L’ESPIA DARRERE DE LA PANTALLA

Joel López Borrallo

2n de Batxillerat B

2025/2026

Iona Colom Diego

Institut Ramon Berenguer IV

Abstracto:
Debido al gran crecimiento de internet en los últimos años, la mayoría de páginas se han visto obligadas a aumentar su moderación, recopilando datos de sus usuarios, dificultando el anonimato de estos. El objetivo principal es analizar cuáles son los métodos principales de recopilación de datos (sean legales o no) y con que fines se utilizan estos datos. Para ello se ha investigado acerca de las políticas de privacidad de distintas webs y sobre algunos de los métodos ilegales de recopilación de información. Como parte práctica se ha programado un sitio web que funciona como simulación de lo que le ocurriría a un usuario al toparse con una página maliciosa.
Palabras clave: política de privacidad, recopilación de datos, página web, malware, programación.

Abstract:
Due to the rapid growth of the internet in recent years, most websites have been forced to increase their moderation practices, collecting user data and making it more difficult for users to remain anonymous. The main objective is to analyse the primary methods of data collection (both legal and illegal) and the purposes for which this data is used. To this end, research was conducted on the privacy policies of various websites and on some illegal data collection methods. As the practical project, a website was programmed to simulate what would happen to a user upon encountering a malicious page.
Keywords: privacy policy, data collection, website, malware, programming.

ÍNDEX

INTRODUCCIÓ

A l'hora de navegar per internet mai ens preguntem quines són les dades que estem compartint, alguns fins i tot no saben que estan compartint informació. És per això que és de vital importància conèixer de quina manera ens exposem en visitar segons quines webs i com ens podem afectar la recopilació d'aquesta informació.

Des que en tinc memòria he conegut usuaris que naveguen per la xarxa sense cap preocupació, exposant informació seva a cents de llocs web sense molestar-se en pensar si poden fer servir aquestes dades per fins il·legítims. És així com arribem a la hipòtesi d'aquest treball: És possible que hi hagi diferents pàgines web que ens robin una quantitat d'informació excessiva amb fins qüestionables.

Per tant, l'objectiu d'aquest treball no és altre que el de compartir quina és la informació que recopilen diferents webs. Ja siguin amb mètodes convencionals i legals que s'han d'especificar a les polítiques de privacitat o amb mètodes fraudulents. A més a més, en aquest treball també intentaré advertir dels riscos que suposen compartir aquestes dades.

En aquesta memòria trobareu primerament la part teòrica, on parlo de la política de privadesa de diferents webs i d'uns quants mètodes il·legítims de recopilació de dades, i a continuació trobareu la part pràctica on faig una petita demostració de com algunes webs poden introduir arxius maliciosos

La metodologia emprada a la part teòrica es basa en cerca bibliogràfica, documentació i redacció. Mentre que la metodologia de la part pràctica es basarà en la programació.

PART TEÒRICA

1. LA IMPORTÀNCIA DE LES NOSTRES DADES

A l'hora de navegar per internet estem autoritzant que centes de les nostres dades siguin recopilades. Però, quines dades recopilen exactament i per què les volen?
En aquest apartat donarem una ullada a les polítiques de privadesa de diferents institucions per així poder veure si les dades recopilades són veritablement importants o si la informació recopilada pot fer-se servir en fins que comprometen la nostra privacitat o anonimat.

1.1. Contextualització: Què és una política de privadesa?

La política de privadesa és un document que les empreses faciliten als usuaris amb la premissa d'informar quina informació és recopilada i amb quins fins és utilitzada. La informació recopilada i l'ús d'aquesta es basa en la legislació dels diferents estats, és per això que la política pot variar, en alguns països no són tan estrictes respecte a quines dades són usades i permeten a les empreses més llibertats.

En Espanya les polítiques de privadesa tenen com a base jurídica lleis com la Llei Orgànica de Protecció de Dades Personals i garantia dels drets digitals o el Reglament General de Protecció de Dades de la Unió Europea. Lleis que tracten sobre com ha de ser regulada la informació dels ciutadans per protegir la seva privacitat a l'hora de navegar per la xarxa.

1.2. Polítiques de privadesa als navegadors

La majoria dels navegadors ens demanen accés a les nostres dades per contribuir al desenvolupament de l'eina, habilitant funcions com recomanar les webs més segures o més útils. Però això no impedeix que hi hagi mesures invasives. A continuació es troba una anàlisi de les polítiques de privacitat de diferents navegadors.

Aquí els navegadors analitzats i perquè han estat escollits:

- **Google Chrome:** És actualment el cercador més gran i és gairebé impossible no fer servir cap dels seus serveis si fas servir internet molt sovint.
- **Tor:** Cercador destacat per la seva extrema privacitat i poca moderació.

1.2.1. Política de privadesa de Google

Google és una de les empreses més grans del món, per tant, no ens hauria d'estranyar la seva quantitat de productes i plataformes. Amb la seva quantitat absurda de serveis és gairebé impossible no fer-ne servir cap, de manera que haurem d'acceptar les polítiques de privacitat de la companyia, però, és ben sabut que la majoria d'usuaris no es paren a llegir-la. Així que a continuació es troba un resum del document oficial de la política de privadesa de Google (https://policies.google.com/privacy?hl=ca), presentant en termes generals quina informació recopila i per què la utilitzen.

Google recopila la següent informació:

- **Els termes cercats:** Google guarda els termes cercats per brindar una experiència més "personalitzada", adreçant webs o anuncis relacionats als termes que cerquen els usuaris.

- **Els vídeos reproduïts:** Igual que amb els termes de cerca, serveis com YouTube recopilen dades dels vídeos que reprodueixen els usuaris per tal de recomanar més vídeos similars i publicitat relacionada.

- **Les visualitzacions de contingut i d'anuncis i les maneres com s'hi interacciona**: Recopilen informació sobre les visualitzacions d'anuncis i les maneres com s'hi interacciona per poder proporcionar als anunciants informes agregats que els indiquen, entre d'altres, si han publicat el seu anunci en una pàgina i si és probable que un usuari l'hagi vist. També poden mesurar altres interaccions, com ara la manera en què es desplaça el ratolí sobre un anunci o si s'ha interaccionat amb la pàgina en què es mostra.

- **Informació de veu i d'àudio**: És possible triar si es vol que Google desi una gravació d'àudio al Compte de Google de l'usuari quan s'interaccioni amb la Cerca de Google, amb l'Assistent i amb Maps. Quan el dispositiu detecta una ordre d'activació d'àudio, com ara "Hey Google", Google grava la veu i l'àudio més uns quants segons abans de l'activació.
  Segons Google (https://support.google.com/websearch/answer/6030020?hl=ca#zippy=%2Chow-audio-recordings-are-saved%2Cproc%C3%A9s-de-revisi%C3%B3-d%C3%A0udio), els arxius d'àudio emmagatzemats als servidors es fan servir per millorar les capacitats de la tecnologia de reconeixement d'àudio. A més a més, no està activada per defecte i no és obligatori fer-lo per utilitzar l'assistent. També si et preocupa saber que has compartit exactament pots revisar-lo a l'historial.

- **Les compres realitzades:** Poden fer servir aquesta informació per verificar la identitat de l'usuari i que està autoritzat a comprar el producte. En cas que no hi hagin prou dades per continuar amb la compra, aquestes seran demanades, inhabilitant-te l'opció de compra si no és compartida aquesta informació.

- **Els usuaris contactats:** Per exemple a serveis com Gmail, Google Voice (un servei de trucades) o Google Meet poden recollir dades com el número de telèfon de l'emissor i el receptor, els números de desviació de trucades, les adreces electròniques del remitent i del destinatari, l'hora i la data de les trucades i missatges, la durada de les trucades, informació d'encaminament, i els tipus i volums de trucades i missatges.

  També val la pena comentar que, encara que no sigui sobre el navegador en si, l'aplicació de "contactes" i "trucades" pertanyen a Google[1], per tant, tenen accés als teus contactes i a la informació (opcional)[2] que comparteixes d'ells.

[1] El nom de les APK assenyalen el seu propietari: https://drive.google.com/file/d/19i8rjaKrhAG0ZN5ZkEEofdkOECo8f9ej/view?usp=drive_link (captura de la meva autoria).
[2] Es pot proporcionar informació com l'adreça del contacte o la seva data de naixement: https://drive.google.com/file/d/1YN1dNtfBVM_4nY5jglwrfKLeO2HwCCWK/view?usp=sharing (captura de la meva autoria).

- **L’activitat en llocs web i aplicacions de tercers utilitzen els serveis de Google:** Els llocs web i les aplicacions que integren serveis de Google, com anuncis i analítica, comparteixen la seva informació. Aquesta informació es recull independentment del navegador o del mode de navegador que s’utilitzi. Per exemple, en visitar un lloc web que té implementats serveis publicitaris com AdSense, que inclou eines d'anàlisi com Google Analytics o que té inserit contingut de vídeo de YouTube, el navegador web envia automàticament determinades dades a Google. Això inclou l'URL de la pàgina consultada i l'adreça IP de l’usuari. Es pot utilitzar l'adreça IP, per exemple, per identificar la ubicació general d’un usuari, per mesurar l'eficàcia dels anuncis i, en funció de la configuració, per millorar la rellevància dels anuncis visualitzats.

  És important mencionar que fer servir el mode d'incògnit a Chrome o altres modes de navegació privada no impedeix que es recullin dades a l’hora de visitar llocs web que utilitzen els serveis de Google.

- **L'historial de navegació de Chrome sincronitzat amb el compte de Google:** L’historial és, essencialment, una eina per l’usuari, serveix, per exemple, per trobar una pàgina en la qual has estat, però no recordes el nom.

1.2.1.1. Conclusió sobre Google (i Chrome)

Google és una empresa revolucionària que ha canviat la vida de tothom. Poder accedir a gairebé tot el contingut del món tan còmodament és una proesa.

Si bé és cert que Google recopila molta informació la gran majoria no deixa de ser per temes de comoditat. L’única cosa que potser incòmoda a més d’un és que certa part de la informació és utilitzada per adreçar-te publicitat, i si bé afavoreix el consumisme desmesurat, Google no deixa de ser una empresa i ha de cercar com monetitzar els seus serveis gratuïts.

En conclusió, Chrome és un cercador molt còmode i funcional. És veritat que molta informació és recopilada amb fins lucratius, però no és pas informació personal que et pugui comprometre.

1.2.2. Què és Tor?

Tor Browser és un navegador que utilitza l'encaminament onion, un sistema que va començar el seu desenvolupament als anys noranta. Aquest sistema d'encaminament té la peculiaritat de crear connexions d'internet que no revelen qui parla amb qui, ni tan sols a algú que supervisa la xarxa. Això s'aconsegueix encriptant i diversificant la informació en diferents nodes.

És a dir, normalment utilitzem sistemes d'encaminament directe, vol dir que quan vols visitar un lloc web aquesta informació va de l'ordinador de l'usuari al seu encaminador, de l'encaminador als encaminadors del seu proveïdor d'Internet (ISP) i finalment als servidors de la web. El desavantatge que representa aquest mètode de connexió és que qualsevol persona que vigili la xarxa podrà identificar l'usuari.

És aquí on entra l'encaminador onion, un sistema el qual envia la informació encriptada a diferents nodes aleatoris els quals reben aquesta informació amb les instruccions de com fer-les arribar fins al seu destí. O dit d'una altra manera, utilitzant un xifratge asimètric, l'emissor (que anomenarem Alice) xifra el missatge per capes (com una ceba). El primer que farà és xifrar el missatge amb la clau pública de l'últim node de la llista, perquè només ell el pugui desxifrar. A més, xifra i inclou les instruccions per a arribar al destí, que és el receptor (Bob). Tot aquest paquet es xifra de nou afegint-li les instruccions per a arribar a l'últim node de la llista amb la finalitat que només aquest pugui desxifrar el paquet i que acabi arribant al node receptor.

