* i les coses que comporta. Segurament alguna vegada buscant alguna cosa per Internet, com un viatja, després d'uns dies et surten anuncis similars i ofertes, o fins i tot a persones del teu entorn. Això passa per les *cookies*.

Les *cookies* són un petit fitxer que emmagatzema en els nostres dispositius tota la informació que hem generat en una pàgina web. Guardant dades de caràcter personal, preferències personals, personalització de continguts, idioma, zona horària, enllaços de xarxes socials, accessos a comptes, etc. La seva finalitat és adaptar el contingut de les webs al perfil de l'usuari i necessitats, facilita una navegació ràpida i senzilla.
També són les encarregades de mantenir una sessió de l'usuari oberta i guardar la informació que s'ha introduït prèviament en un formulari, es poden utilitzar de manera abusiva envaint la nostra privacitat sent un risc per la seguretat en Internet.
Les *cookies* no van associades a la persona o usuari, sinó al navegador web, per exemple si navegues habitualment per Google Chrome i vols provar navegar per la mateixa web, però amb Firebox veuràs que la web no s'adonarà que ets la mateixa persona.

Tipus de *cookies*

Hi ha diferents *cookies* tenint en compte com l'ús en el temps, qui és el propietari o la funcionalitat.

- Duració en el temps:

- ➔ **Persistents**: generalment són *cookies* de preferència i estadística que s'emmagatzema en el disc dur fins que són eliminades per l'usuari o arribant a una data límit, s'eliminen automàticament.
- ➔ **De sessió**: aquestes serveixen per mantenir la sessió oberta mentre navegues per diferents pàgines. S'eliminen quan s'ha tancat el navegador o es tanca la sessió.

- Propietat:
  - ➔ **Pròpies i de configuració de la pàgina**: aquelles que pertanyen a la pàgina web i que serveixen per emmagatzemar les preferències i la sessió de l'usuari mentre navega en la pàgina.
  - ➔ **De tercers**: són aquelles que s'utilitzen per crear un perfil de l'usuari a partir de recopilar les pàgines que visita, les recerques, els seus gustos generades per servidors o proveïdors, per explotar-les amb fins publicitaris.
- Funcionalitat:
  - ➔ **Preferències**: serveixen perquè la pàgina estigui amb els requisits i gustos de l'usuari, com idioma, regió, etc.
  - ➔ **Seguretat**: s'encarrega d'identificar els usuaris i evitar l'ús incorrecte de les credencials per part de terceres persones.
  - ➔ **Processos**: utilitzades pel correcte funcionament de la pàgina en el navegador.
  - ➔ **Publicitàries**: per fins publicitaris personalitzats.
  - ➔ **Estats de la sessió**: recapta la informació del comportament de l'usuari en una pàgina web, com el temps que ha passat.

Els usos maliciosos de les *cookies*

Les *cookies* no poden ser perilloses per si mateixes, sinó un protocol que utilitza Internet per facilitar la comunicació entre servidors i usuaris.

El seu perill és quan són obstaculitzades o falsificades per ciberdelinqüents o empreses que infringeixen la política de privacitat. Això significa que es poden fer-se passar per qualsevol usuari en una pàgina web, recopilar dades personals de forma secreta o fins i tot robar credencials.

Les accions que poden realitzar són:

- ❑ Vulnerabilitat en el software de l'equip o en el navegador web robant *cookies* de sessió, com credencials.
- ❑ Botigues *online* fraudulentes: mentre navegant per Internet, les *cookies* de tercers registren totes les recerques que es comet i el frau és quan tota aquesta informació s'utilitza per dirigir l'usuari a botigues fraudulentes a partir de publicitat enganyosa.
- ❑ *Fake new*s: el propietari guanya diners a partir de la publicitat que penja i el volum de tràfic que obté.
- ❑ Robatori de *cookies* o segrest de sessió: és quan s'introdueix una *cookie* modificada en el navegador de l'usuari que anteriorment ha accedit a la pàgina web controlada. A continuació quan la pàgina necessita autentificació la *cookie* modificada es farà passar per la legítima i obtindrà credencial de l'usuari, del correu electrònic i xarxes socials.

Llavors que haurien de fer amb elles. Primer, les *cookies* es poden eliminar, acceptar o no i bloquejar configurant el navegador.
Acceptar o no acceptar les *cookies* comporten riscos. No acceptar-les comporten que, per exemple, en les botigues *online* serà impossible realitzar comprar *online* i s'haurà de trucar o visitar la botiga física.

Per poder evitar els usos maliciosos hi ha una sèrie de consells:

1. Sigui la que sigui la decisió d'acceptar o no les *cookies*, es recomana que es consulti la política de *cookies* de cada pàgina web que visita per considerar les opcions.
2. Configurar en el navegador les *cookies*.
3. Actualitza el navegador.
4. Borra en un període de temps les teves dades de navegació, com les *cookies*.
5. Mira els missatges o notificació de les pàgines webs abans d'acceptar-les.
6. Navega en mode incògnit o privat en dispositius públics.
7. Cada cert temps analitza el teu dispositiu amb un antivirus.
8. Utilitza gestor de contrasenyes per protegir les claus.

Les *cookies* de tercers a les empreses

Ja sabem que les empreses utilitzen les *cookies* de tercers en els navegadors per personalitzar el teu navegador, obtenint una informació molt valuosa sobre els consumidors i creant perfils dels usuaris amb els seus gustos, aficions, dades personals, etc.

Hi ha hagut casos d'empreses que han utilitzat les *cookies* de manera fraudulenta (Burgueño, 2014). Aquestes empreses van ser sancionades per utilitzar Google Analytics, Google Maps, Youtube, WordPress i Zopim, entre altres, instal·lant cookies sense complir la Llei de *Cookies*. L'agència Espanyola de Protecció de dades va posar multes de 4.500 i 500 € a les empreses anònimes.

Les coses estan canviant i Google ha anunciat que va eliminar les *cookies* a tercers ("¿Qué pasará cuándo Google elimine las cookies de terceros?", 2020), ja que altres navegadors ja les han eliminat com Firefox i Safari, i Google no es podia quedar enrere.
Amb aquesta modificació millora la privacitat de tots els usuaris, anuncis més controlats i informació detallada sobre el comportament dels usuaris. Encara que eliminin les cookies de tercers, existeixen més tipus i a partir d'aquí sostrauran la informació.

4.3. Big Data

Actualment, les empreses generen i controlen una quantitat molt valuosa d'informació i són conscients de la importància que tenen i els beneficis que poden produir.
En Internet l'enorme quantitat de dispositius connectats a la xarxa fa que el volum d'informació dels usuaris vagi augmentant exponencialment.
Tot això és conegut com el Big Data, un enorme volum d'informació generada cada dia emmagatzemada, analitzada i processada perquè en funció dels resultats es pugui obtenir conclusions que permetin fer decisions per minimitzar costos, maximitzar producció, ajustar horaris, gestionar comandes, etc. D'acord amb les dades obtingudes en la fase d'anàlisis de dades dels usuaris.

Maneres de recopilar informació i els seus usos

Ja sabem que a partir dels ordinadors i els nostres telèfons mòbils les empreses recopilen informació constantment, però existeix una gran varietat de dispositius que també poden enviar informació valuosa diàriament. Qualsevol dispositiu que tingui connexió a Internet té la capacitat de recopilar informació sobre l'usuari de com l'utilitzem i qualsevol acció que fem com una transacció bancaria, trucades, bateria utilitzada, etc.

Per això grans companyies com Google o Amazon centren el seu negoci en la recopilació d'informació dels seus usuaris creant perfils i patrons de comportament. Dirigint publicitat adequada per cada usuari generant molts beneficis.

