CSI-COP

Científics ciutadans que investiguen el compliment del RGPD de les *cookies* i aplicacions

MOOC CSI-COP: *El teu dret a la privacitat en línia*

En línea_v2

ÍNDEX

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

MOOC

El curs gratuït d'aprenentatge informal de CSI-COP (curs *online* massiu i obert —MOOC—) pot dur-se a terme en línia o descarregant-lo com a document. El temps estimat per a la seva realització és d'unes 2,5-3 hores.

Aquest MOOC tracta del de **les teves dades i el teu dret a la privacitat en línia**. A Internet, les teves dades es recopilen a través de tecnologies digitals de llocs web o aplicacions (programes de *software* dels dispositius mòbils). Aquestes tecnologies inclouen *cookies*; petits arxius de text que, en visitar una pàgina a Internet, s'emmagatzemen en els ordinadors d'escriptori, portàtils o dispositius intel·ligents (com tauletes o telèfons mòbils). Les *cookies* poden incloure rastrejadors digitals, com ara el seguiment de la ubicació precisa del teu dispositiu. La configuració de l'aplicació també pot tenir permisos per accedir als teus contactes, a la càmera, als missatges, al micròfon i a altres dades dels teus dispositius mòbils. La ubicació d'un dispositiu pot identificar la persona que utilitza o és propietària del dispositiu, de manera que el seu rastreig té implicacions en relació a la protecció de dades i la privadesa.

El projecte finançat per CSI-COP EU Horizon2020 té com a objectiu principal educar informalment al gran públic en les tecnologies de rastreig en línia i en la seva desactivació, de manera que aquest públic pugui convertir-se, si ho desitja, en «científic ciutadà». Un científic ciutadà (CC) és un membre de la població general involucrat en la recopilació i anàlisi de dades, com a part d'un projecte de col·laboració amb científics professionals. L' objectiu de CSI-COP és involucrar els científics ciutadans perquè es **s'uneixin a l' equip de el projecte CSI-COP** per investigar fins a quin punt el rastreig (*tracking*) es realitza de manera predeterminada a Internet. El reglament general de protecció de dades (**RGPD**) de 2018 ofereix una llista de verificació amb la qual es pot avaluar el seu compliment. L'equip de CSI-COP creu que el enfocament des de la ciència ciutadana és necessari per forjar la col·laboració entre ciutadans i científics i investigar fins a quin punt els nostres dades són rastrejades en línia a través dels llocs web que visitem i de les aplicacions que fem servir.

Per a qui és aquest curs?
Aquest curs s'adreça a qualsevol persona major d'edat que estigui interessada en comprendre de quina manera les nostres dades es recullen a través d'Internet i per mitjà de les aplicacions que fem servir, i que vulgui aprendre com protegir la seva privacitat en línia.

Què necessites per a realitzar aquest curs?
Un *smartphone*, tauleta, ordinador portàtil o d'escriptori amb connexió a Internet. Si accedeixes a la xarxa wifi d'una universitat o biblioteca, has de tenir en compte que els beneficis d'una xarxa wifi pública i gratuïta comporten el risc que els pirates informàtics puguin accedir a les teves dades. Consulta la informació de Kaspersky sobre com evitar riscos en les xarxes públiques de wifi aquí: https://bit.ly/3v6thff

Si utilitzes Twitter
Al final de cada secció (pas), et fem una proposta de tuit que pots enviar a tercers per fer-los saber que estàs duent a terme el curs d'aprenentatge informal de CSI-COP. Si ho desitges, també pots etiquetar a CSI-COP: @cop_csi.

Consulta els detalls del curs a la pàgina 3, i realitza tots els exercicis dels passos 1, 2, 3, 4 i 5 que trobaràs a partir de la pàgina 4.
A cada pas es fa una breu introducció dels objectius d'aprenentatge i del contingut de la secció i, per tal d'ampliar informació, al final de cada etapa, hem posat a la teva disposició un apartat amb propostes de lectura addicional, on trobaràs enllaços a una sèrie de material juntament amb el nom dels seus autors.
Per tal de millorar el teu aprenentatge i comprensió del curs, respon a la ***pregunta clau*** de cada pas, que t'invita a considerar una qüestió sobre un tema abans d'aprendre més sobre el particular.