Fig. 1.1. Esquema de xifrat asimètric.
Extret de: *Geeky Theory*.
https://geekytheory.com/que-es-y-como-funciona-la-red-tor/

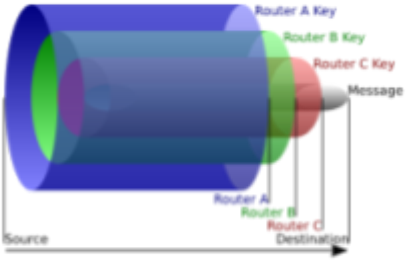

Fig. 1.2. Esquema de xifrat asimètric.
Extret de: Geeky Theory.
https://geekytheory.com/que-es-y-como-funciona-la-red-tor/

1.2.2.1. Política de privadesa de Tor

Una vegada vist què és Tor i com funciona, falta comprovar si realment amb totes aquestes mesures s'aconsegueix plena privacitat. Comprovem la política de privadesa de Tor Project. https://support.torproject.org/es/tbb/privacy-policy/.

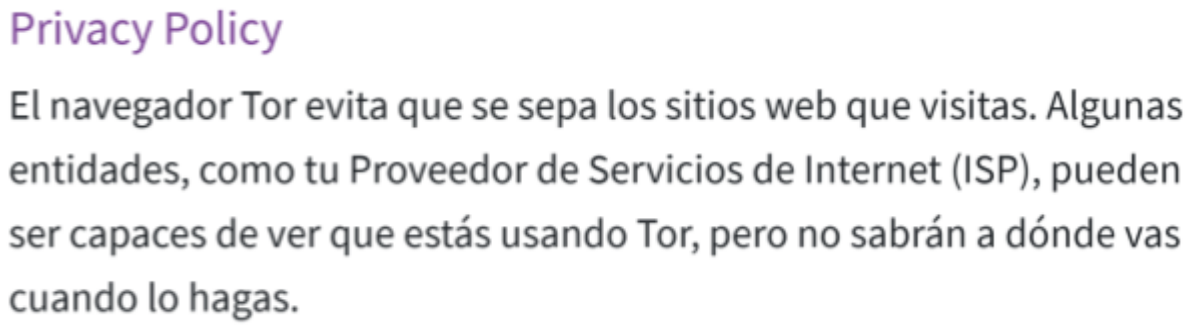

Fig. 1.3. Captura pressa de Tor Browser Privacy Policy. https://support.torproject.org/es/tbb/privacy-policy/

La política de privadesa no profunditza en quins moments es pot comprometre la privacitat, però a la mateixa pàgina Tor Project. support.torproject.org hi ha diferents apartats en els quals es mencionen situacions en què el cercador pot fracassar en l'intent d'anonimat.

Aquestes situacions són les següents:

- En **fer servir Tor amb un altre cercador** es poden produir filtracions no desitjades.
- **Utilitzar BitTorrent** (una eina d'intercanvi d'arxius de gran mida) sobre Tor pot comprometre la privacitat de l'usuari, ja que es realitzen connexions directes encara que es configuri per utilitzar Tor. Per un servei similar, però més anònim, Tor recomana OnionShare una eina d'intercanvi d'arxius que usa els serveis onion del navegador.
- En **completar un formulari web** l'usuari ja no és anònim per a la pàgina que està visitant, menys encara si proporciona altra informació personal.
- **Visitant pàgines que no fan servir el xifratge HTTPS.** Tor xifra el trànsit dins de la xarxa Tor, però el xifratge del trànsit al lloc web de destí final depèn d'aquest lloc web. Per garantir més privacitat Tor inclou una eina que força el xifratge HTTPS a les pàgines que ho admetin.
- **Obrint documents** (DOC o PDF) **descarregats a través de Tor mentre s'està en línia**, ja que els documents poden contenir recursos d'internet que l'eina que obre el fitxer descarregarà sense utilitzar Tor, revelant així la IP

sense cap mena de xifratge, per evitar-ho es pot obrir l'arxiu amb un ordinador desconnectat d'internet.

- El navegador oculta l'usuari dels llocs web que es visiten, però **mostra que es fa servir Tor**, si això suposa un problema es pot fer servir Tor com a pont perquè no sigui tan fàcil de detectar, però s'ha de tindre en compte que pot alentir la connexió[3].

1.2.2.2. Conclusió sobre Tor

Tor és un navegador que no defrauda quant a privadesa, però és normal que hi hagi vegades que fracassa pel que fa a la comoditat.

Molta de la informació que recopila Google tenen com a funció principal garantir el benestar de l'usuari. Informació com l'idioma, les contrasenyes guardades o l'historial de navegació són eines pensades perquè l'usuari les faci servir, encara que això porta com a conseqüència compartir part de la seva informació tant al cercador com a un possible espia. Pot passar que amb la manca de privadesa algú extern pugui aconseguir informació personal (com contrasenyes o adreces), però si no es visita cap pàgina poc fiable i s'administren les contrasenyes de la manera correcta (per exemple, no fent servir sempre la mateixa contrasenya, que sigui complexa barrejant nombres i lletres minúscules i majúscules i comprova la fiabilitat de les pàgines on introdueixes aquestes dades) no hi hauria cap problema. Llavors, què és exactament el que volen ocultar els usuaris de Tor? En llegir quines són les situacions que comprometen l'anonimat fan especial èmfasi en el fet d'intentar ocultar els llocs web visitats. És a dir, es vol ocultar la visita de llocs web amb contingut il·lícit.

L'anonimat que brinda Tor ha estat aprofitat per milers de ciberdelinqüents que utilitzen el cercador per ingressar a l'anomenada internet fosca, part de l'internet inaccessible pels cercadors habituals (internet profunda o deep web).

Aquesta part d'internet és censurada pels altres cercadors, però Tor et dona total llibertat a internet, cosa la qual et permet accedir a aquestes webs on es pot trobar material il·lícit (venda de substàncies o armes sense llicència són exemples del que podem trobar[4]). Aquestes webs solen ser freqüentades per ciberdelinqüents que

[3] Tor Project. (2025, juliol). *Using Bridges*. https://tb-manual.torproject.org/bridges/
[4] Lisa Institute. (2025). *Dark Web: riesgos, contenidos y cómo acceder.* https://www.lisainstitute.com/blogs/blog/dark-web-riesgos-contenidos-como-acceder

realitzen atacs directes a altres usuaris, atacs que són efectius encara que s'utilitzi Tor, per tant, fer servir el navegador d'aquesta manera no és gens aconsellable.

En conclusió, Tor és un cercador que brinda molta llibertat a l'usuari, però aquesta llibertat s'ha de fer servir responsablement. L'anonimat que Tor aporta pot usar-se amb fins productius i no nocius, com per exemple amb fins d'investigació, podent accedir a webs que normalment passarien desapercebudes o serien censurades, cosa que permet que usuaris de països amb polítiques repressives puguin accedir a reportatges o altra informació que el seu govern oculta amb fins de controlar i manipular la població.

1.3. Polítiques de privadesa a les xarxes socials

Una gran quantitat del temps que inverteixen els usuaris en internet va destinat a les xarxes socials. I és normal, com éssers humans necessitem relacionar-nos i expressar-nos, i que millor lloc que a les xarxes on l'abast és molt més massiu.

Tot i això, com ja hem vist en analitzar els cercadors web, l'internet no destaca per garantir el teu anonimat.
Això no suposa un problema a les xarxes, el que vol l'usuari és que sàpiguen d'ell. És aquest qui posa la barrera de quanta informació vol compartir amb altres usuaris o amb l'aplicació, però per garantir que és així analitzem les polítiques de les següents xarxes socials:

- **Instagram:** Xarxa social amb milions d'usuaris arreu del món que pertany a Meta Platforms, Inc. (abans Facebook, Inc.). És pertinent parlar d'un producte de Meta pel fet que ofereixen altres plataformes populars com Facebook o WhatsApp les quals comparteixen similituds amb Instagram a les seves polítiques de privadesa.

- **TikTok:** Una altra xarxa social molt popular pertanyent a una empresa xinesa anomenada ByteDance. En aquest cas la intenció és comprovar si les seves polítiques són diferents de les de pàgines de països com E.E.U.U. o de la Unió Europea que ja coneixem.

1.3.1. Política de privadesa d'Instagram

Instagram en ser una xarxa social amb una gran quantitat d'usuaris, on cadascun comparteix opinions, pensaments o fins i tot detalls de la seva vida. Però és important que l'usuari s'asseguri que no comparteix dades de més.
Observem quines són les dades que recopila l'aplicació.
Cal aclarir, que la informació inclosa a continuació és mencionada a la política de privadesa global de Meta. https://privacycenter.instagram.com/policy/, és a dir afecta igual a tot el món, però el com tracten les dades pot variar d'una regió a altra.

Per poder digerir tota la informació de millor manera s'ha dividit la informació en els següents apartats:

- **Informació social.** Informació compartida amb altres usuaris i, per tant, amb la plataforma.
- **Informació d'accés.** Informació que es proporciona a la plataforma per tal d'accedir a totes les funcions d'aquesta.
- **Informació comercial.** Informació que recopila la web per tal de prendre decisions empresarials o d'adreçar-te publicitat.

- **Informació social.**
    - A que es dona "like".
    - Les publicacions, comentaris i àudios de l'usuari.
    - Les fotos i missatges enviats.
    - Qui són els amics o seguidors de l'usuari i les seves interaccions amb ell (per exemple si l'han etiquetat, trucat a través de l'aplicació, bloquejat, etc.).
    - Quins hashtags fa servir l'usuari.

- **Informació d'accés.**
    - La informació proporcionada per crear un compte, com per exemple adreça de correu electrònic, número de telèfon o data de naixement.
    - El contingut brindat a través de la càmera de l'aplicació, a través de les característiques de veu activada les fotos o a les quals es permet que

l'aplicació accedeixi. Aquesta informació és utilitzada per filtres, avatars, efectes, etc.

- Interaccions amb la IA de Meta.
- Informació dels contactes si es permet l'accés, com el nom, l'adreça de correu electrònic o número de telèfon. També pot ser que tinguin informació d'algú que no sigui usuari de cap dels seus productes si algun contacte seu li ha permès a l'aplicació l'accés a aquesta informació. Aquesta funció existeix per tal de trobar coneguts dins de la plataforma.
- Les transaccions fetes dins de l'aplicació.
- Senyals del dispositiu com GPS o Bluetooth.
- Informació de la xarxa a la qual s'està connectat. Això inclou:
  - Nom de l'operador o proveïdor d'internet.
  - Idioma.
  - Zona horària.
  - Número de telèfon.
  - Adreça IP.
  - Connexió i velocitat de descàrrega.
  - Capacitat de la xarxa.
  - Informació sobre altres dispositius que estan a prop o a la xarxa de l'usuari.
  - Punts d'accés Wi-Fi que es connecten per utilitzar l'aplicació.

  Aquesta informació pot ajudar a connectar diferents dispositius per habilitar diferents funcions, com per exemple poder veure l'aplicació des del televisor o altre dispositiu.

- **Informació comercial.**
  - Informació del dispositiu, com de quin tipus és (si és una tauleta tàctil, un telèfon mòbil o un ordinador), quin model és o quina versió de l'aplicació s'utilitza. Això pot ser usat per considerar canvis en l'aplicació, com canviar la interfície per tal que sigui més còmode per la majoria dels usuaris (per exemple, si el sistema més fet servir és el telèfon mòbil poden considerar tindre un disseny més vertical o més

horitzontal en cas que sigui l'ordinador) o si és rendible que l'aplicació sigui compatible amb sistemes més antics.