La majoria d'empreses han de tenir molt clar els conceptes de seguretat i privacitat. Els usuaris han de tenir la sensació de comoditat i seguretat perquè són les empreses les que gestionen la seva informació. Això significa, que han de ser transparentes la forma en què recopilen i processen les dades, sent aquestes accions conscients pels usuaris. Però també hi ha empreses que no respecten la legalitat de com recopilar la informació i accedint aquesta a tercers a partir de falses campanyes de vals descomptes.
La Llei Espanyola recull el dret fonamental a la protecció de dades personals. La LOPD (Llei Orgànica de Protecció de Dades de Caràcter Personal) obliga a les persones, empreses i organitzacions, tant privades com públiques, que depenguin de dades de caràcter personal a complir una sèrie de requisits i aplicar determinades mesures de seguretat en funció del tipus de dades que tinguin, el seu origen de les característiques del tractament, etc.

Com evitar la recopilació abusiva

En la LOPD existeix un concepte de recollida abusiva de dades, en la qual es denunciable.
Per evitar la recopilació abusiva de dades i conèixer tots els detalls sobre que us faran, hem de seguir les següents recomanacions:

- Llegir les condicions d'ús del servei, limitar la informació que recopilaran i configurar com és farà servir aquesta informació.
- Abans d'enviar o publicar informació, pensar que podria fer-se pública.
- Quan ens registrem en els comptes com Instagram, Twitter, etc. És important comprovar que informació compartirem i en cas de vincular dos comptes hem de limitar al màxim la informació compartida.
- Quan sigui necessari un registre per poder utilitzar un servei és millor utilitzar l'opció d'adreça de correu per limitar l'accés a informació personal que tenim a la xarxa social.
- Formulari de registre que permet accedir a través del compte de Facebook, Google i correu electrònic.
- Abans d'instal·lar una aplicació per a dispositius mòbils comprovar que permisos sol·liciten.
- Si l'empresa que recopila dades té seu a Espanya podem exercir els drets ARCO «Accés, Rectificació, Consulta i Oposició» segons indica la LOPD, ha d'estar inclòs en la informació legal del web o en l'aplicació.
- Abans de comprar un dispositiu amb accés a Internet, especialment els Iot, comprovar que dades recopila i on les envia. Si és possible configurar-lo perquè enviï els menys possibles.

Denunciar els casos d'incompliment legal per:

- Recull abusiva d'informació.
- Cessió il·legal de dades a altres companyies.
- Comunicacions comercials no sol·licitades com ara el correu brossa.
- No informar o atendre peticions sobre els drets d'accés, rectificació, Consulta o Oposició (ARCO) de dades personals.

5. Intel·ligències artificials

En l'actualitat les intel·ligències artificials són una part revolucionaria en la indústria tecnològica i podem observar que cada vegada s'està incorporant al nostre dia a dia.
La Intel·ligència artificial és aquella que proporciona una intel·ligència simulada a la dels éssers humans a una màquina, a partir de sistemes capacitats per aprendre i raonar com una persona.
Les opcions més properes que tenen els usuaris avui en dia són els assistents virtuals de veu, que els podem trobar en qualsevol dispositiu tecnològic com en un dispositiu Android l'assistent de Google o Apple, Siri. Aquesta funció ve incorporada ja en el telèfon mòbil, però també hi ha dispositius individuals com altaveus intel·ligents com l'Amazon Echo amb l'assistenta Alexa o Google Home. La majoria d'usuaris tenen activat o utilitza aquests serveis, ja que és fàcil d'utilitzar i fa accions com posar música o mirar el temps. Accions més còmodes

i senzilles. Els altaveus intel·ligents també permeten connectar-se a les instal·lacions elèctriques domèstiques i fer accions com encendre o apagar llums amb una ordre amb la veu.

Però alguna vegada hauràs parlat sobre un producte i el mòbil o fins i tot el teu altaveu intel·ligent estava al costat teu, i un dia t'apareix un anunci sobre aquest mateix producte. De cop i volta et qüestiones si de veritat t'estan escoltant i "espiant".
Si tens connectat i funcionant els assistents del teu telèfon mòbil o el teu altaveu intel·ligent evidentment l'àudio està connectat tota l'estona fins al moment que l'actives pronunciant per exemple "OK Google" o "Hey, Siri". Llavors és normal que aquest assistent estiguin escoltant tota l'estona fins que activis el seu servei per veu, però i si les coses que li diguessis s'estiguessin guardant, registrant i analitzant? Per defecte, en el cas de Google, fa un registre i un emmagatzemament en el núvol de tots els àudios que has fet dient "OK Google". Tot això ho pots comprovar en ("Google - My Activity", n.d.) Activitat en la Web i en Aplicacions de Google. Aquí veuràs, a part de la teva activitat en el buscador, totes les peces d'àudio que has fet i faràs registrades i podràs reproduir-les.
Tot això no queda aquí, una investigació per part d'un nord-americà (Day et al., 2019) demostra com Amazon utilitza transcripcions humanes per analitzar aleatòriament tota mena de petits fragments d'àudios a través dels assistents Alexa del altaveu intel·ligent per fer informes que permeten millorar els algoritmes.
També (Hernández et al., 2019), tant Google com Apple, diuen que fan servir aquesta funció per millorar els seus serveis i experiències dels usuaris.

6. La "nova normalitat" en la nostra privacitat en època de la COVID-19

La pandèmia del 2020, la COVID-19 ha posat a tot el món en una situació d'emergència sanitària, aportant mesures per poder controlar els contagis i la seva evolució.

Les iniciatives proposades per àmbits públics i privats suposa la utilització d'informació personal dels ciutadans i ciutadanes del país. Aquestes idees seran desenvolupades per aplicacions específiques o pàgines web.
Però això que suposarà pels ciutadans i ciutadanes en la seva privacitat i seguretat. Una vulneració per poder controlar la pandèmia? (Véliz, 2020) Perquè alguns governs com el de la Xina han posat mesures de seguretat tecnològiques que vulneren la privacitat dels seus ciutadans i ciutadanes. També en Corea del Sud hi han publicat informació personal de persones que han sigut afectades per la COVID-19. Israel podria utilitzar serveis d'intel·ligència secrets per vigilar i controlar els ciutadans i ciutadanes a través del seu mòbil. Els Estats Units estan desenvolupant idees similars que violen els drets dels ciutadans.

A Espanya s'estan desenvolupant unes aplicacions ("Comunicado de la AEPD sobre apps y webs de autoevaluación del Coronavirus | AEPD", 2020), on la seva finalitat serà el control de la pandèmia on únicament les dades personals seran utilitzades per aquest fi. Una de les funcions per les quals s'utilitzarà la informació, serà informar sobre l'ús de la mateixa aplicació d'autoavaluació realitzada per les administracions públiques o l'obtenció d'estadístiques com les dades de geolocalització per informar les zones més o menys afectades. Aquesta informació serà facilitada a les persones majors de 16 anys. Els menors de 16 es requereix l'autorització del seu pare, mare o tutor/a legals.
Per saber si d'aquestes aplicacions són fiables i el tractament de les dades de caràcter personal solament les autoritats públiques competents, el Ministre de Sanitat i els Consellers de Sanitat de les Comunitats Autònomes, podran compartir dades entre ells i els professionals sanitaris que tractin amb els pacients o intervenen en el control de la pandèmia.
Els organismes privats que col·laboren amb les autoritats competents solament poden utilitzar les dades segons les instruccions d'aquestes.
Segons el Reglament UE i LOPDGDD es pot notificar si hi ha hagut algun problema de seguretat de les dades personals, obligació de comunicar als interessats dels seus drets i llibertats.