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

Pots discutir la pregunta clau (i altres) amb els teus familiars i amics, o parlar amb d'altres persones al fòrum que trobaràs a la web de CSI-COP (et caldrà registrar-te prèviament en el següent enllaç: https://csi-cop.eu/citizenscientistlogin/).

Després de cada pas, també podràs avaluar el teu aprenentatge gràcies a una sèrie d'exercicis relacionats. I, en finalitzar la darrera secció, trobaràs un apartat per revisar tot el curs, així com la informació necessària per poder unir-te a l'equip CSI-COP i convertir-te en científic ciutadà, investigar sobre la privadesa en línia i ser un **defensor de la privacitat**.

Esperem que gaudeixis molt del curs!

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

DETALLS DEL CURS

MOOC CSI-COP: un curs d'autoaprenentatge informal	El teu dret a la privacitat en línia
Objectius del MOOC	El curs en línia gratuït de CSI-COP està dissenyat en **cinc passos.** Completar cada pas et proporcionarà els coneixements necessaris per prendre decisions informades sobre el teu dret a la privacitat en línia i per dotar-te de les habilitats necessàries per cercar i bloquejar les tecnologies de rastreig a Internet i en les aplicacions dels teus dispositius Android (per exemple, mòbils o tauletes Samsung). Un cop completat el curs, podràs sol·licitar un certificat d'educació informal CSI-COP. I, seguidament, podràs passar de ser un estudiant informal a convertir-te en un científic ciutadà voluntari que s'uneixi a l'equip CSI-COP per investigar fins a quin punt es fa un seguiment de les teves dades a través d'Internet (més informació al pas 5). **https://cordis.europa.eu/project/id/873169**
Què pots esperar d'aquest curs *(objectius d'aprenentatge)*	1) Adquisició de coneixements sobre la privadesa acordats als estatuts de drets humans. 2) Habilitats pràctiques (*coneixements tècnics*) per descobrir les tecnologies de rastreig en línia integrades en llocs web i en aplicacions d'Android. 3) Informació sobre com convertir-se en un científic ciutadà i com unir-se a l'equip de CSI-COP per investigar l'abast del rastreig en línia a través de les tecnologies de rastreig digital.
Durada del curs	El curs està dissenyat per poder ser realitzat de les maneres següents: • Realització dels cinc passos en una sola sessió —tant a nivell teòric com pràctic— en unes **2,5 o 3 hores.** • Al teu ritme.
Detalls del curs d'aprenentatge informal	
Títol	*Protegeix les teves dades*
Objectius i resum	Aquest curs- taller està dissenyat per a ser completat en mig dia i d'una sola vegada. No obstant això, pots esglaonar els passos d'aprenentatge per adaptar-los a la teva disponibilitat. En aquest curset en línia, comprendràs de manera integral les diferents facetes de la privacitat i quina relació té tot plegat amb la forma com les teves dades personals poden ser emprades per part de tercers durant la teva interacció en línia en llocs web i durant l'ús d'aplicacions. Així mateix, aprendràs com prendre decisions informades sobre les teves dades personals i com verificar la transparència en la manera en què es recopilen.
Què aprendràs *(resultats de l'aprenentatge)*	**Resultats d'aprenentatge previstos en aquest curs:** 1. Descriure i analitzar les diferents facetes de la privacitat. 2. Identificar i avaluar la manera com es recopilen dades personals durant la navegació per Internet i l'ús d'aplicacions en dispositius intel·ligents. 3. Comprendre els drets a la privacitat resultants dels estatuts per a la protecció de dades.
Contingut del curs	• La privacitat i les seves diferents facetes

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

	• Què són les dades personals? • Com es recopilen les dades personals a través del nostre ús d'Internet? • Dret a la privacitat (ONU; EU; RGPD) • Protecció de les dades personals en línia