- Tipus de contingut vist o interactuat. Aquesta informació brinda la possibilitat que aparegui més contingut similar.
- El temps, freqüència i duració de les activitats de l'usuari dins de l'aplicació.
- El que fa l'usuari amb dispositiu quan l'aplicació està en primer pla o si el ratolí es mou (cosa que pot ajudar a diferenciar als humans dels robots).
- Identificadors per diferenciar els diferents usuaris.
- Alguna informació relacionada a la ubicació, encara que la funció d'ubicació del dispositiu estigui desactivada. Això inclou utilitzar l'adreça IP de l'usuari per estimar la seva ubicació.
- Informació de rendiment de l'aplicació al dispositiu.
- Informació de *cookies* i similars.

1.3.2. Política de privadesa de TikTok

La idea principal d'analitzar la política de privadesa de TikTok era veure si en ser una empresa de la Xina (un estat molt diferent del nostre tan econòmica com socialment) es prenia més o menys llibertats quant a la privadesa, però igual que les polítiques de privadesa anteriors (exceptuant Tor) consta de diferències basades en la jurisdicció de cada país. A més la mateixa pàgina et facilita revisar totes les variants de la política de privacitat sense la necessitat d'una VPN.

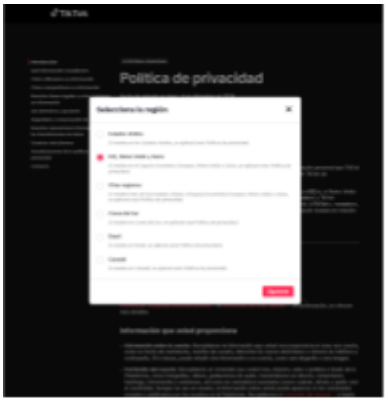

Fig. 1.4. Captura que mostra com es pot escollir quina política de privadesa es desitja veure. Extreta de TikTok. (s.d.). *Política de Privicidad. https://www.tiktok.com/legal/page/row/privacy-policy/es*

Evidentment, revisarem la política que ens afecta, és a dir, la de l'Espai Econòmic Europeu. https://www.tiktok.com/legal/page/eea/privacy-policy/es.

- **Informació que proporciones**
    - **Informació sobre el compte**: Informació que es proporciona en crear un compte, com la data de naixement, nom d'usuari, adreça de correu electrònic o número de telèfon i contrasenya. També inclou la informació opcional com una biografia o una imatge.
    - **Contingut de l'usuari:** El contingut creat, importat, pujat o publicat a través de la plataforma, com fotografies, vídeos, gravacions d'àudio, etc. així com les metadades associades (quan, on i qui va crear el contingut). Encara que algú no sigui usuari, pot aparèixer informació seva en els continguts creats o publicats pels usuaris a la plataforma. La plataforma recopila el contingut que l'usuari carrega, importa o crea (text, imatges, vídeos), encara que no es guardi definitivament, per exemple per fer recomanacions. També pot recopilar contingut del porta-retalls quan l'usuari copia i enganxa o comparteix informació amb altres plataformes. A més, recull dades d'ubicació si l'usuari decideix afegir-les al seu contingut.
    - **Missatges:** Igual que Instagram, TikTok recopila el contingut de tots missatges enviats i rebuts en la plataforma i les metadades associades.
    - **Contactes i altres vincles:** funciona igual que com hem vist a Instagram.
    - **Informació de compres dins de l'app.**
    - **Enquestes, sondejos i promocions:** L'aplicació recopila la informació que proporcionada en participar en una enquesta, sondeig, promoció, o similars.
    - **Informació quan es posa en contacte amb la institució:** Quan un usuari contacta amb la institució es recopila la informació enviada, com proves d'identitat o d'edat, comentaris o consultes sobre l'ús de la plataforma o infraccions de certes polítiques.
    - **Informació dels formularis:** Es recopila la informació proporcionada en els formularis per a així brindar l'opció d'emplenar-los automàticament.

- **Informació recopilada automàticament**
    - **Informació tècnica:** Igual que Instagram, TikTok recopila informació del dispositiu (incloent-hi els patrons o ritmes de pulsació de tecles, configuració del dispositiu, rendiment de l'aplicació, etc.) i de la xarxa (per exemple l'adreça IP o informació de dispositius connectats) quan s'està connectat a la plataforma. A més també s'usen identificadors d'usuari i dispositiu fent-los servir per exemple per identificar activitat del compte en altres dispositius, podent així detectar activitats sospitoses.
    - **Informació sobre la ubicació:** Es recopila informació relacionada a la ubicació aproximada basant-se en informació de la targeta SIM, de l'adreça IP, o dels serveis de localització opcionals de l'aplicació de TikTok.
    - **Informació d'ús:** Es recopilen les interaccions amb el contingut, els usuaris i els anuncis. També es té present l'historial de cerques.
    - **Funcions i característiques dels continguts:** Es recopilen característiques sobre els vídeos, imatges i gravacions d'àudio per així afegir efectes com filtres o avatars.
    - **Informació inferida:** La web dedueix atributs de l'usuari (com el rang d'edat i el sexe) i els seus interessos a partir de la seva informació. Això es fa amb el propòsit de moderar el contingut i adreçar publicitat personalitzada.
    - ***Cookies*:** Es fan servir per recordar preferències d'idioma, no adreçar el mateix vídeo més d'una vegada al mateix usuari i per motius de seguretat.

- **Informació d'altres fonts**
    - **Socis publicitaris, de mesurament i altres:** Els anunciants i els socis de mesurament, entre altres, comparteixen amb la plataforma informació de les accions que realitzen els usuaris fora d'aquesta amb la intenció d'adreçar publicitat personalitzada.
    - **Venedors i proveïdors de pagament i tramitació de transaccions:** La plataforma recopila informació que pot incloure els detalls de

confirmació de pagament i informació sobre el lliurament de productes que s'hagin comprat a través de les funcions de compres de l'aplicació.

- **Plataformes de tercers i socis:** Plataformes de tercers proporcionen informació dels usuaris (com l'adreça de correu electrònic, la ID d'autentificació i el perfil públic) a TikTok quan es registren o inicien sessió en la plataforma utilitzant les funcions d'inici de sessió proporcionades per aquestes terceres. Quan l'usuari interactua amb serveis de tercers integrats amb TikTok, la plataforma rep la informació necessària per oferir funcions com l'inici de sessió en altres aplicacions o el fet de compartir continguts entre plataformes. Això passa, per exemple, quan s'usa el compte de TikTok per accedir a altres serveis o el botó de compartir. A més, TikTok pot rebre informació de proveïdors externs amb finalitats de seguretat i moderació de continguts.
- **Fonts addicionals:** Es poden recopilar o rebre informació dels usuaris a través d'organitzacions, empreses, persones i altres parts, incloses, per exemple, fonts d'accés públic, autoritats governamentals, organitzacions professionals i grups benèfics. La plataforma també recopila informació quan l'usuari és esmentat o inclòs en publicacions, missatges, comentaris, queixes o sol·licituds, així com quan altres usuaris o tercers faciliten les seves dades de contacte.

1.3.3. Conclusió de la privadesa a les xarxes socials

Com ja sabem les xarxes socials són webs on la majoria d'usuaris tenen la intenció de compartir informació seva per donar-se a conèixer, per tant, no té massa sentit cercar anonimat dins d'aquestes. Però en cas de voler fer-ho és bastant plausible, ja que gran part de la informació és recopilada una vegada es dona consentiment a la funció concreta que requereix dita informació. Per exemple, abans de publicar una foto de l'emmagatzematge es demana l'accés a aquest i és l'usuari qui decideix quan ho fa.

Evidentment, hi han dades que es comencen a recopilar una vegada es fa servir la plataforma per primera vegada, i si bé no és informació gaire reveladora, sí que pot suposar un problema per certs usuaris.

Les xarxes socials són, a priori, gratuïtes, però igual que tots els serveis existents han de cercar una forma de monetitzar. I és aquí on es troba el problema, perquè aquestes plataformes cerquen la manera perquè els seus usuaris consumeixin la major quantitat de publicitat possible. El sistema que han trobat les xarxes per aconseguir-ho és mantenir els usuaris dins de la plataforma el màxim temps possible.
La informació sobre el contingut vist i la manera com s'hi interactua s'utilitza per alimentar algoritmes que recomanen contingut similar, mantenen l'atenció de l'usuari i permeten mostrar anuncis personalitzats. El format de vídeos curts que TikTok va popularitzar potencia aquest efecte, fomentant una experiència addictiva orientada al consum de publicitat i al consumisme.

Llavors, que podem extreure de tot això? Les xarxes són webs on es pot tenir cert anonimat, perquè és l'usuari qui posa el límit de quanta informació comparteix a través de les publicacions. És veritat que la plataforma tindrà encara més informació, però tot és amb el fi de garantir la seguretat i la convivència entre usuaris (evitar l'assetjament, evitar el fet de compartir enllaços a material il·legal a través de publicacions, etc.). El problema resideix en com aquestes empreses s'aprofiten dels usuaris per monetitzar.
La publicitat personalitzada no és necessàriament negativa, però combinada amb les estratègies per retenir els usuaris a la plataforma pot resultar excessiva i provocar problemes de salut mental, com el consum desmesurat o l'addicció a la mateixa plataforma.
Per tant, no només hem de vigilar quines dades compartim, sinó que també hem de ser conscients de per què les fan servir i de si realment val la pena utilitzar segons quins serveis.

1.4. Polítiques de privadesa a la IA

A causa del gran impacte que té el desenvolupament de la intel·ligència artificial sobre la nostra societat actual és de vital importància comprovar si la IA és realment segura quant a privadesa es refereix. S'analitzarà la política de privadesa següent:

- **OpenAI:** És l'empresa darrere del conegut xatbot ChatGPT. Actualment, és de les IA més desenvolupades, si no la que més. A més moltes altres IA (com Microsoft Copilot[5] o Perplexity AI[6]) estan basades en models d'OpenAI o mínim inspirades, per tant, analitzant la política d'aquesta empresa ja és més que suficient per fer-se una idea de com és la situació actual de la privadesa a les IA.

1.4.1. Política de privadesa d'OpenAI

Com sempre es tindrà en compte únicament la política de la Unió Europea d'OpenAI. https://openai.com/ca-ES/policies/eu-privacy-policy/.

Dades personals recollides:

- **Dades personals proporcionades:**
  - Informació del compte: El nom, la informació de contacte, les credencials del compte, la data de naixement, la informació de pagament i l'historial de transaccions.
  - Continguts de l'usuari: Es recullen les dades personals que es proporcionen en accedir als serveis d'OpenAI, incloses les publicacions i la resta de continguts que es pugen, com ara fitxers, imatges i àudios.
  - Informació de comunicació: En contactar amb l'empresa és possible que es recullin dades personals com ara el nom, la informació de contacte i el contingut dels missatges.
  - Altra informació proporcionada: Informació recopilada en participar en certs esdeveniments o enquestes de la companyia o proporcionada per determinar la identitat o edat de l'usuari.