La funció que més temor fa als ciutadans i ciutadanes d'Espanya és la geolocalització. Aquesta funció serà utilitzada aquelles persones que han donat positiu per COVID-19 a través del seu telèfon mòbil, on han facilitat prèviament el seu nombre al mòbil, per controlar la seva quarantena, prendre mesures i limitar la circulació de les persones. També s'està implementant notificar a persones que han estat a prop de les persones amb signes de COVID i que aquestes també facin la quarantena, això significa que encara que no hagis donant positiu en COVID-19 hauràs de donar permís per la funció de la geolocalització i fer una quarantena encara que no sàpigues si has donat positiu perquè no està previst fer test per confirmar.

Aquestes idees estan en fase de prova i encara que siguin un extra per poder controlar la pandèmia no són una eina d'exactitud que digui quines persones estan afectades, ja que haurien de fer test a qualsevol persona que ha estat al voltant de la persona afectada per determinar el nombre exacte i poder controlar la seva quarantena.
Llavors la qüestió és perquè no posen com prioritat fer test. Les mesures, com les aplicacions, suposadament seran temporals fins que hi hagi una vacuna i en tot el món estigui controlat, però i si aquestes mesures ja no siguin temporals amb l'excusa d'un rebrot quan ja existeix una vacuna efectiva? Aquí és on està el problema i on cada ciutadà i ciutadana ha de vigilar els seus drets de privacitat.

Encara que aquestes mesures no estan implementades completament cap persona sap com evolucionarà la pandèmia i si finalment aquestes mesures seran activades per tots els ciutadans i ciutadanes d'Espanya. Però si ens hem d'assegurar que els nostres drets i llibertat siguin efectuats per l'Agència de Protecció de Dades i no vulnerin la nostra privacitat ni abusin d'ella.

7. Entrevista a professionals

Per a la part pràctica d'aquest treball he seleccionat a persones professionals amb coneixements de seguretat i privacitat.

Josep Cañabate Pérez
Advocat especialitzat en protecció de dades i drets digitals.

1. **La política de privacitat beneficia els usuaris sobre com s'està gestionant les seves dades i informant-los?**

En teoria hauria de ser així, les polítiques haurien d'incloure tota la informació sobre la finalitat perquè s'utilitzen les dades, les mesures de seguretats, el dret d'accés, oposició, rectificació, supressió, etc., qui és el responsable del tractament, si es fan transferències internacionals, etc, és a dir, tot el que obliga el Reglament General de Protecció de Dades que és una norma de la Unió Europea, i la Llei Orgànica de Protecció de Dades i Garantia de Drets Digitals. Tanmateix, en moltes ocasions o no es compleix amb el que es diu a les polítiques, i es fa un ús de les dades no conforme amb la normativa, o les polítiques no estan ben realitzades. He vist molts casos en el que es fa un copiar i pegar d'altres web, p.e., això és indicatiu de que no es prenen en serio la privacitat.

- **És fàcil violar aquesta política?**

Doncs, lamentablement sí. És molt fàcil vulnerar les polítiques, i fer servir les dades per altres finalitats, o vendre-les a tercers, i com he dit és complicat en moltes ocasions que l'usuari sigui conscient d'aquesta vulneració.

2. **Creus que les lleis establertes pel Govern protegeixen la seguretat i privacitat dels usuaris quan cedeixen les seves dades de caràcter personal?**

Des de l'aprovació del RGPD s'ha avançat molt, però és insuficient, ja que la tecnologia de la informació encara avança més ràpid, i les possibilitats de vulnerar la llei augmenten exponencialment.

- **Com ho fan?**

Obliguen als responsables de tractaments a establir mesures de seguretat, a organitzar les seves empreses per protegir les dades, a formar als seus empleats. També estableixen mecanismes d'inspecció, canals de denúncia, etc.

- **Les accions que han de prendre són eficaces i ràpides?**

No són del tot eficaces, ja que com he dit internet i les tecnologies de la informació ofereixen possibilitats de fer un ús incorrecte de les dades. La solució està en la línia de la privacitat pel disseny, és a dir, fer sistemes de la informació que ja respectin la privacitat de les dades, per exemple, xifrat, anonimització, minimització.

3. **Quines són les sancions que s'imposen quan infringeixen les lleis?**

Et passo aquest enllaç a on ho expliquen molt bé https://ayudaleyprotecciondatos.es/2019/02/19/sanciones-rgpd-lopd-2019/ en general ha augmentat molt en relació a la legislació anterior, i representen percentatges de la facturació global, el qual és un salt molt elevat en las sancions.

- **Quan una gran empresa, com Google, infringeix les lleis les sancions són suficients per a què no hi hagi cap infracció més?**

Em temo que no, tot i que les multes són multimilionàries, el guanys encara són més grans, per tant, de cara a la galeria semblen que les multes són molt elevades, però en realitat no ho són tant, ja que el seu negoci es basa quasi totalment en explotar les dades dels usuaris, sempre al límit de la legalitat.

4. **El Reglament General de la Protecció de Dades implementada per la Unió Europea protegeix a la ciutadania de possibles problemes, però creus que aquest reglament és efectiu, es compleix i els càstigs per a qui les incompleix són ràpides i eficaces?**

La situació ha millorat molt, i quan les autoritats de control detecten una possible infracció la investiguen i sancionen, també estan els canals de denúncia, però com he dit hi ha una "xifra fosca" molt difícil de controlar, que és el veritable problema. En aquest sentit, el càstig per les grans companyes no són efectius, a més, poden recórrer les multes, arribar als tribunals, etc. Com he dit la solució és canviar el model de recollida de dades, potser amb intermediaris tecnològics als quals apoderem i tingui el control de les nostres dades amb tecnologies com Blockchain que possibilita el control sobre les nostres dades.

Jordi Delgado
Com a organitzador de Cryptoparties des de 2013.

1. **Encara que hi hagi evidències que les grans empreses utilitzen la informació dels usuaris per al seu propi benefici, com algun cas de Facebook, per què les persones segueixen cedint la seva informació perquè pugui ser vulnerada?**

Imagino que hi ha dos factors principals:

1) El servei proporcionat per les empreses és percebut com imprescindible per aquestes persones. Diguem que pensen que no poden viure sense aquest servei.

2) La poca consciència del dret a la privadesa i la seva importància. Això seria conseqüència de la creença, molt estesa, de que "jo no tinc res a amagar". Òbviament, aquesta creença és falsa. Adonar-se d'això és el punt de partida de la conscienciació.

2. **Què aconselles als usuaris per poder protegir la seva privacitat i seguretat?**

Primer de tot cal ser conscient de fins a quin punt la privadesa és important. Aquest seria un pre-requeriment imprescindible.

Després, canviar d'hàbits i sacrificar comoditat en adoptar comportaments més sensibles a les dades i la seva privadesa. Un exemple el tens en la resposta a la següent pregunta

3. **¿Vostè protegeix la seva seguretat a Internet i la seva privacitat? Com?**

La resposta és sí. Com? Doncs:

1) No formant part de CAP xarxa social (ni twitter, ni facebook, ni instagram, etc). Sí que estic a Mastodon (xarxa social oberta semblant a Twitter) però no ho faig servir.

2) Caldria evitar l'ús d'eines associades a empreses i canviar-les per eines de programari obert. Aquesta part és molt difícil d'assolir, sobre tot donada la dependència que patim tots de Google i Microsoft i/o Apple. Personalment només faig servir Linux, però no sóc "lliure" de Google (faig servir telèfons Android, tinc adreça de Gmail, utilitzo Google Maps, etc.)