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

PAS 1

Títol pas 1:	**Diferents facetes de la privacitat**
En aquest pas aprendràs a:	1.Descriure i analitzar les diferents facetes de la privacitat.
Tema	La privadesa i les seves diferents facetes
Pregunta clau	*La privacitat és un privilegi o un dret humà?* Pregunta als teus familiars i amics què pensen de la **privadesa**. Pots compartir els vostres punts de vista (teus i dels teus contactes) al fòrum de la web de CSI-COP (https://csi-cop.eu/forum/). Per tal de publicar al fòrum, caldrà que et registris a la web i iniciar sessió mitjançant aquest enllaç: https://csi-cop.eu/citizenscientistlogin/.
Resum breu	Jan Holvast (2009) «La discussió sobre qüestions de privacitat és tan antiga com la humanitat» . (Consulta l'apartat de lectures addicionals al final d'aquest pas).
Contingut	**Breu història de la «privacitat»** Segons Jan Holvast (2009), «la discussió sobre qüestions de privacitat és tan antiga com la humanitat . Començant per la **protecció de el cos i la llar propis,** aquesta aviat va evolucionar cap al **control de la informació personal**».  El 1890, Warren i Brandeis van escriure: «que l'individu hagi de tenir protecció total en relació a la seva persona i a les seves possessions és un principi tan antic com el dret consuetudinari», i també : «en temps molt primerencs, la llei només resolia les ingerències físiques en la vida i la propietat» . I van afegir que «ara [el 1890], el dret a la vida ha passat a significar... el dret a viure tranquil», mentre que «el terme "propietat" ha crescut fins a abastar totes les formes de possessió, tant intangibles com tangibles» . El 2001, Nissenbaum va informar que «l'any 2010 va ser un gran any per a la privacitat en línia. Els informes d'errors de privacitat, com ara els relacionats amb Google Buzz o les volubles polítiques de privacitat de Facebook, van aparèixer a les portades dels mitjans de comunicació més destacats. En la seva secció «**What They Know**» (El que saben), *The Wall Street Journal* va alertar sobre el rastreig desenfrenat dels individus en vistes a la publicitat conductual i per altres raons.

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

En relació a l'*ètica de la privadesa*, Marijn Sax (2018) es centra en preguntes com: «**Quin és el valor de la privacitat?**» i «**Quines normes de privadesa han de respectar els individus (inclosos nosaltres mateixos), la societat i l'estat?**».

El 10 d'abril de 2022, el còmic britànic John Oliver al seu programa d'HBO "Last Week Tonight" va posar l'atenció al dany dels "agents de dades" que capturen i ajunten les nostres "molles de dades digitals" en línia per desanonimitzar-nos i vendre les nostres dades a terceres" (a The Guardian, 11 d'abril de 2022). Oliver va informar que els intermediaris de dades són "part d'una indústria multimilionària" que "recull la teva informació personal i després la revenen o la comparteixen amb altres" amb les "eines principals que són les galetes, que permeten als llocs web recordar-te i han evolucionat per incloure't galetes de tercers, que fan un seguiment dels llocs visitats a Internet". (The Guardian). Tornarem a les galetes al pas 3.

Google Chrome

És possible que tinguis activat el mode **incògnit** del navegador Chrome de Google per mantenir la teva privacitat. Tot i així, sembla que Google «recopila en secret grans quantitats de dades d'Internet, fins i tot si els usuaris naveguen en mode "incògnit" per tal de mantenir la privacitat de la seva activitat de recerca» (Nayak i Rosenblatt, 2021). Una notícia de Bloomberg (2021) informa que «uns consumidors han presentat una "demanda col·lectiva" al·legant que "fins i tot amb la recopilació de dades a Chrome desactivada, altres eines de Google utilitzades pels llocs web acaben acumulant la seva informació personal"» (Nayak i Rosenblatt , 2021). Pots obtenir més informació sobre aquest cas en el nou lloc de Bloomberg aquí: https://bloom.bg/3gFt4vV.

Facebook: 533 milions de violacions de dades d'usuaris

Es possible que hagis vist les últimes notícies sobre el fet que no importa si intentem mantenir la nostra informació mínimament privada, perquè, si fem servir les xarxes socials, quedem a disposició del propietari de la plataforma i de la competència per assegurar la nostra privacitat.