[5] Confirmació que Microsoft Copilot està basada en models d'OpenAI: https://blogs.bing.com/search/march_2023/Confirmed-the-new-Bing-runs-on-OpenAI%E2%80%99s-GPT-4/

[6] Confirmació que Perplexity AI està basada en models d'OpenAI: https://www.perplexity.ai/help-center/en/articles/10352155-what-is-perplexity

- **Dades personals compartides a partir de l'ús dels serveis:**
    - Dades de registre: Informació que el navegador o dispositiu envia automàticament en utilitzar els serveis d'OpenAI incloent l'adreça IP, el tipus i la configuració del navegador, la data i l'hora de la sol·licitud, i com s'interactua amb els serveis de la companyia.
    - Dades d'ús: La plataforma recopila informació sobre com l'usuari fa servir els serveis, com els continguts que consumeix, les funcionalitats que utilitza i les accions que realitza, així com dades tècniques i d'accés com el país, el fus horari, el dispositiu i la connexió.
    - Informació del dispositiu: La informació sobre el dispositiu que es fa servir és recollida en accedir als serveis, com ara el nom del dispositiu, el sistema operatiu, els identificadors del dispositiu i el navegador utilitzat. La informació recollida pot dependre del dispositiu emprat i de la configuració que tingui.
    - Informació sobre la ubicació: És possible que la plataforma dedueixi la ubicació aproximada del dispositiu a través de l'adreça IP per motius de seguretat (per exemple, protegint el compte detectant una activitat de connexió inusual) i per millorar l'experiència del producte (proporcionar respostes més acurades). A més, alguns serveis permeten que l'usuari faciliti una ubicació més precisa, com la del GPS.
    - *Cookies* i similars: S'emmagatzema informació (amb compte o sense) per mantenir les preferències de l'usuari.
    - Informació rebuda d'altres fonts: Informació que rep la plataforma per part de col·laboradors com col·laboradors de seguretat (per evitar ciberatacs) o de proveïdors de màrqueting (per facilitar informació sobre els possibles clients dels serveis comercials d'OpenAI).
    - Informació pública: Es recull informació pública d'internet per desenvolupar models (com ChatGPT) dels serveis d'OpenAI.

Com s'utilitzen les dades personals abans esmentades

Les dades personals poden ser fetes servir amb les finalitats següents:

- Per proporcionar anàlisis i mantenir els serveis.
- Per millorar i desenvolupar els serveis i dur a terme tasques de recerca.

- Per poder contactar amb l'usuari i enviar-li informació sobre actualitzacions dels serveis o d'esdeveniments.
- Per evitar el frau, l'activitat il·legal o l'abús dels serveis i per protegir la seguretat d'aquests mateixos.
- Per complir obligacions legals i protegir els drets, la privacitat, la seguretat o la propietat dels usuaris, de l'empresa o de tercers.

Les dades són agrupades o anonimitzades perquè sigui impossible identificar a l'usuari. Aquestes mateixes dades poden ser utilitzades amb fins d'analítica o de millora dels serveis (els fitxers, les imatges i els àudios enviats a la IA poden ser usats per entrenar-la). La informació no serà reidentificada a menys que la llei ho exigeixi.

Revelació de dades personals

Algunes de les dades recopilades poden ser compartides en les circumstàncies següents:

- Per oferir els seus serveis, la plataforma pot compartir dades amb diversos proveïdors externs (allotjament, atenció al client, anàlisi, pagaments, seguretat o serveis al núvol). Aquests només poden accedir i tractar les dades personals seguint les instruccions de la companyia i únicament per complir les seves funcions.
- En cas que OpenAI estigui sota una transacció, reorganització, insolvència, administració judicial o transició de proveïdors les dades poden ser divulgades amb les contraparts corresponents, incloent-hi filials.
- OpenAI pot compartir dades amb autoritats governamentals, empreses del sector o altres tercers de conformitat amb la llei en cas que:
    - Si és un requisit o creien de bona fe que és necessari per complir amb una obligació legal.
    - Per protegir i defensar els drets i propietats de la companyia.
    - Si determinen que hi ha hagut una violació dels termes o polítiques de l'empresa o una violació de la llei.
    - Per detectar o evitar el frau o altres activitats il·legals.
    - Per protegir la seguretat i la integritat dels productes, treballadors i usuaris o del públic.
    - Per protegir-se de responsabilitat jurídica.

- En crear un compte ChatGPT Enterprise o d'empresa els administradors del compte podran controlar-lo i accedir als continguts. A més si el compte és creat amb una adreça de correu electrònic d'alguna institució, podran compartir certa informació amb aquesta.
- Es pot compartir informació voluntàriament amb l'opció de ChatGPT de compartir els xats a través d'un enllaç.

Conservació

Les dades personals es conservaran segons:

- La finalitat de tractament de les dades (com ara si han de conservar les dades per prestar els serveis d'OpenAI).
- La quantitat, la naturalesa i la confidencialitat de la informació.
- El risc potencial de danys derivats d'un ús o revelació no autoritzats.
- Qualsevol requisit legal a què la companyia està subjecta.

1.4.2. Conclusió de la política de privadesa d'OpenAI

La intel·ligència artificial pot arribar a ser una eina extraordinària, brinda respostes concretes a les preguntes alliberant als usuaris de la feina que suposa cercar informació. Si bé és veritat que no és una eina pas anònima no suposa cap risc per als usuaris.

Tota la informació és recopilada per contribuir al funcionament de l'eina, sigui per mantenir els serveis o per contribuir al desenvolupament de la IA. L'única forma que té l'empresa de fer servir aquesta informació en contra dels usuaris és en cas que aquests estiguin sota investigació judicial i que les autoritats contactin amb la companyia sol·licitant informació. Però és un procés llarg i complicat: primer les autoritats han de contactar amb OpenAI, després la companyia ha d'accedir a contribuir a la investigació, s'han de cercar les dades concretes de l'usuari d'entre milions per desanonimitzar-les, i finalment pot concloure que les proves no són prou contundents. Per tant, és difícil que la informació pugui arribar a perjudicar a algú realment.

És important tindre en compte que els continguts enviats a la IA són recopilats per contribuir al desenvolupament d'aquesta, doncs, en cas que algú estigui en contra

del desenvolupament d'aquesta la recomanació és no utilitzar-la perquè analitza els missatges, imatges, vídeos, etc. per després ser capaç d'imitar-les.

En resum, els serveis d'OpenAI són fiables quant a privacitat, però s'ha de tindre en compte que el contingut dels usuaris és la base del que genera la IA, per tant, hem de ser conscients amb el que li ensenyem.

2. FILTRACIÓ IL·LEGAL DE DADES (MALWARES I SIMILARS)

Ja hem comprovat com diverses pàgines web recopilen dades nostres fent-nos rastrejables a través de la web sense dret real a l'anonimat.
Afortunadament, aquestes pàgines recopilen informació amb fins legítims, recopilant les dades justes i necessàries per poder gaudir de totes les funcions de la web. A més a més, si bé no som anònims gràcies a les dades recopilades, la majoria d'aquestes no són de gaire importància, no revelen informació de la nostra vida personal, i en cas que sigui necessari com per exemple per fer una transacció bancària la informació és completament xifrada per dificultar la filtració d'aquesta.

Això no vol dir que la informació sigui llibre de ser filtrada. Com hem vist en parlar de Tor, accedir a una pàgina web és com una conversa en la qual hi pot haver receptors no desitjats, en xifrar la informació és com si a la conversa es comencés a xiuxiuejar i a parlar en un idioma que només l'emissor i el receptor pertinent coneixen. Però és això suficient perquè les dades no siguin filtrades?

Aquí és on entrem als mètodes de filtració de dades (clarament il·legals), en aquest apartat investigarem diferents mètodes de filtració o robatori de dades de diferents tipus.

2.1. Objectiu de les filtracions de dades

Amb el primer apartat hem pogut veure quines dades poden ser recopilades, però quins són els motius per realitzar aquests atacs?

Segons Kaspersky a *Qué es una filtración de datos y cómo prevenirla.* https://www.kaspersky.es/resource-center/definitions/data-breach: "és possible que

es produeixin danys reals si la persona amb accés no autoritzat roba i ven informació d'identificació personal (IPI) o dades intel·lectuals corporatives per a obtenir beneficis econòmics o causar danys".
Individualment, pot portar problemes com comprometre dades importants (direccions, informació de comptes bancàries, etc.) i aquestes dades poden ser utilitzades pel benefici d'altres o com a eina de xantatge.
En l'àmbit empresarial la cosa és diferent, la filtració de dades pot suposar la filtració de prototipus de futurs productes, la qual cosa pot beneficiar a la competència a més de donar una mala imatge de cara al consumidor.

Per tant, podríem concloure que en la majoria dels casos es realitzen amb fins lucratius, sigui venent informació o fent xantatge.

2.2. Mètodes de robatori de dades a través de la web

2.2.1. Atacs d'enginyeria social

L'enginyera social és una tècnica de manipulació que aprofita l'error humà amb diferents fins. En aquests casos l'agressor sol infondre urgència a la víctima amb l'objectiu que tingui menys temps de resposta, per tant, aquesta actuï sota pressió i sense raonar-ho dues vegades. En conseqüència, davant d'un d'aquests atacs és important mantenir la calma, moltes de les amenaces de l'agressor són ideades amb el fi de fer sentir a la víctima sota un perill real, tot i que el més probable és que l'agressor encara no tingui cap dada seva.

El mètode de robatori per excel·lència on s'aplica aquesta tècnica és el **Phishing (pesca de dades)**. En el Phishing l'atacant es fa passar per una organització o persona de confiança per tal que la víctima introdueixi les seves dades personals. N'hi ha de diferents tipus:

- **El phishing per correu electrònic** és el mitjà més tradicional de phishing, ja que utilitza un correu electrònic que insta a respondre o fer un seguiment per altres mitjans. Es poden usar enllaços, números de telèfon o arxius adjunts de malware.

- **Els missatges de text de phishing** o els missatges d'aplicacions mòbils poden incloure un enllaç web o un missatge de seguiment a través d'un correu electrònic o un número de telèfon fraudulents.
- **Phishing per veu** és un altre mètode molt popular, en el qual una persona truca fent-se passar per una altra amb l'excusa que és una urgència i amb aquest sentiment provocar que la víctima doni les seves dades.
- **El phishing d'Angler** es duu a terme en les xarxes socials, on un atacant fingeix ser de l'equip de servei al client d'una empresa de confiança. Intercepten les comunicacions amb una empresa per a segrestar i desviar la conversa a missatges privats, on després fan avançar l'atac.
- **El phishing en cercadors** intenta col·locar enllaços a llocs web falsos en la part superior dels resultats de cerca. Aquests poden ser anuncis pagats o poden usar mètodes d'optimització legítims per a manipular les classificacions de cerca.
- **El phishing durant la sessió** apareix com una interrupció de la navegació web normal. Per exemple, és possible que veure finestres emergents d'inici de sessió falses per a les pàgines que s'està visitant.

2.2.2. Atacs de força bruta

Mètode en el qual els hackers utilitzen eines de software (aplicacions) per tractar d'endevinar les contrasenyes de la víctima provant totes les combinacions possibles. Segons la llargada i la dificultat de la contrasenya aquest procés pot trigar des d'uns segons fins a uns quants anys.

2.2.3. Malwares

Els malwares o programes maliciosos són programes dissenyats amb l'objectiu de danyar, interrompre o accedir al sistema operatiu sense el consentiment de l'usuari.
En aquest apartat s'abastaran els tipus més coneguts de malware, explicant breument quin és el funcionament habitual de cada tipus.

2.2.3.1. Troià

Deu el seu nom al mite del cavall de Troia, ja que aquest programa es fa passar per un arxiu legítim quan en realitat és un malware. Tal com el cavall de Troia es feia passar per un regal quan en realitat no era més que una tapadora perquè els soldats grecs poguessin entrar a la ciutat de Troia.

2.2.3.2. Adware

Aquests programes no tenen per què ser malwares, però llastimosament es poden fer servir amb aquest fi. Entrant en matèria, l'adware o software publicitari és un programa que mostra anuncis emergents sense consentiment. Aquests anuncis redirigeixen els resultats de les cerques a llocs web de publicitat (de vegades maliciosos) i recopila les dades dels usuaris per a vendre'ls a anunciants sense el seu consentiment.