3) Utilitzant navegadors diferents per tasques diferents:

- Chrome per a webs de confiança on he de treballar/consultar habitualment (facultat, banc, escola fills, etc)

- Mozilla Firefox + extensions (HTTPS Everywhere, NoScript, uBlock Origin, FoxyProxy, etc.) per navegar per llocs arriscats o que desconec.

- Tor Browser quan vull nivells afegits de privadesa i anonimat.

4) Fent servir i gestor de paraules de pas de codi obert (KeePassX) i fent servir paraules de pas diferents i, sobre tot, llargues (20 caràcters o més) per a cada lloc web on cal que em doni d'alta.

5) Xifrant-ho tot. Navegació a internet, e-correus (amb GnuPG, i l'extensió Enigmail del gestor d'e-correu Thundrerbird de Mozilla) quan cal, tramesa de fitxers des de o cap al núvol (núvol propi del departament on treballo, no un servei alié), etc.

6) Canviant de sistema operatiu si cal: Habitualment faig servir Linux, però de tant en tant utilitzo Tails (versió de Linux proporcionada pel projecte Tor, on tota comunicació va per Tor).

4. **Està segura la nostra privacitat implementant mètodes i barreres de seguretat o sempre hi haurà una bretxa que ens exposi?**

No existeix la seguretat al 100%. Facis el que facis, sempre hi haurà algun tipus de vulnerabilitat mitjançant la qual podran arribar a tu.

Ara bé, això depèn de quin tipus de persona siguis. Si no fas res destacable (des del punt de vista de ser "persona d'interès") no has de patir gaire. Si ets l'objectiu d'alguna agència d'intel·ligència d'un estat, hi ha poc que puguis fer per evitar atacs.

5. **Com creus que serà la nova normalitat amb el tema dels rastrejadors i / o aplicacions per detectar i controlar la COVID-19? Serà una invasió a la nostra privacitat per a un bé major temporalment o això durarà i serà una eina del dia a dia per vigilar-nos i controlar-nos? Creus que seran segures i que no s'utilitzés per a altres fins que no és a controlar la pandèmia?**

No sé, tècnicament, com son aquestes aplicacions. Si sé que, *si volen*, les poden fer respectuoses amb la privadesa de l'usuari i que suposin una violació "lleugera" de la nostra intimitat, no més enllà de saber si cal avisar-nos del risc de haver estat encomanats del COVID-19. No sé per a què més es poden fer servir, però això només ho podrà saber qui analitzi i entengui el codi d'aquestes aplicacions, per tant és *imprescindible* que aquestes aplicacions siguin de codi obert i es puguin auditar.

Tot i això, jo sóc dels que pensa que el problema principal que tenim entre mans ara mateix és acabar amb la pandèmia, i que qualsevol altra consideració passa a segon pla. Això inclou els drets i les llibertats que presumptament s'estan "violant" ara mateix. Si et fixes, hi ha gent que es queixa de la possible pèrdua de privadesa que aquestes aplicacions poden suposar i que tenen comptes de facebook i instagram.

Imagino que veus com d'absurd és això.

Òbviament, un cop es doni per acabada la pandèmia, la meva recomanació seria desinstal·lar aquestes aplicacions i fer un "hard reset" dels dispositius.

David Samper

Techical consultat en HP. Enginyer tècnic de telecomunicacions, especialitzat en sistemes de comunicació.

1. **¿Cómo experto en criptografía que aconsejas a los usuarios inexpertos en el tema para proteger su privacidad? ¿Crees que estos métodos son eficaces?**

Aunque ya he matizado que no soy experto en criptografía, en general, para proteger la privacidad lo más importante es la prudencia. Ante cualquier comunicación por email (o incluso telefónica), debemos plantearnos qué datos nos están solicitando y si realmente la empresa que los solicita nos haría “esas preguntas”. Nunca compartir un PIN, contraseña o código secreto por esos medios y si tengo recordatorios de contraseñas, usar herramientas para la encriptación de las mismas (el propio almacén de contraseñas de Google, Samsung o cualquier otro fabricante según el dispositivo al que nos conectemos). Nunca tener una nota o archivo de texto plano almacenado con esas contraseñas. A nivel general, la agencia española de protección de datos ofrece un listado de medidas: https://www.aepd.es/es/areas-de-actuacion/recomendaciones/medidas

2. **¿Cómo experto en Seguridad, podrías decir qué barreras de seguridad utilizan en tu empresa para que hackers o ciberdelincuentes no puedan acceder a la información de los usuarios?**

Aquí no voy a entrar en las herramientas concretas que usa nuestra empresa pero en general hay cortafuegos, filtros anti spam y otras medidas para tratar de evitar los ataques. También, como medida de protección existe una tendencia a migrar a servicios en la nube, entendidos como más seguros (ejemplo: Office365**)**

3. **¿Cómo se gestionan los datos de los usuarios?**

Lo más importante es informar de los riesgos y concienciar de la necesidad de ser prudentes. Para proteger los datos, es importante no usar discos externos o llaves usb no encriptadas y almacenar la información en las herramientas cloud corporativas (sharepoint, onedrive, googledrive u otros.

4. **¿Cómo profesional cómo protege su seguridad y privacidad ante ataques ciberdelincuentes?**

Aunque me repita, la máxima es la prudencia. Proteger la wifi de casa y no entrar en redes desconocidas o públicas. Es mucho mejor usar el 3/4G que una wifi desconocida. No se deben descargar aplicaciones dudosas o que no provengan de las tiendas oficiales (Google play, iTunes, etc.). Y además, pensar si la necesito antes de instalarla. (Ejemplo: hay una app para ver la ubicación en tiempo real de la estación espacial internacional y tengo curiosidad… ¿realmente lo necesito?**)**

5. **A causa del COVID-19 los Gobiernos han implementado rastreadores i/o aplicaciones para poder controlar la pandemia. ¿Qué medidas de seguridad debería de tener estas aplicaciones para poder proteger nuestra seguridad y privacidad?**

Para evitar malentendidos, lo más importante es que el consumidor sepa la fuente oficial para descargarla, que sea "segura por definición" y trate los datos de forma anónima en la medida de lo posible. No hay que olvidar que el estado también debe cumplir la ley de protección de datos.

Efraín Foglia
Dissenyador en interaccions digitals, investigador i docent. El seu treball es posiciona en la intersecció entre el disseny, l'activisme ciutadà i les tecnologies en xarxa.

1. **¿Cómo profesional que aconsejas a los usuarios inexpertos para proteger su seguridad? ¿Crees que estos métodos son eficaces? ¿Cómo protege su seguridad y privacidad?**

Lo primero que necesitamos es ser conscientes de que estamos en un problema bastante relevante, entonces es posible que el primer paso para resolver este problema, que es muy relevante y qué es muy complejo, es analizar, estudiar, informarse de cuáles son los verdaderos riesgos en temas de privacidad digital que son sumamente parecidos a los de la privacidad física como la conocemos. Nadie iría por ahí imprimiendo su foto, poniendo sus datos y pegándola en la calle simplemente porque sí, entonces nos tendremos que preguntar ¿y por qué lo hacemos digitalmente porque lo entregamos todo? Esto es fundamental porque si la gente no es consciente de lo que se está jugando es sumamente difícil realmente poder implementar algo relacionado a esto es como decirle a alguien que fuma, que deje de fumar. Por lo tanto aquí uno de los grandes problemas, que tenemos es con esa especie de incredulidad de que no pasa nada.