Les **dades personals de més de 530 milions d'usuaris de Facebook es van trobar disponibles en un lloc web per a pirates informàtics l'abril de 2021** (Holroid, 2021). La informació personal dels 533 milions de persones afectades inclou usuaris de Facebook ens els següents països:

—Més de 35 milions a Itàlia,
—més de 32 milions a EE.UU.,
—gairebé 20 milions de comptes a França,
—11 milions d'usuaris al Regne Unit i
—6 milions d'usuaris a la Índia.

Lomas (2021) informa que el bolcat de dades (de la informació que els usuaris de Facebook han compartit en aquesta plataforma) inclou:

—IDs de Facebook,
—noms complets,
—números de telèfon,
—ubicacions,
—dates de naixement,
—biografies i
—algunes adreces de correu electrònic.

Pots llegir més sobre el tema a: TechCrunch.

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

Si ets usuari de Facebook i vols esbrinar si la teva informació està inclosa en aquesta violació de dades de Facebook, ho pots comprovar ja sigui mitjançant el teu correu electrònic, la teva ID de Facebook o el teu número de telèfon a les següents pàgines web:

- Have I been pwned? (M'han enganyat?). Aquí: https://haveibeenpwned.com/
- Have I been Zucked? (M'han «absorbit»?). Aquí: https://haveibeenzucked.com/

També pots seguir els tuits de The Real Facebook Oversight Board, «fer que Facebook reti comptes», a Twitter: https://twitter.com/FBoversight

Potser heu sentit el nom de Frances Haugen. És científica de dades i antiga empleada de Facebook. Haugen va donar testimoni al Senat dels Estats Units el 5 d'octubre de 2021, al parlament del Regne Unit el 25 d'octubre de 2021 i al parlament europeu el 8 de novembre de 2021. Haugen va exposar l'estratègia de beneficis de Facebook sobre el benestar dels usuaris (llegiu més sobre la defensa de Frances Haugen per la "responsabilitat i transparència a les xarxes socials" al seu lloc web: https://www.franceshaugen.com/).

La Comissió Irlandesa de Protecció de Dades "va imposar una multa de 17 milions d'euros a Meta Platforms Ireland Limited per una sèrie d'infraccions de dades entre el 7 de juny de 2018 i el 4 de desembre de 2018" (Des d'aquí: https://bit.ly/3MmUIKN).

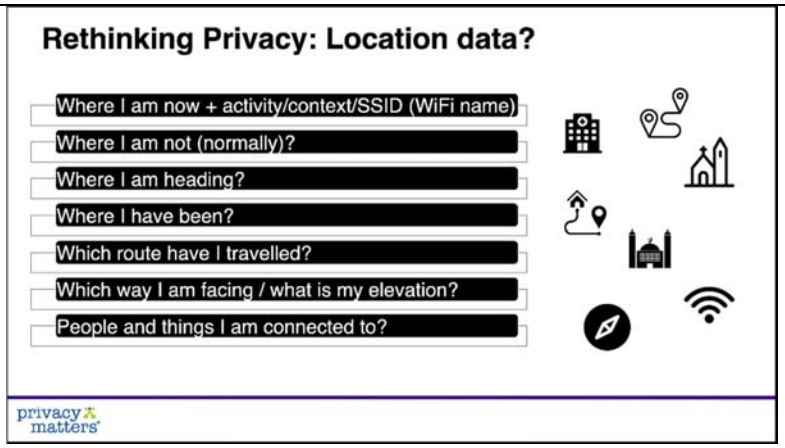
Christopher Wylie, antic científic de dades de Cambridge Analytica i autor del llibre de 2019 "MindF*ck: Inside Cambridge Analytica's Plot to Break the World" afirma: Facebook té massa poder sense control" (pàgina 225).

El 2021, el Tribunal de Districte dels Estats Units del Districte Sud de Nova York va presentar una acció civil: Google Digital Advertising Antitrust. El paràgraf 175 de la pàgina 64 del document judicial dels EUA diu:
"Google presenta una imatge pública de la preocupació per la privadesa, però darrere de les escenes Google es coordina estretament amb les empreses Big Tech per pressionar el govern perquè retardi o destrueixi les mesures que realment protegeixin la privadesa dels usuaris" (d'Acció Civil núm.: 1:21-md-03010-PKC document accessible des de courtlistener.com).