2.2.3.3. Spywares

Es considera spyware aquell programa dissenyat per robar les dades d'un dispositiu per enviar-les a un tercer sense el coneixement o consentiment de l'usuari. Aquesta informació pot incloure la recopilació de dades confidencials, com a contrasenyes (en aquests casos se'ls anomena Keyloggers), números PIN, nombres de targetes de crèdit, la supervisió de les pulsacions de tecles, el rastreig dels hàbits de navegació i la recopilació d'adreces de correu electrònic.

2.2.3.4. Cucs (Worms)

Els cucs o worms són un tipus de malwares que es propaguen a través de xarxes informàtiques mitjançant l'explotació de vulnerabilitats dels dispositius. Aquests programes són independents, és a dir, no requereixen cap intervenció. Normalment, aquests softwares es solen utilitzar per executar alguna línia de codi que danyi el sistema, provocant per exemple l'eliminació o encriptació d'arxius, el robatori de dades o la creació de botnets.

2.2.3.5. Bots i botnets

En aquest context els bots són dispositius infectats que són controlats per un individu remotament. Es pot fer servir per a executar més atacs o formar part d'una

xarxa de bots (botnet). Aquests botnets poden ajudar el hacker a atacar altres dispositius.

2.2.3.6. Ransomware

El ransomware és un malware que actua com una espècie de segrestador de sistemes operatius. Aquests tipus de programes encripten tots els arxius del dispositiu impedint-ne l'accés fins que no es pagui certa quantitat (normalment el pagament es fa en bitcoin per dificultar el rastreig del delinqüent).

2.2.3.7. Malware de criptomineria

Un malware de criptomineria és un codi potencialment no desitjat o maliciós dissenyat per a utilitzar la potència de processament en repòs d'un dispositiu de destí per a minar criptomonedes. L'activitat minera sol estar oculta o executar-se en segon pla sense obtenir el consentiment de l'usuari afectant el rendiment del dispositiu.

PART PRÀCTICA

3. INTRODUCCIÓ I OBJECTIU DE LA PART PRÀCTICA[7]

Una vegada observat com i per què és causat el robatori de dades, s'ha decidit per aquesta part pràctica desenvolupar un exemple de pàgina web "maliciosa" amb l'objectiu de conscienciar sobre la seguretat a internet.

En aquesta pràctica es desenvoluparà una pàgina web a la qual en clicar a cert botó de la pàgina l'usuari serà reenviat a altra part on es descarregarà automàticament un arxiu que simularà ser un malware, en aquest cas simularà ser un ransomware.
És una simple demostració sense cap intenció de perjudicar cap dispositiu, l'arxiu descarregat no serà cap malware sinó un arxiu batch (s'explicarà que és més endavant) que només imita visualment el que passaria amb un ransomware real.

[7] **Important:** en cas que no s'indiqui el contrari totes les imatges vistes en aquesta part pràctica són de la meva autoria.

4. DESENVOLUPAMENT DEL FALS MALWARE

Per aconseguir l'efecte visual desitjat s'utilitzarà un arxiu "batch", que té com extensió ".bat". Aquests arxius són arxius de text conformats per comandaments, que, en executar el fitxer, són enviats a la consola del sistema, la qual abreviarem com **CMD**. El que volem és que amb aquests comandaments podem simular visualment un ransomware.

En ser un arxiu de text l'única eina que necessitarem per desenvolupar el fitxer és el bloc de notes que ve predeterminat a Windows, amb la diferència que una vegada es guardi el fitxer s'haurà de canviar l'extensió de ".txt" (arxiu de text) a ".bat".

El primer que farà aquest arxiu és tancar la majoria dels processos de l'ordinador, però com fer això indiscriminadament amb qualsevol procés sí que podria resultar perjudicial, el que farà és tancar processos populars per així generar l'efecte impactant desitjat.

Per fer això s'utilitza el comandament "taskkill". El qual té la següent estructura:

taskkill /IM "nom del procés" /F

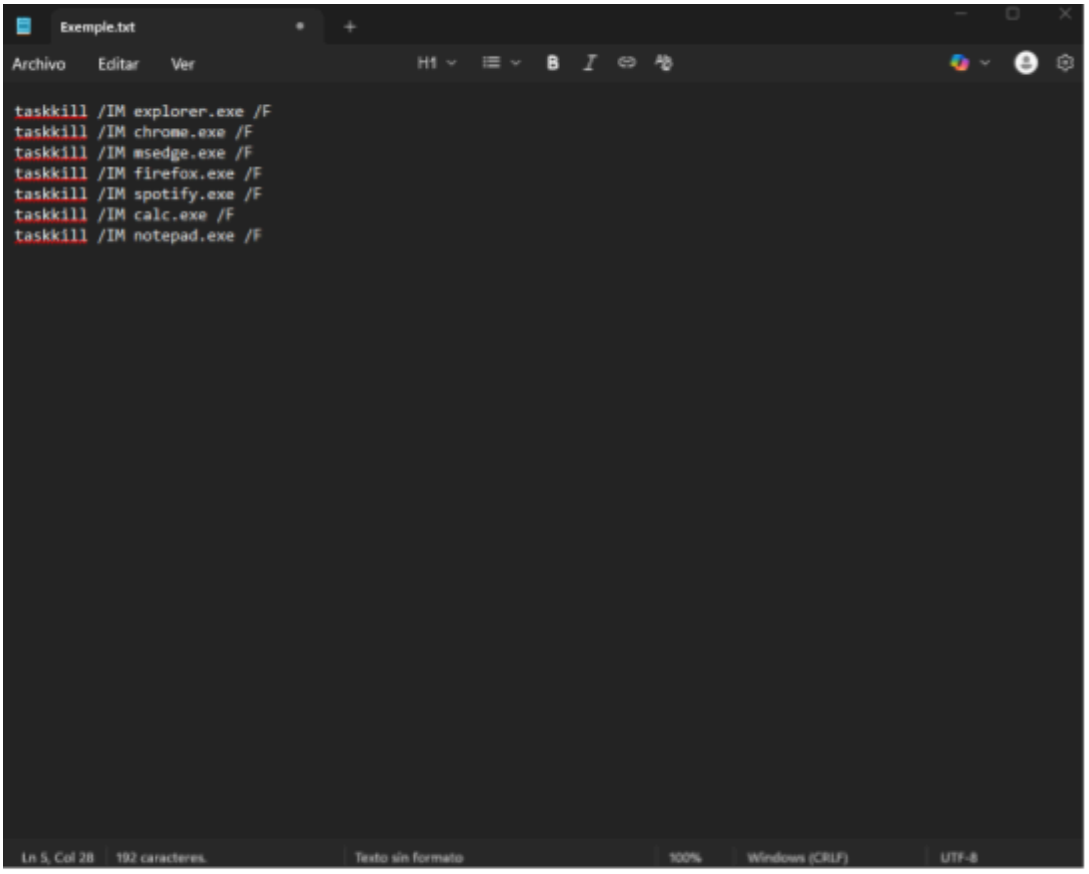

Fig. 4.1. Captura de la programació de l'arxiu batch.

A la captura es pot observar com s'ha aplicat aquest comandament amb:

- L'explorador d'arxius.
- Diferents navegadors, en aquest cas: Chrome, Microsoft Edge i Firefox.
- Spotify.
- La calculadora (encara que no sempre funciona, ja que no a tots els ordinadors té el mateix nom).
- El bloc de notes.

Després volem interactuar amb l'usuari per la CMD.

Per això es pot assignar un títol a la pestanya amb: **title "nom"** i utilitzar el comandament **"echo"** per fer que la pestanya escrigui qualsevol missatge que es desitgi.

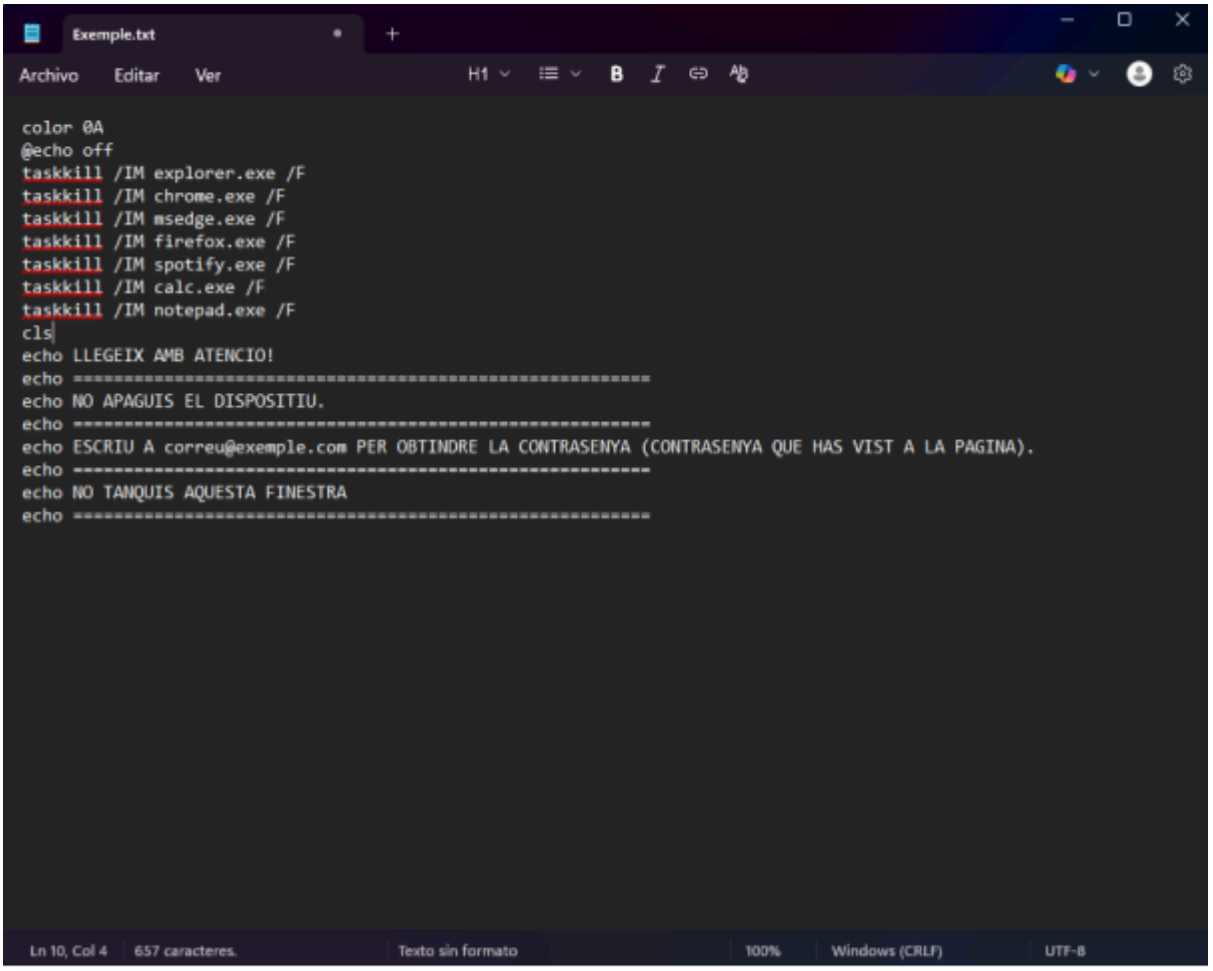

Fig. 4.2. Captura de la programació de l'arxiu batch.

En aquest cas s'han escrit les línies que es poden veure a la imatge perquè sembli un ransomware de veritat.
També, amb fins estètics s'han implementat els següents comandaments:

- **color 0A:** dona a la CMD els colors negre i verd.
- **@echo off:** fa que no es vegin tots els comandaments a la CMD.