Muy parecido a muchos problemas sociales que tenemos como el alcoholismo, la violencia, como fue el SIDA, ahora mismo que del coronavirus de mucha gente que no encuentra su problemática hasta qué punto, hasta que le sucede algo, entonces estamos hablando que uno de los primeros consejos sería el de la prevención y poder acercarse cada vez más especialistas para que vean la gravedad de este asunto.
A partir de ahí se necesita documentar, por ejemplo, qué tipo de herramientas o de dispositivos son eficaces para palear esto. En principio no hay uno solo siempre te tienes que tomar en cuenta que en el Estado español hay más del 100% de penetración de los teléfonos, los Smartphone, por lo tanto imagínate resolver ese caso tomando en cuenta que hay muy pocas compañías de telecomunicaciones y marcas de teléfonos, que también nos están haciendo responsable de todas estas dinámicas. Entonces se necesita empezar gradualmente poco a poco desde antes mejor en cuanto edad para informarse, de qué tipo de cosas son las más peligrosas también tomen en cuenta que hay un montón de cosas que son opacas, que está sucediendo debajo de nuestros teléfonos por dentro y no lo sabemos.
A partir de aquí yo lo que empezaría es por buscar un especialista que nos expliquen en escuela de forma material en el aula, ¿cuáles son los problemas de privacidad? Por ejemplo con las grandes y mayoritarias redes quesería en Facebook, Instagram, WhatsApp y exactamente, qué tan frágil nos hace el hecho de estar en ellas. Seguramente la respuesta de mucha gente joven será: Vale, pero me vale la pena. Respondo porque yo tengo experiencia en talleres y a partir de ahí, aunque les digas todo lo malo que pasa algunos lo decidirán u otros no, pero tiene que ser gradual en un solo paso no se puede hacer. De alguna forma que se introdujera en las aulas en los estudios y en todo lugar, ya que el teléfono está muy presente e Internet también porque en los ordenadores dejar como constancia de que esto es un elemento vertebral, porque aparte es un elemento económico en la sociedad y que lo tenemos que subir tanto como las violencias de género, tanto como la comida chatarra, tanto como el racismo, etc. De hecho ese tipo de dispositivos como los teléfonos e Internet son capaces de catalizar en negativo todos los problemas y más he venido mencionando violencias en red, etc. Estamos hablando de algo que nos corresponde como sociedad y qué es verdaderamente serio.

2. **¿Cómo diseñador en interacciones digitales que métodos de seguridad implementan en tus diseños para proteger la privacidad y la seguridad de los usuarios? ¿Cómo lo gestionan principalmente los datos de carácter personal?**

Yo trabajo principalmente con plataformas que no son las mayoritarias, sino con plataformas basadas en el software libre que permiten la transparencia y hacer una gobernanza mucho más horizontal con la gente, por ejemplo, tenemos un proyecto que se llama la xarxa de ràdios comunitàries de Barcelona, que es un proyecto construido en comunidad y con desarrolladores bastante éticos y una de las principales ventajas es esta que podemos realmente garantizar mucho más, pero nunca al 100%, la privacidad y los datos de los usuarios. En las normas de uso nos hemos asesorado con abogados, con bufete abogados para poder hacer firmar a la gente y también responsabilizarnos de esta situación. Piensa que el uso de empresas más pequeñas o proyectos más pequeños que conozcas a quién lo hace te da mucha más confianza de cara a poder preguntar lo que sucede. ¿Qué pasa si te googleas en Instagram? ¿A quién le preguntas si hay un problema de datos y además que gobierna es capaz de realmente exigir a estas

empresas que nos las den? Entonces nosotros trabajamos a pequeña escala como muchos otros proyectos en Barcelona y en Cataluña en los que igual no son tan sofisticados como sus grandes, pero te permiten que esto esté en debate y te permiten protegerlo, entonces lo que yo hago es que me relaciono y diseño desde plataformas que sean garantistas con este sistema, por ejemplo, si usas un Gmail pues ya da igual todas las plataformas que tengas porque mismo Gmail ya te está siendo frágil, entonces tenemos que buscar distribuidoras de correos electrónicos que sean éticas y que sean cercanas de la ciudad y que hay tengan una trayectoria realmente interesante la protección de esto a nivel ético, como por ejemplo pangea.org, sería un ejemplo de lo que te estoy explicando.

3. **Debido a la Covidien-19 los Gobiernos han implementado rastreadores o aplicaciones para poder controlar la pandemia. ¿Qué medidas de seguridad debería tener estas aplicaciones para poder proteger nuestra seguridad y privacidad?**

Bueno, principalmente sabemos muy poco de estas implementaciones. Yo le he hecho un seguimiento de la que ha sacado el ministerio de Madrid, de todo esto y tardo muchísimo en mostrar el código fuente, ¿qué es? La estructura de cómo está escrito dicha app, por lo tanto nos causa mucha desconfianza el hecho de que desde el minuto cero no hayan publicado, cómo se construyó y que podamos ver si nos roban datos, a quien se los dan, etc. Entonces es muy muy difícil poder entender esto, de hecho hay muchas otras que no sabemos quién las hizo, entonces no sabemos cómo están usando nuestros datos y como se los están quedando, es un tema sumamente delicado, pero hasta ahora la app o el rastreador más importante que es, que me parece más radar COVID, que es el oficial de España, ha sido bastante opaca su publicación. Ahora ya lo liberaron el código, por lo tanto especialistas en todo esto pueden ver cómo está construido y pueden detectar problema, entonces tienes una mejor situación porque ya te pueden dar una verificación, pero tú imagínate toda la gente que no sabe de lo que estamos hablando aquí es código fuente, pues simplemente dar sus datos, usa el radar y está ofreciendo sus datos a quien sabe quién, ¿no? Es un tema sumamente delicado y los que trabajamos en esto lo vemos y no solamente eso, imagínate que realmente esta App es transparente y es justa, pero al pasar por servidores de grandes compañías de telecomunicaciones como garantizamos que nuestros datos no nos están revendiendo.

Me gustaría matizar en la app del COVID porque entramos en una paradoja muy grande yo un momento diría que no hay que usarla porque nos encontramos con el clásico dilema de sí salvando vidas a partir de esa app estaría justificado que nos robaron nuestros datos, ¿no? Que eso no tiene respuesta pregunta o si la tienes primero va la vida y luego los datos no sé qué priorizar cosas porque es muy difícil encontrar un balance por lo tanto de ninguna forma diría no, no, no se usen la app de radar COVID porque estamos sin problema más grave, que es la vida o la muerte de parte de la población de la infección, pero si hay que reflexionar en torno, a quién encuentra un dilema ético y moral y casi jurídico es muy importante, pero me da la impresión de que la prioridad en este caso es la vida, a diferencia de entrar en Instagram la diferencia es ser popular o molar, mostrar fotos, compartir, con qué roben mis datos, que estos ejemplos no son equiparables, pero si nos pueden demostrar en qué punto deberíamos quizás dejar de preocuparnos un poco o preocupándonos pero tenemos que tomar una acción directa con el caso del COVID a diferencia nuestra vida cotidiana donde vamos publicando todo. Eso

no significa que no seamos conscientes y exijamos al Gobierno que libere el código fuente para entender cómo funciona, pero sería también verdaderamente drástico decir no se usen porque sería casi como estar negando una medicinas, que las medicinas también las hacen las grandes farmacéuticas y no sabemos tampoco, tenemos el desconocimiento de cómo funcionan, pero sabemos que curan qué tal y tal es un problema mucho más grave que matizar eso para que no te dará la impresión de que estoy promoviendo que no se usen diferentes apps en relaciones a este tema, el COVID, es un problema sumamente complejo.