Carissa Veliz, autora del llibre de 2020 'Privacy is Power' adverteix:

- Internet es finança principalment per la recollida, l'anàlisi i el comerç de dades... l'economia de les dades" (pàgina 1)
- "Gran part d'aquestes dades són dades personals: dades sobre tu" (pàgina 1)
- "... telèfon intel·ligent.... Enregistrant el teu viatge i quant de temps hi vas estar...". (pàgina 2)
- "L'economia de les dades, i la vigilància omnipresent de la qual s'alimenta, ens va agafar per sorpresa" (pàgina 2)

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

	 Traducció: Repensar la privacitat: Què passa amb les dades d'ubicació? On soc ara + activitat / context / SSID (identitat de la wifi) On no estic (normalment)? On vaig? Quin trajecte he recorregut? Amb qui i amb què he connectat? <u>Què esperar dels propers passos del curs</u> En el següent punt (pas 2) començarem a fixar-nos en la informació i les *dades personals*. En el tercer pas, veurem *com es realitza el rastreig de les nostres dades*. En el quart, veurem quins *drets tenim sobre la nostra privacitat*. I en l'últim punt d'aquest curs, el pas 5, descobrirem *quines eines en línia* podem utilitzar per *assegurar millor la nostra privacitat i protegir les nostres dades*. <u>Revisa el teu aprenentatge</u> Comprova el que has après en aquest pas responent la pregunta següent i realitzant els exercicis proposats a continuació.
Revisa el teu aprenentatge	Què es la *privacitat*?
Exercicis	**Exercici 1** La següent afirmació és vertadera o falsa? «El debat sobre la privacitat és nou, des de la invenció de Facebook». **Exercici 2:** Discuteix el concepte de privacitat amb la família, amics, veïns o companys de treball. Què has après del que entens per privacitat i del que en pensen altres? Recordatori: pots compartir els vostres punts de vista (teus i dels teus contactes) al fòrum de la web de CSI-COP (https://csi-cop.eu/forum/). Per tal de publicar al fòrum, caldrà que et registris a la web i iniciar sessió mitjançant aquest enllaç: https://csi-cop.eu/citizenscientistlogin/.
Objectiu dels exercicis	Entendre les *facetes de la privadesa*.
Proposta de tuit	En l'era de l'accés mòbil a Internet, hauria d'importar més la comoditat que la privacitat?

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

Lectures addicionals per al pas 1	Els enllaços a les lectures addicionals esmentades en aquest punt es poden consultar clicant el text subratllat. **Lectures recomanades** —Lomas, N. (2021). *Answers being sought from Facebook over latest data breach*. Tech Crunch. Pots llegir l'article en anglès aquí: https://tcrn.ch/3xfrTsE —Nayak, M. i Rosenblatt, J. (2021). *Google Must Face Suit Over Snooping on 'Incognito' Browsing* Bloomberg Technology. Pots llegir l'article en anglès aquí: https://bloom.bg/3gFt4vV —The Real Facebook Oversight Board (el compte de la Junta de Supervisió de Facebook). Compte de Twitter: @Fboversight (https://twitter.com/FBoversight) **Lectures addicionals** —Holroyd, M. (2021). «Ireland launches data protection inquiry into Facebook hack». *Euronews – Ireland*. Pots llegir l'article en anglès aquí: https://bit.ly/3mOfIOM —Holvast, J. (2009). «History of Privacy». En V. Matyàš et al. (Eds.): *The Future of Identity*, IFIP AICT 298, pàgs. 13-42, 2009. IFIP International Federation for Information Processing 2009. Pots llegir-lo en anglès a ResearchGate: https://www.researchgate.net/publication/225802214_History_of_Privacy —Nissenbaum, H. (2011). «A Contextual Approach to Privacy Online». *Dædalus, Journal of the American Academy of Arts & Sciences*, Vol. 140, Nº. 4 (Tardor 2011), pàgs. 32-48. Pots llegir l'article en anglès aquí: https://www.amacad.org/publication/contextual-approach-privacy-online —Guardian (2022). *John Oliver on Data Brokers: What they can buy is pretty troubling*. Guardian Culture. 11 April 2022: https://bit.ly/3wzX0j3 —Sax, M. (2018). «Privacy from an Ethical Perspective». Capítol a: B. Van der Sloot & A. De Groot (Eds.), *The Handbook of Privacy Studies: An Interdisciplinary Introduction* (pàgs. 143-173). Amsterdam: Amsterdam University Press. Pots llegir l'article en anglès aquí: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3299047 —Warren, S.D. & Brandeis, L.D. (1890). «The Right to Privacy». *Harvard Law Review*, Vol. 4, núm. 5. (Dic. 15, 1890), pàgs. 193-220. Pots llegir l'article en anglès si segueixes aquest enllaç: The Right to Privacy on JSTOR