Exemple:
Sense @echo off:
C:\>echo Hola
Hola

Amb @echo off:
Hola

- **cls:** esborra el que hi havia escrit prèviament a la CMD.

Per acabar, com tot Ransomware, es vol una contrasenya que ho retorni tot a la normalitat.
Per això s'utilitza:
set /p pass="text"
El qual indica a la CMD que escrigui un "text" que serà el senyal perquè l'usuari escrigui la contrasenya.

A continuació s'assigna la contrasenya i s'indica que passa en cas d'encertar i que passa en cas de fallar.
En aquest cas:
if %pass%==TdR (goto passcorrecto) ELSE (goto bucle)
Aquí s'indica que si la contrasenya és "TdR", el sistema haurà de realitzar el comandament "passcorrecto", però en cas de fallar el sistema tornarà on s'assigni el bucle, en aquesta ocasió es posicionarà just abans del comandament "cls".

El comandament "passcorrecto" assignat és
:passcorrecto
echo Molt be! Et torno el teu dispositiu.
start explorer.exe
pause

exit

El qual indica que en encertar la CMD ha d'escriure el missatge "Molt be! Et torno el teu dispositiu.**"**, tornar a activar el procés de l'explorador d'arxius i sortir del fitxer batch.

Així queda el codi final:

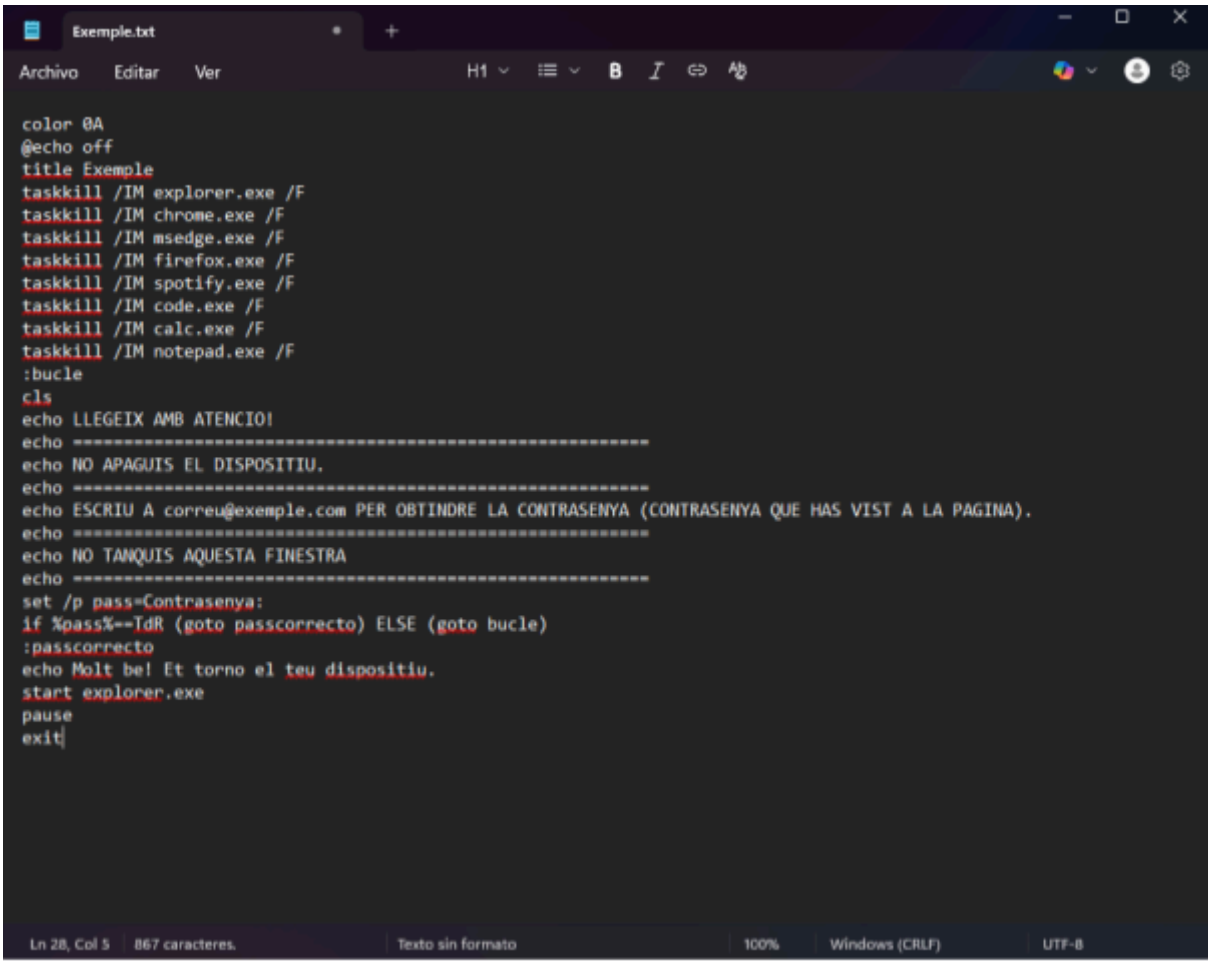

Fig. 4.3. Codi final de l'arxiu batch.

Es guardarà el fitxer com "HackTdR.bat". És important canviar l'extensió a ".bat" perquè l'arxiu es transformi d'un arxiu de text a un arxiu batch.

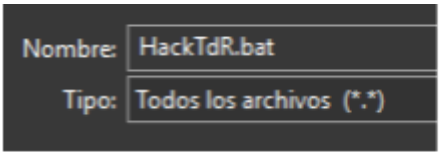

Fig. 4.4. Captura de com s'ha desat l'arxiu.

5. DESENVOLUPAMENT DE LA PÀGINA WEB

Bé, una vegada creat l'arxiu que farà de malware s'haurà de desenvolupar la pàgina web.

Per programar la pàgina s'ha fet servir l'editor de codi anomenat "Visual Studio Code" que es pot trobar gratuïtament a la "Microsoft Store".

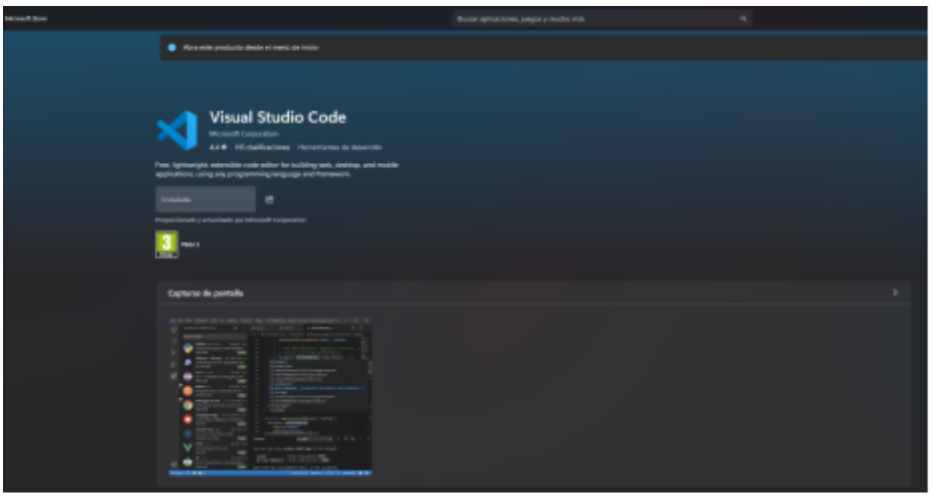

Fig. 5.1. Captura de l'aplicació Visual Studio Code a la Microsoft Store.

5.1. Començament i principis bàsics

El primer que haurem de fer és crear una carpeta al nostre ordinador, carpeta la qual contindrà tots els elements de la pàgina.

En aquest cas s'assignarà el nom de "Pàgina TdR". Una vegada feta la carpeta s'arrossega dins de l'editor per començar el projecte.

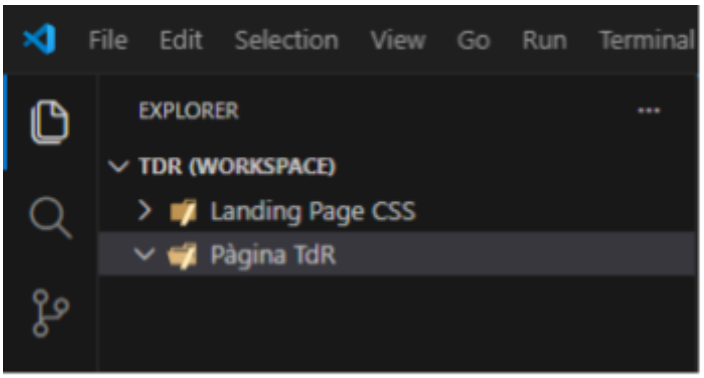

Fig. 5.2. Captura que mostra l'estat inicial de la carpeta de la pàgina.

Posteriorment, es crea un arxiu HTML (.html).

HTML és l'idioma de programació en el que es basen la majoria de les pàgines web. Dins d'aquest fitxer es crearà el codi principal de la pàgina.

A més de l'arxiu HTML, es creen també dues carpetes dins de l'anterior, una d'aquestes carpetes contindrà les imatges (s'ha d'anomenar "images") i l'altra contindrà el codi CSS (la carpeta ha de tindre "css" com a nom i tots els seus arxius han de tindre l'extensió ".css").

El CSS és un llenguatge emprat a HTML per estilitzar la pàgina. És a dir, amb HTML es crea l'element i amb CSS s'indica com es vol que es mostri de cara al visitant de la web.

Dins de la carpeta crearem els arxius "estils.css" i "normalize.css", els quals programarem més endavant.

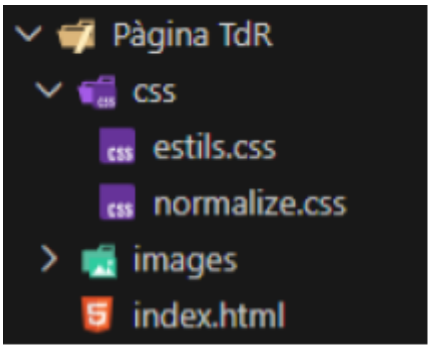

Fig. 5.3. Progrés de la carpeta de la pàgina.

5.2. Programació de l'arxiu HTML (index.html)

En aquest apartat s'explicarà el codi de la pàgina. Com que explicar que fa cada línia dificultaria l'enteniment de la pàgina, el que faré és dir que fa cada bloc de codi.

- **Bloc 1: Encapçalat**

```
<!DOCTYPE html>
<html lang="ca">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Treball de Recerca</title>
    <link rel="shortcut icon" href="./images/favicon.png" type="image/x-icon">
    <link rel="stylesheet" href="./css/normalize.css">
    <link rel="stylesheet" href="./css/estils.css">
</head>
```

Fig. 5.4. Secció de codi de "index.html" anomenada "Bloc 1", defineix diferents funcions bàsiques.

En aquest bloc es defineix l'arxiu com a arxiu HTML i selecciona d'idioma el català. També s'indica que l'estil de la pàgina és el determinat per "estils.css" i "normalize.css".

A més a més, també se li dona títol i un “favicon” (que es troba dins de la pestanya “images”), és a dir una icona.

Fig. 5.5. Mostra visual de com es veu el títol (encerclat en vermell) i el favicon o icona (encerclat en verd).

La imatge utilitzada com a favicon és la següent:

Fig. 5.6. Imatge usada com a favicon. Extreta de Institut Puig Cargol.
https://agora.xtec.cat/iespuigcargol-calonge/treball-de-recerca/

- **Bloc 2: “Hero container”**

Fig. 5.7. Secció de codi de “index.html” anomenada “Bloc 2”, defineix el “hero container”.