4. **¿Crees que nuestra privacidad está segura implementando métodos y barreras de seguridad o siempre habrá una brecha que nos exponga? ¿Cómo protege su privacidad?**

Bueno es parecido a medio repuesta de la uno. Bueno, imagínate que tú te quieres, o sea quieres protegerte conduciendo un auto, ¿no? Que son es un dispositivo de una tonelada y que va 90 km por hora, ¿no? Que no solamente te puedes matar si conduces mal, si no puedes matar a alguien más. Cuáles son las medidas de seguridad por un lado, puedes tener el auto más seguro, el más claro y el que tenga 1000 sensores, pero por otro lado si tú conduces ebrio o si tienes problemas de vistas pues se mezclan los factores. El auto no te va a arreglar eso, entonces es un problema 360°.
Es un problema por un lado de los dispositivos, pero por otro lado de Educación, de ética, de conocimiento y de entender que el tema de las TICs y de toda la cultura digital no solamente para los Gibs, sino que ahora todo el mundo está muy inmiscuido en este tipo de dinámica. Entonces necesitamos necesariamente tomarnos en serio y estudiar ponernos a tono de lo que está pasando y de la misma forma ver qué tipo de dispositivo usamos, que tan confiable. Como la gente antes de comprar algo de sus características de memoria, de los megapíxeles, de la cámara, etc. Pues nosotros tenemos que ver qué sistema operativo y podemos buscarlo en Google, es más fiable, cómo puedo tener la privacidad de mis hijos, si es que me tomo una foto que tengo que ser conscientes y quiere estar en Instagram lo que se implica de que estoy regalando mis imágenes y mis datos a Facebook, que básicamente es el dueño, entonces es un conocimiento cultural amplio en el cual nos tenemos que comprometer y no es solamente a partir de dispositivos tecnológicos, sino también del conocimiento y de la conciencia de cómo los estamos.

5. **¿Cómo mejoraría la seguridad y la privacidad para los usuarios de Internet?**

Es parecida a lo que te estoy explicando. Primero, tengo que ser consciente de los riesgos y hasta donde quiero optar, ¿no? Y a partir de ahí en la serie dispositivos ya creados que luchan por esto para mejorar estoy yo te recomendaría Fundación Mozilla, que es la diseñadora de Firefox el navegador tiene un montón de herramientas para poder proteger tu privacidad, hay por ejemplo un rastreador, un buscador, un dexador que se llama DuckDuckGo, que sale un patito y este es un reemplazo Google y este es muy interesante porque cuando tú buscas información ahí te dice quién te está queriendo robar información, entonces usando correo electrónico, usando calendario, redes de sociales, si tú buscas cuáles están montadas con

software libre y busca las opciones en Internet podrás encontrar varias te podría hacer una lista, pero en un año seguramente cambiaría. Lo importante es ver qué características tiene, por ejemplo los buscadores, ¿no? Que buscador me puede dar privacidad y no vender mis datos, etc. También compañía de teléfono, cuáles compañías de teléfono bloquean información de las luchas feministas, antirracistas, etc. Esto es importante, pero repito puede hacer una lista ahora, pero en un mes saldrán nuevas cosas o habría un cambio de modelo de teléfono y volver a cambiar lo importante es casi como cuando comes, ¿no? Ver si esa carne está hecha con producción ética, etc. O alomejor me tengo que hacer vegano, pero también ser vegano no es lo mismo un aguacate del Carrefour que no de km 0, etc.

Karma Peiró
Periodista especialitzada en las Tecnologies de la Informació i la Comunicació (TIC) des de 1995.

1. **Com gestionen les empreses i governs la informació dels usuaris i ciutadans? Creus que es pot millorar? Com?**

Entenc que per 'informació' et refereixes a dades personals.

No et puc respondre amb exactitud a la primera pregunta (massa general), perquè cada govern i cada empresa gestiona les dades dels clients/ciutadania de la manera que consideren.
Sí que es pot dir que des del 2018, tots (governs i empreses) ubicats a la UE tenen l'obligació de complir amb el Reglament General de Protecció de Dades (RGPD) (https://apdcat.gencat.cat/ca/documentacio/RGPD/), que per resumir-ho molt els obliga que demanin el consentiment (a clients/ciutadania) per tractar la informació personal.
Abans era al contrari: s'agafava i analitzaven les dades i si algú no estava conforme havia de reclamar.
També comporta obligacions de compliment més específiques, que pots veure aquí https://apdcat.gencat.cat/ca/documentacio/preguntes-frequents/

Sobre la 2a pregunta, crec que és bo que existeixi el RGPD perquè és una presa de consciència per part de les empreses/governs i de la ciutadania en general.
Ara, crec que encara falta temps perquè aquesta presa de consciència sigui real.
Sovint ens demanen el consentiment i aprovem a cegues, sense llegir les clàusules de privacitat (quines dades ens agafen i per a què?).
Sovint anem a un metge o entrem a un gimnàs i ens diuen: 'Firmi aquí, és per allò de les dades' i signem sense llegir el que diu el paper i ens quedem tan tranquils.

2. **La implementació de las Intel·ligències Artificials a la societat, com assistents de veu, implica una vulnerabilitat de la informació per part dels usuaris? Una transparència de la informació per part de les empreses que**

les gestionen? Com s'hauria de gestionar i quines barres de seguretat s'haurien d'implementar?

La implementació de la IA no necessàriament ha d'implicar una desprotecció o vulnerabilitat la informació dels clients/usuaris.

Depèn de com tingui regulats o controlats els aspectes ètics l'empresa fabricant o que dona el servei.

Però la tecnologia no és dolenta o perjudicial d'entrada. És l'ús que se'n faci d'ella el perjudicial.

Seria bo que les empreses fabricants o de serveis fossin transparents explicant quina mena d'informació/dades personals agafen dels usuaris amb l'ús d'aquell aparell intel·ligent.

Seria bo que els usuaris/clients reclaméssim, com a dret, ser informats de quin ús se'n fa, a quines empreses es passa (sempre diuen que 'a tercers' però sovint no se saben quins són aquests per temes de competència comercial o perquè simplement els acords es fan constantment i no informen cada dia d'un nou acord amb una empresa 'tercera' que compra les dades).

El mateix amb els governs, haurien de ser transparents en la implementació dels sistemes intel·ligents per oferir serveis públics i explicar quin ús fan de les dades que recullen.

Bé, sobre com s'hauria de gestionar, la Comissió Europea ha publicat en el darrer any molta documentació al respecte.

Des del Llibre Blanc de la IA, fins a les Directrius Ètiques per a una IA fiable. A més de moltes altres recomanacions sobre la Protecció de Dades quan s'implementa la IA. (pots cercar a Google els enllaços).

3. **Creus que la nostra privacitat està segura implementant mètodes i barreres de seguretat o sempre hi haurà una bretxa que ens exposi? Com protegeix la seva privacitat?**

Les dues coses.

Crec que es necessària reglamentació que obligui a protegir les nostres dades.

També crec que 100% segura mai estarà perquè sempre hi ha mecanismes/maneres perquè estiguin exposades.

Mira Facebook i l'escàndol de Cambridge Analytica.

(https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal)

I cada dia hi ha un munt de robatoris de dades personals de grans empreses, multinacionals, que no ho diuen o se sap poc d'elles.(Aquí tens una visualització dels hackejos de dades més grans del món per anys https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/).

D'altra banda, per sort qui vol protegir de veritat la seva informació, i deixar poc rastre dels seus moviments, també pot fer-lo (amb molt d'esforç) amb eines que ho possibiliten.

4. **Com creus que serà la nova normalitat amb el tema dels rastrejadors i / o aplicacions per detectar i controlar la COVID-19? Serà una invasió a la nostra privacitat per a un bé major temporalment o això durarà i serà una eina del dia a dia per vigilar-nos i controlar-nos? Creus que seran segures i que no s'utilitzés per a altres fins que no és a controlar la pandèmia?**

Està per veure.

L'app del govern espanyol anunciada Radar Covid-19, encara no està habilitada a tota Espanya. A Catalunya, per exemple, a data d'avui encara no està operativa.

Han promès que no agafen dades personals, i que no perdrem privacitat.

Seria bo dues coses:

1. Que deixessin clar (des del govern) fins a quan ens seguiran el rastre amb aquesta app (no una data, però si sota quines condicions. Però quan ja la quota de contagis baixi a tal nivell)

2. Que s'alliberés el codi de l'app, perquè la comunitat científica i experts en desenvolupament tecnològic puguin contrastar-la, auditar-la i detectar possibles errors, a més de comprovar que el govern espanyol no agafa dades personals tal i com ha promès. Demanat per + de 200 científics (https://www.elconfidencial.com/tecnologia/2020-09-05/radar-covid-dp3t-sedia-apps-rastreo-contactos_2736168/).

5. **Creus que la informació dels usuaris és un negoci que benefici a les empreses que les gestionen? Per què? Com creus que ho fan? Legalment o il·legalment?**

Aquí et remeto a l'Informe en el que vaig col·laborar i presentar aquest any, amb l'Autoritat Catalana de Protecció de Dades, on soc co-autora:

"Intel·ligència Artificial. Decisions automatitzades a Catalunya".

https://apdcat.gencat.cat/web/.content/04-actualitat/noticies/documents/INFORME-INTELLIGENCIA-ARTIFICIAL-FINAL-WEB-OK.pdf

Ves a la pàg. 60, apartat • Les dades de comportament, les més valuoses*

Crec que respon al que preguntes..

El que explico a l'informe és legal.

Però com tot... el que va fer Facebook amb Cambridge Analytica era il·legal. I...??

Continua amb milions d'usuaris. Per què?

6. Com milloraria la seguretat i la privacitat pels usuaris d'Internet?

Amb molta ètica, responsabilitat de les empreses i governs, i molta transparència.

És la única manera que veig que es pot continuar confiant en la tecnologia.

8. Conclusions

Per finalitzar, puc dir que he pogut assolir els objectius que tenia l'inici del treball. He pogut identificar com les empreses gestionen les dades dels usuaris, si s'utilitzen sense el nostre consentiment i ens perjudica, si la informació personal dels usuaris és un negoci i les mesures de seguretat que implanten. També referenciar els mètodes recomanats per gestionar i millorar la nostra privacitat al telèfon mòbil. He entrevistat un a advocat especialitzat en protecció de dades i drets digitals. Un activista amb coneixements de seguretat i privacitat, a un *Techical consultat* en HP enginyer tècnic de telecomunicacions, especialitzat en sistemes de comunicació. Un dissenyador en interaccions digitals, investigador i docent, i una Periodista especialitzada en les Tecnologies de la Informació i la Comunicació.

He pogut arribar a la conclusió de què els usuaris estan protegits per la política de privacitat, tot el que declara el Reglament General de Protecció de Dades de la UE i la Llei Orgànica de Protecció de Dades i Garantia de Drets Digitals. Les empreses estan obligades a posar mesures de seguretat per protegir la mateixa empresa d'atacs, la privacitat dels seus usuaris i ser transparents en la seva gestió. No obstant com afirma Josep Cañabate en les entrevistes << *en moltes ocasions o no es compleix amb el que es diu a les polítiques, i es fa un ús de les dades no conforme amb la normativa, o les polítiques no estan ben realitzades* >>. Confirmant que és fàcil violar aquesta política i utilitzen la informació pel seu propi benefici.

Això deixa clar que lleis que protegeixen els usuaris són insuficients perquè les conseqüències d'infringir les normes, com per exemple Google, encara que les multes siguin multimilionàries, com afirma Josep Cañabate, no són suficients en comparació amb el negoci d'aprofitar les dades dels seus clients, sempre al límit de la legalitat. La solució que els experts estan anunciant és utilitzar sistemes que respectin la privacitat de les dades, com xifrats, i responsabilitat per part de l'empresa, però sobre tots dels governs donant una transparència en la seva gestió.

Nosaltres com usuaris i part de la ciutadania hem de lluitar pels nostres drets. No obstant això en aquests moments és difícil deixar a banda tots els aparells tecnològics que exposen la nostra privacitat perquè són part de la nostra vida. Encara que sabem que no s'estan utilitzant correctament les nostres dades, falta consciència del dret a la privacitat i la importància que té. Per altra banda quan utilitzem el nostre telèfon mòbil navegant per internet implementem mètodes per gestionar i millorar la privacitat i la seguretat als nostres telèfons mòbil i Internet, mencionat en el treball, però hem de saber que sempre hi haurà una bretxa que ens exposi, com

afirmen les persones entrevistades Jordi Delgado, Efraín Foglia i Karma Peiró. Això confirma la meva hipòtesi: utilitzar el mòbil implica la teva vulnerabilitat de la privacitat.

La solució d'això seria començar a conscienciar a la població del valor de les nostres dades i privacitat, que cap de nosaltres som un producte i això es fa a partir de l'educació i de l'ètica. Ensenyar a la gent un bon ús d'Internet i del telèfon mòbil. Ja que com diu Karma Peiró en l'entrevista << *la tecnologia no és dolenta o perjudicial d'entrada. És l'ús que se'n faci d'ella el perjudicial*>>.

9. Agraïments

Voldria agrair en primer lloc al meu tutor del treball de recerca, Jordi Flavià, per escoltar-me, guiar-me, assessorar-me per fer el treball. També per la seva paciència perquè aquest any amb el tema de la COVID-19 no ha sigut fàcil i donar-me ànims per continuar fent el treball. En segon lloc a Laia Sánchez responsable del Col·laboratori i el Social Media Lab del citilab de Cornellà de Llobregat per donar-me consell pel meu treball, els seus suggeriments, per aclarir els meus dubtes, per suggerir-me persones amb el perfil per poder fer-li les entrevistes i dedicar el seu temps per ajudar-me.

Agrair a Josep Cañabate Pérez, Jordi Delgado, David Samper, Efraín Foglia i Karma Peiró per accedir a fer les entrevistes via Gmail, semipresencials per les circumstàncies de la pandèmia i dedicar el seu temps per contestar les preguntes.

També, vull donar les gràcies a la meva cosina, per aconseguir fer una entrevista a un dels professionals d'aquest tema.

Moltes Gràcies.

10. Llistat de referència

González, Y. (2020). *Privacidad digital - ¿Qué es? ¿Características? Ventajas y desventajas*. Grupo Atico34. Recuperat el 3 de juliol de 2020, des de https://protecciondatos-lopd.com/empresas/privacidad-digital/

Agencia Española de Protección de Datos. (2018). *Guia de protección de datos y prevención de delitos* [Ebook]. Recuperat de https://www.aepd.es/sites/default/files/2019-09/guia-proteccion-datos-y-prevencion-de-delitos.pdf

Agentes móviles. (2020). Recuperat el 3 de juliol de 2020, des de https://www.informatica.us.es/~ramon/tesis/agentes/moviles.html

Big Data: cómo afecta a los usuarios. (2016). Recuperat l'1 de juliol de 2020 https://www.osi.es/es/actualidad/blog/2016/06/14/big-data-como-afecta-los-usuarios

BOE.es - Documento DOUE-L-2016-80807. Boe.es. (2016). Recuperat el 3 de juliol de 2020, des de https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Burgueño, P. (2014). Primeras multas por vulnerar la Ley de Cookies. Explicamos el caso. Abanlex. Recuperat el 29 de juliol de 2020, des de https://www.abanlex.com/2014/01/primeras-multas-por-vulnerar-la-ley-de-cookies-explicamos-el-caso/