Aquí s’està creant un “hero container” que és el contenidor de text i imatges que s’utilitza per introduir una pàgina.
Dins d’aquest contenidor hi ha inclòs un petit índex amb quatre elements (elements “nav”), que són: Introducció, Objectiu, Funcionament i Memòria. La seva funció és que en clicar aquests elements ens transporti directament a la secció corresponent. És a dir, en clicar “Introducció” l’usuari serà transportat a la secció del mateix nom que es definirà al Bloc 3.

També dins del contenidor hi ha un títol central on diu “Treball de Recerca” i un subtítol que té com a text una petita presentació.
En resum, la funció d’aquest bloc és crear el contenidor que dona la benvinguda a l’usuari.

- **Bloc 3: Part principal**

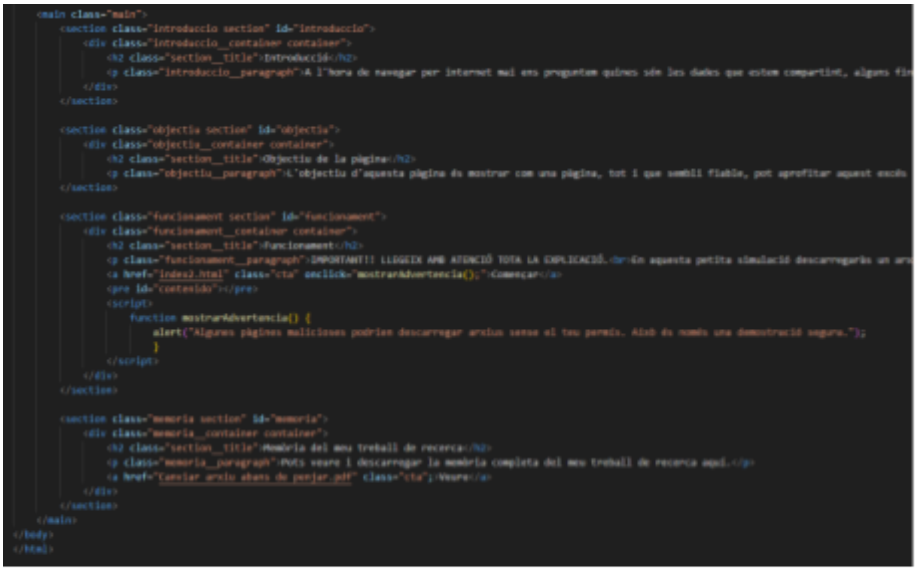

Fig. 5.8. Secció de codi de “index.html” anomenada “Bloc 3”, defineix la part principal de la pàgina.

Aquí es defineix la part principal de la pàgina.
Aquest bloc és bastant més complex, en conseqüència, es dividirà en tres per un millor enteniment.

- **Bloc 3.1.: Seccions simples**

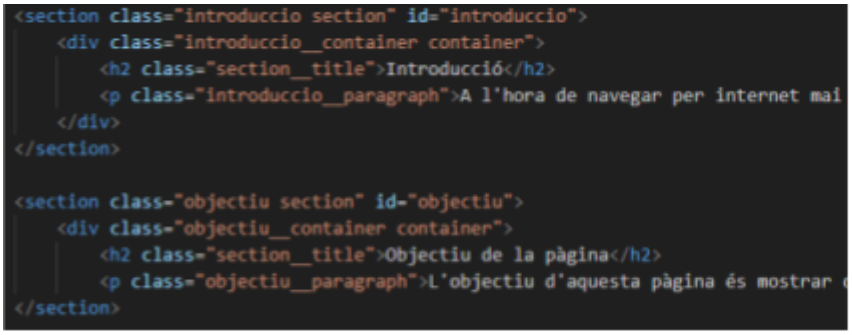

Fig. 5.9. Seccions més simples del “Bloc 3”, defineixen els apartats “introducció” i “objectius”.

Aquí estic creant dues de les seccions ja mencionades al bloc anterior, en concret la secció “introducció” i la secció “objectiu”. En aquestes seccions només hi ha un títol (a cada secció) i unes quantes línies de text que introdueixen la pàgina i explica l’objectiu d’aquesta, per això les considero com “seccions simples”.

- **Bloc 3.2.: Secció “memòria”**

```
        <section class="memoria section" id="memoria">
            <div class="memoria__container container">
                <h2 class="section__title">Memòria del meu treball de recerca</h2>
                <p class="memoria__paragraph">Pots veure i descarregar la memòria completa del meu treball de recerca aquí.
                <a href="Joel López Borrallo TdR L'espia darrere de la pantalla.pdf" class="cta";>Veure</a>
            </div>
        </section>
    </main>
</body>
</html>
```

Fig. 5.10. Secció del “Bloc 3”, defineix l’apartat “memoria”.

Aquesta secció es troba després de la secció “funcionament”, però és millor explicar aquesta primer perquè és més simple i ens ajudarà a comprendre el bloc 3.3.
El que fa aquest bloc és crear la secció “memòria”, definint el seu títol i el text del seu paràgraf. Però a diferència de les seccions “introducció” i “objectiu”, aquí s’ha creat un element “cta” (un botó), que en clicar-ho s’obrirà aquest mateix document.

- **Bloc 3.3.: Secció “funcionament”**

```
<section class="funcionament section" id="funcionament">
    <div class="funcionament__container container">
        <h2 class="section__title">Funcionament</h2>
        <p class="funcionament__paragraph">IMPORTANT!! LLEGEIX AMB ATENCIÓ TOTA LA EXPLICACIÓ.<br>En aquesta petita simulació descarregaràs
        <a href="index2.html" class="cta" onclick="mostrarAdvertencia();">Començar</a>
        <pre id="contenido"></pre>
        <script>
            function mostrarAdvertencia() {
                alert("Algunes pàgines malicioses podrien descarregar arxius sense el teu permís. Això és només una demostració segura.");
                }
        </script>
    </div>
</section>
```

Fig. 5.11. Complexa secció del “Bloc 3”, defineix l’apartat “funcionament”.

Aquesta secció és la més complexa i important.
Aquí es defineix la secció “funcionament” amb el seu títol i paràgraf, però també es crea un element “cta” que en clicar-ho mostra una advertència que recorda que això és només una demostració. Una vegada es clica “Acceptar” a l’advertència el que fa és reencaminar a l’usuari a altra “part” de la pàgina.
Però per fer això es necessita altra “part” de la pàgina, es necessita altre arxiu HTML.

5.2.1. Creació de la segona part de la pàgina (index2.html)

- **Bloc 1: Encapçalat**

```html
<!DOCTYPE html>
<html lang="ca">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Treball de Recerca</title>
    <link rel="shortcut icon" href="./images/favicon.png" type="image/x-icon">
    <link rel="stylesheet" href="./css/normalize.css">
    <link rel="stylesheet" href="./css/estils2.css">
</head>
```

Fig. 5.12. Secció de codi de "index2.html" anomenada "Bloc 1", defineix les mateixes funcions bàsiques que el "Bloc 1" de "index.html".

Té la mateixa funció que el bloc 1 d'"index.html", fins i tot conserva el mateix títol i la mateixa icona.

Un dels documents que defineix l'estil de la pàgina continua sent "normalize.css", però l'altre document que també ho defineix serà "estils2.css". Per tant, s'ha de crear altre arxiu.

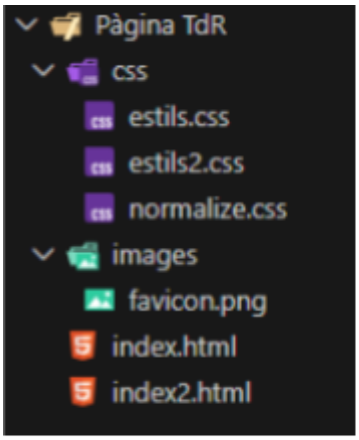

Fig. 5.13. Progrés de la carpeta de la pàgina.

- **Bloc 2: Script (Comandament)**

```html
<script>
window.onload = function(){
  var a = document.createElement("a");
  a.href = "HackTdR.bat";
  a.download = "HackTdR.bat";
  a.click();
};
</script>
```

Fig. 5.14. Secció de codi de "index2.html" anomenada "Bloc 2", defineix el "script" que s'executarà a la secció "index2.html" de la pàgina.

Aquest bloc té com a funció descarregar el fals malware. Com a resultat, s'ha d'afegir l'arxiu a la carpeta.

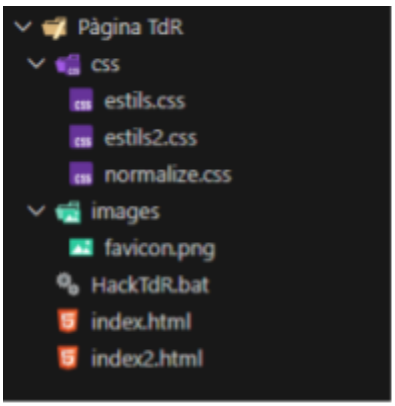

Fig. 5.15. Progrés de la carpeta de la página.

Per més realisme, s'ha fet que l'arxiu es descarregui automàticament una vegada hagi carregat la part "index2" de la pàgina.

- **Bloc 3: "Hero container"**

```
<body>
    <header class="hero">
        <section class="hero__container container">
            <h1 class="hero__title">GENIAL!</h1>
            <p class="hero__paragraph">Executa l'arxiu per continuar amb l'experiència.</p>
        </section>
</body>
</html>
```

Fig. 5.16. Secció de codi de "index2.html" anomenada "Bloc 3", defineix el "hero container".

Molt simple, l'únic que fa el bloc és afegir un curt text que diu "GENIAL! Executa l'arxiu per continuar amb l'experiència."

6. DESENVOLUPAMENT DELS ARXIUS CSS

6.1. "normalize.css"

Tots els navegadors tenen diferents estils per defecte que dificulten la compatibilitat de pàgines web entre navegadors, és per això que algunes pàgines es poden veure en alguns navegadors i en altres no.

Llavors, volem que la nostra pàgina sigui compatible amb la majoria de navegadors possibles, per aquest motiu es crea l'arxiu "normalize.css", per mantenir sempre el mateix estil a tots els navegadors.

No és necessària l'explicació del codi bloc per bloc, ja que la seva funció és essencialment aquesta i el codi es pot trobar amb facilitat a internet.

De fet, el codi en aquest cas ha sigut extret de:
Gallagher, N. [Nicolas]. https://github.com/necolas/normalize.css/.

6.2. Programació d'"estils.css"

Com ja s'ha explicat amb anterioritat, "estils.css" és l'arxiu que defineix la visualització d'"index.html".
L'explicació dels blocs serà escarida per facilitar la comprensió.

- **Bloc 1: Tipologia**

```css
@import url('https://fonts.googleapis.com/css2?family=Poppins:wght@300;400;600;700&display=swap');

:root {
    --padding-container: 100px 0;
    --color-title: #333;
}

body {
    font-family: "Poppins", sans-serif;
}
```

Fig. 6.1. Secció de codi d'"estils.css" anomenada "Bloc 1".

Defineix la tipologia de lletra com la tipologia "Poppins" i també defineix aspectes globals com el color de la lletra i certes dimensions dels contenidors.

- **Bloc 2: Decoració general**

En aquest apartat es troben tots els blocs que tenen la funció de definir l'estètica general dels elements "hero" i "nav". És a dir defineixen les dimensions i la posició dels d'aquest tipus d'apartats. També defineixen com es veurà el text: l'interlineat, l'alineació, el color, etc.

```css
.nav{
    --padding-container:0;
    height: 100%;
    display: flex;
    align-items: center;
}

.nav__title {
    font-weight: 300;
}

.nav__items{
    list-style: none;
}

.nav__link{
    margin-left: auto;
    padding:0;
    display: grid;
    grid-auto-flow: column;
    grid-auto-columns: max-content;
    gap: 2em;
}

.nav__links{
    color: #fff;
    text-decoration: none;
}
```

Fig. 6.2. Part del "Bloc 2" d'"estils.css", defineix diferents aspectes dels elements "nav".

```css
.container {
    width: 90%;
    max-width: 1200px;
    margin: 0 auto;
    padding: 20px;
    overflow: hidden;
}

.hero {
    width: 100%;
    height: 100vh;
    min-height: 300px;
    max-height: 500px;
    position: relative;
    display: grid;
    grid-template-rows: 100px 1fr;
    color: #fff;
}
```

Fig. 6.3. Part del "Bloc 2" d'"estils.css", defineix diferents aspectes dels contenidors i de la secció "hero".

```css
.nav__menu{
margin-left: auto;
display: none;
cursor: pointer;
}

.hero__container{
    max-width: 800px;
    display: grid;
    --padding-container:0;
    grid-auto-rows: max-content;
    justify-content: center;
    align-content: center;
    text-align: center;
    padding-bottom: 100px;
}

.hero__title{
    font-size: 4rem;
    margin-bottom: 10px;
}

.hero__paragraph{
    font-size: 1.5rem;
}

.hero__bottom{
    margin-bottom: 20px;
}
```

Fig. 6.4. Part del "Bloc 2" d'"estils.css", defineix diferents aspectes dels elements "nav" i de la secció "hero".

- **Bloc 3: Imatge introductòria**

```css
.hero::before {
    content: "";
    position: absolute;
    top: 0;
    left: 0;
    width: 100%;
    height: 100%;
    background: linear-gradient(180deg, #0000008c 0%, #0000008c 100%), url("../images/ciberseguretat.png");
    background-size: cover; clip-path: polygon(0 0, 100% 0, 100% 100%, 0% 100%);
    z-index: -1;
}
```

Fig. 6.5. Secció de codi d'"estils.css" anomenada "Bloc 3", agrega un fons a la secció "hero".

Aquest bloc té la funció d'afegir un fons a la secció "hero", indicant la forma d'aquest, la seva posició respecte al text i també afegir un petit filtre que atenuï la imatge.

En aquest cas ha d'afegir la imatge "ciberseguretat.png", per tant, l'hem d'afegir a la carpeta d'arxius.

Així:

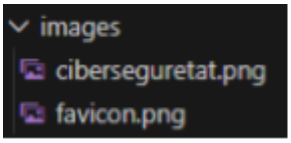

Fig. 6.6. Imatges que conté la pàgina.

El resultat és el següent:

Fig. 6.7. Imatge final de la secció "hero" de la pàgina.

La imatge utilitzada ha estat aquesta:

Fig. 6.8. Imatge utilitzada a la pàgina.
Font: Gómez Villarreal, F.M. [Fernando Martín]
https://www.segurilatam.com/seguridad-por-sectores/financiero/continuidad-de-negocio-relacionada-con-ciberataques-a-la-banca_20200604.html

- **Bloc 4: Part principal**

```css
.introduccio__paragraph{
    text-align: justify;
    margin-bottom: 10px;
    margin-top: 5px;
    line-height: 1.5;
    font-size: 20px;
}

.objectiu__paragraph{
    text-align: justify;
    margin-bottom: 10px;
    margin-top: 5px;
    line-height: 1.5;
    font-size: 20px;
}

.memoria__paragraph{
    text-align: justify;
    margin-bottom: 10px;
    margin-top: 5px;
    line-height: 1.5;
    font-size: 20px;
}

.funcionament__paragraph{
    text-align: justify;
    margin-bottom: 10px;
    margin-top: 5px;
    line-height: 1.5;
    font-size: 20px;
}
```

Fig. 6.9. Secció del codi de "estils.css" anomenada "Bloc 4", defineix l'estil del text de la part principal de la pàgina.

La funció d'aquest bloc és definir com serà el text de les seccions "introducció", "objectiu", "memoria" i "funcionament", especificant l'alineació de text, els marges, l'interlineat i la mida de la lletra.

- **Bloc 5: Element "cta"**

```css
.cta{
    display: inline-block;
    background-color: #2091f9;
    justify-self: center;
    color: #fff;
    padding: 13px 20px;
    text-decoration: none;
    border-radius: 20px;
    display: grid;
    --padding-container:0;
    justify-content: center;
    align-content: center;
    text-align: center;
    margin-top: 30px;
}
```

Fig. 6.10. Secció de codi de "estils.css" anomenada "Bloc 5", defineix com es mostraran els elements "cta".

La funció d'aquest bloc és definir com es mostraran els elements "cta", tant el que ens porta a "index2.html" com el que ens mostra la memòria.

En aquest cas defineix la posició, els marges, el color, la forma i el color del text.

Resultat:

Fig. 6.11. Resultat final de com es veuràn els elements "cta".

6.3. Programació d'"estils2.css"

Una vegada acabada la decoració d'"index.html" cal decorar també "index2.html" creant així "estil2.css".

En ser una secció molt similar i més simple part del codi serà reciclat de l'anterior.

- **Bloc 1: Tipografia**

```
Pàgina TdR > css > # estils2.css > .hero__paragraph
1   @import url('https://fonts.googleapis.com/css2?family=Poppins:wght@300;400;600;700&display=swap');
2
3   :root {
4       --padding-container: 100px 0;
5       --color-title: #333;
6   }
7
8   body {
9       font-family: "Poppins", sans-serif;
10  }
```

Fig. 6.12. Secció de codi d'"estils2.css" anomenada "Bloc 1". És idéntica al "Bloc 1" d'"estils.css".

- **Bloc 2: Decoració de "hero"**

```
.hero__container{
    display: flex;
    flex-direction: column;
    justify-content: center;
    align-items: center;
    text-align: center;
    height: 100vh;
}

.hero__title{
    font-size: 5em;
    font-weight: 600;
    margin-bottom: 20px;
}

.hero__paragraph{
    font-size: 2.5em;
}
```

Fig. 6.13. Secció del codi d'"estils2.css" i part del seu "Bloc 2", defineix diferents aspectes de la secció "hero".

```
.container {
    width: 90%;
    max-width: 1200px;
    margin: 0 auto;
    padding: 20px;
    overflow: hidden;
}

.hero {
    width: 100%;
    height: 100vh;
    min-height: max-content;;
    max-height: max-content;;
    position: relative;
    display: grid;
    grid-template-rows: 100px 1fr;
    color: #fff;
}
```

Fig. 6.14. Secció del codi d'"estils2.css" i part del seu "Bloc 2", defineix diferents aspectes dels contenidors i de la secció "hero".

Recordem que aquesta part només està composta per una secció "hero" que ocuparà tota la pàgina, per tant, només s'ha de decorar aquesta.
La principal diferència és que les seves dimensions són més grans.

- **Bloc 3: Fons**

```
.hero::before {
    content: "";
    position: absolute;
    top: 0;
    left: 0;
    width: 100%;
    height: 100%;
    background: linear-gradient(180deg, #0000008c 0%, #0000008c 100%), url("../images/ciberseguretat.png");
    background-size: cover; clip-path: polygon(0 0, 100% 0, 100% 100%, 0% 100%);
    z-index: -1;
}
```

Fig. 6.15. Secció de codi d'"estils2.css" anomenada "Bloc 3", és idéntica al "Bloc 3" d'"estils.css".

CONCLUSIONS FINALS

Un cop realitzada la investigació es pot concloure que la hipòtesi ha quedat demostrada. Serveis com Google, Instagram o TikTok recopilen una gran quantitat d'informació dels seus usuaris i molta d'aquesta informació es fa servir amb fins de lucre.
Tal com s'indica a les seves polítiques de privacitat, recopilen informació de les activitats dels usuaris dins i fora dels seus serveis amb la intenció d'adreçar publicitat. Si a això li afegim el model addictiu que estan adoptant aquests serveis (en especial les xarxes socials) dona com a resultat una experiència que genera dependència i que indueix al consumisme.

Tot i això, aquests serveis no utilitzen la informació per només aquests fins, gran part d'aquesta és usada per contribuir al manteniment i moderació dels seus serveis com fa OpenAI. Com hem pogut veure a Tor, com que no recopila informació dels seus usuaris, manca de certs serveis que milloren la qualitat de vida dels usuaris, i respecte a la moderació també s'ha pogut comprovar que la llibertat que brinda el navegador no sempre és aprofitada de la millor manera.

La quantitat de dades recopilades també és un aspecte que cal tindre en compte, doncs, en cas de sofrir un ciberatac per una pàgina poc fiable, les dades poden ser robades als serveis, aconseguint informació de l'usuari en qüestió per utilitzar-la de forma il·legítima i perjudicial.

Per tant, com a conclusió final, hem de ser curosos a internet, procurant compartir la menor informació possible i només amb pàgines de confiança, ja que, com demostra la part pràctica d'aquest treball, qualsevol és capaç de crear llocs web maliciosos amb la intenció d'aprofitar-se dels usuaris incauts.

REFERÈNCIES BIBLIOGRÀFIQUES

- Alumnos, A. (s.d.). *Dark Web: riesgos, contenidos y cómo acceder [Guía Práctica]*. LISA Institute. https://www.lisainstitute.com/blogs/blog/dark-web-riesgos-contenidos-como-acceder. (30/07/2025).
- *Confirmed: the new Bing runs on OpenAI's GPT-4*. (s. d.). Bing.com. https://blogs.bing.com/search/march_2023/Confirmed-the-new-Bing-runs-on-OpenAI%E2%80%99s-GPT-4/. (17/08/2025)
- Esteso, M. P. (2015, September 28). *¿Qué es y cómo funciona la red Tor?* Geeky Theory. https://geekytheory.com/que-es-y-como-funciona-la-red-tor/ (17/07/2025).
- Gallagher, N. [Nicolas]. (2018, 5 de novembre). *normalize.css.* GitHub. https://github.com/necolas/normalize.css/. (08/12/2025)
- *Gestionar les gravacions d'àudio a Activitat al web i en aplicacions*. (n.d.). Google.com. https://support.google.com/websearch/answer/6030020?hl=ca. (08/07/2025)
- *Instagram*. (2025, 16 de juny). Instagram. https://privacycenter.instagram.com/policy/. (31/07/2025)
- *Política de privacidad*. (2024, 4 de desembre). Tiktok.com. https://www.tiktok.com/legal/page/eea/privacy-policy/es. (02/08/2025)
- *Política de privacidad*. (s. d.). Tiktok.com. https://www.tiktok.com/legal/page/row/privacy-policy/es. (02/08/2025)
- *Política de privacitat*. (2024, 4 de novembre). Openai.com. https://openai.com/ca-ES/policies/eu-privacy-policy/. (17/08/2025)
- *Política de Privadesa – Privadesa i condicions – Google*. (2025, 1 de juliol). Google.com. https://policies.google.com/privacy?hl=ca. (07/07/2025)
- *Qué es una filtración de datos y cómo prevenirla*. (2024, 15 d'abril). *Kaspersky.es*. https://www.kaspersky.es/resource-center/definitions/data-breach. (24/10/2025)
- Tor Project Inc. (s.d.-a). *Censorship circumvention*. Support. https://tb-manual.torproject.org/bridges/. (28/07/2025)

- Tor Project Inc. (s.d.-b). *Support*. Support. http://support.torproject.org. (22/07/2025)
- Tor Project Inc. (s.d.-c). Torproject.org. https://support.torproject.org/es/tbb/privacy-policy/. (22/07/2025)
- *Treball de recerca*. (s. d.). Xtec.cat. https://agora.xtec.cat/iespuigcargol-calonge/treball-de-recerca/. (06/12/2025)
- (S. d.). Perplexity.ai. https://www.perplexity.ai/help-center/en/articles/10352155-what-is-perplexity. (17/08/2025)