Business insider España. (2019). Más de 1.300 apps te siguen espiando el móvil aunque no les hayas dado permiso, y entre las implicadas están Samsung, Baidu o Disney. Recuperat el 3 de juliol de 2020, des de https://www.businessinsider.es/comprueba-1300-apps-espian-android-aunque-no-tengan-permisos-452301

¿Cómo podemos sobrevivir al mundo sin cookies que plantea Google?. (2020). Recuperat el 29 de juliol de 2020, des de https://tecnohotelnews.com/2020/02/27/que-pasara-cuando-google-elimine-las-cookies-de-terceros/

Cómo saber qué apps te espían por el micro del móvil: Cómo desactivarlo. (2020). Recuperat el 3 de juliol de 2020, des de https://as.com/meristation/2019/06/12/betech/1560374083_168548.html

Comunicado de la AEPD sobre apps y webs de autoevaluación del Coronavirus | AEPD. (2020). Recuperat el 9 de juliol de 2020, des de https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad

¡Conexión gratis a la vista! ¿Conecto mi móvil?. (2019). Recuperat el 3 de juliol de 2020, des de https://www.osi.es/es/actualidad/blog/2019/05/02/conexion-gratis-la-vista-conecto-mi-movil

Cookies en una web: así afectan a la privacidad. Recuperat el 3 de juliol de 2020, des de https://www.redeszone.net/tutoriales/seguridad/cookies-web-afectar-privacidad/

Day, M., Turner, G., & Drozdiak, N. (2019). Amazon Workers Are Listening to What You Tell Alexa. *Bloomberg*. Recuperat el 9 de juliol de 2020, des de https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio

Disseny de la portada Computer Grey. Recuperat el 20 d'octubre de 2020, des de https://descargarportadas.com/

Ejerce tus derechos | AEPD. AEPD. (2019). Recuperat el 3 de juliol de 2020, des de https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos

Entre cookies y privacidad. (2018). Recuperat el 29 de juliol de 2020, des de https://www.osi.es/es/actualidad/blog/2018/07/18/entre-cookies-y-privacidad

Garrigues, C., Robles, S., Borrell, J., & Navarro-Arribas, G. (2010). *Promoting the development of secure mobile agent applications* (Licenciatura). aEstudis d'Informàtica, Multimèdia i

Telecomunicacions, Universitat Oberta de Catalunya, Rambla del Poblenou 156, 08018 Barcelona, Spain bDept. d'Enginyeria de la Informació i de les Comunicacions, Edifici Q (ETSE), Universitat Autònoma de Barcelona, 08193 Bellaterra, Spain cIIIA, Institut d'Investigació en Intelligència Artificial, CSIC, Consejo Superior de Investigaciones Científicas, 08193 Bellaterra, Spain.

Google - My Activity. Myactivity.google.com. Recuperat el 9 de juliol de 2020, des de https://myactivity.google.com/activitycontrols/webandapp?promo=vaa&pli=1

Iglesia, E. (2020). Criptografía, en clave Ciberseguridad. Recuperat el 3 de juliol de 2020, des de https://www.campusciberseguridad.com/blog/item/91-criptografia-en-clave-ciberseguridad

Hernández, Á., fotos), M., Mcloughlin, M., & Mcloughlin, M. (2019). *Ojo con lo que dices al altavoz de Amazon: hay gente escuchando las conversaciones*. El Confidencial. Recuperat el 5 de juliol de 2020, des de https://www.elconfidencial.com/tecnologia/2019-04-11/amazon-altavoz-echo-escucha-espia-empleados_1936706/

La identidad digital,huella digital, privacidad digital,ciberbullying y sexting. (2020). Recuperat el 3 de juliol de 2020, des de https://sites.google.com/site/trabajoticbyjmgx/home/la-huella-digital/la-privacidad-digital

Más información sobre las cookies | La Huella Digital. (2020). Recuperat el 3 de juliol de 2020, des de http://www.lahuelladigital.com/mas-informacion-sobre-las-cookies/#

Notificación de brechas de seguridad de los datos personales durante el estado de alarma | AEPD. (2020). Recuperat el 9 de juliol de 2020, des de https://www.aepd.es/es/prensa-y-comunicacion/blog/notificacion-de-brechas-de-seguridad-de-los-datos-personales-durante-el

Otero, C. (2018). Tu móvil no te espía por el micro, pero sí puede grabarte por la cámara. *As*. Recuperat el 3 de juliol de 2020, des de https://as.com/meristation/2018/07/04/betech/1530713687_227709.html

Otero, C. (2019). Cómo saber qué apps te espían por el micro del móvil: Cómo desactivarlo. *As*. Recuperat el 3 de juliol de 2020, des de https://as.com/meristation/2019/06/12/betech/1560374083_168548.html

Pérez, D. (2014). Primera multa por el uso de 'cookies' en el comercio y la publicidad online. Recuperat el 29 de juliol de 2020, des de https://cincodias.elpais.com/cincodias/2014/01/27/empresas/1390817773_540852.html

Política de privacidad | Uso de cookies y RGPD. (2020). Recuperat el 3 de juliol de 2020, des de https://www.cookiebot.com/es/politica-de-privacidad-para-mi-web/?gclid=Cj0KCQjwudb3BRC9ARIsAEa-vUsnnJQotdo64sWqdIyfTtHQ50JJAtcaXvpL5ng1xCWTdU1fULXZ2k8aAmC0EALw_wcB

Política de Privacidad. (2020). Recuperat el 3 de juliol de 2020, des de http://www.eees.es/es/opciones-politica-privacidad

Protección de Datos: Guía para el Ciudadano. (2019). [Ebook]. Recuperat de https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf

Qué es la navegación en modo incógnito de mi navegador. (2020). Recuperat el 3 de juliol de 2020, des de https://www.zitelia.com/que-es-navegar-modo-incognito/#:~:text=El%20modo%20inc%C3%B3gnito%2C%20ventana%20privada,guarda%20ning%C3%BAn%20tipo%20de%20informaci%C3%B3n

¿Qué pasa cuando aceptamos las cookies? - IT Lab Applications. (2020). Recuperat el 3 de juliol de 2020, des de http://www.grupoepositlab.com/aceptar-las-cookies/

Reardon, J., Feal, Á., Wijesekera, P., Elazari Bar On, A., Vallina-Rodriguez, N., & Egelman, S. (2019). *50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System* [Ebook]. Recuperat de

https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_serge_egelman.pdf

RGPD, G. (2020). ¿Qué es y cómo funciona la política de privacidad? | Grupo Adaptalia España. Recuperat el 3 de juliol de 2020, des de https://www.grupoadaptalia.es/blog/articulos-explicativos-legales/que-es-y-como-funciona-la-politica-de-privacidad/

Santana Vega, C. (2018). □ *¿TE ESCUCHA Google a través del móvil? - Análisis y Experimento* [Video]. Recuperat de https://www.youtube.com/watch?v=-BG6WZcRJCg&t=348s

Seguridad en Big Data, privacidad y protección de datos - IIC. (2016). Recuperat l'1 de juliol de 2020, des de https://www.iic.uam.es/innovacion/seguridad-big-data/

TEAM, A. (2019). Qué es la huella digital y cuál es su importancia. Recuperat el 29 de juliol de 2020, des de https://www.ambit-bst.com/blog/huella-digital-importancia

Véliz, C. (2020). Tribuna | La privacidad en tiempos de coronavirus. Recuperat el 9 de juliol de 2020, des de https://elpais.com/elpais/2020/03/23/opinion/1584954197_094726.html