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

PAS 2

Títol pas 2:	**Informació i dades personals**
En aquest pas aprendràs a:	1.Descriure i analitzar les diferents facetes de la privacitat.
Tema	Què són les dades personals?
Pregunta clau	*Per què hauria d'importar qui té accés a les meves dades si no tinc res a amagar?* Pregunta als teus familiars i amics què pensen sobre les seves dades. Pots compartir els vostres punts de vista (teus i dels teus contactes) al fòrum de la web de CSI-COP (https://csi-cop.eu/forum/). Per tal de publicar al fòrum, caldrà que et registris a la web i iniciar sessió mitjançant aquest enllaç: https://csi-cop.eu/citizenscientistlogin/.
Resum breu	Andreas Weigend (2017): «Cada vegada que busquem alguna cosa a Google, contactem amb algú a través de Facebook, demanem un Uber en algun lloc o fins i tot si simplement encenem una llum, generem dades que les empreses recopilen». (Consulta la secció de lectura s addicional al final d'aquest pas).
Contingut	**Què són les dades (*data*)?** Recapitulació : en el primer pas hem introduït el concepte de «privacitat». En aquesta segona etapa del curs d' educació informal de CSI-COP, comprendràs «què són les dades (*data*)» i quines «dades sobre tu» resulten involucrades en diferents moments de la teva vida a la xarxa; ja sigui en comprar per Internet, enviar missatges a amics o durant la recerca d' informació, entre d'altres. En anglès, el singular de «*data*» (dades) és «*datum*»: • Una única porció de *qualitat* o *quantitat* sobre alguna cosa. «*Data*», en anglès, és un nom col·lectiu (més que un sol ítem): • Punts d'informació. Per exemple, *dades sobre tu*: —Si ets estudiant (tant si ets estudiant «local» com internacional) —Data de naixement —Qualificacions per aconseguir plaça a la universitat —Adreça postal (de la llar o la residència habitual durant el curs) —Número de contacte —... Les dades («*data*») es troben a tot arreu i s'emmagatzemen de diferents maneres: • *Sense estructurar*: —Visionat de vídeos de YouTube —Consulta de les imatges d'Instagram —Lectura de correus electrònics —Imatges per satèl·lit —Dades meteorològiques —... • Estructurades: —Número d'identificació de l'estudiant o personal (cadena de números) —Número de la Seguretat Social

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

—Reserves aèries

—...

	Structured Data	Unstructured Data
Characteristics	• Pre-defined data models • Usually text only • Easy to search	• No pre-defined data model • May be text, images, sound, video or other formats • Difficult to search
Resides in	• Relational databases • Data warehouses	• Applications • NoSQL databases • Data warehouses • Data lakes
Generated by	Humans or machines	Humans or machines
Typical applications	• Airline reservation systems • Inventory control • CRM systems • ERP systems	• Word processing • Presentation software • Email clients • Tools for viewing or editing media
Examples	• Dates • Phone numbers • Social security numbers • Credit card numbers • Customer names • Addresses • Product names and numbers • Transaction information	• Text files • Reports • Email messages • Audio files • Video files • Images • Surveillance imagery

Font de la imatge: https://bit.ly/2PhkKHa

Traducció de la imatge:

	Dades estructurades	Dades no estructurades
Característiques	Models de dades predefinides —Generalment només text —Fàcils de cercar	Models de dades no predefinides —Pot tractar-se de textos, imatges, arxius d'àudio o vídeo o altres formats —Difícils de cercar
Emmagatzemades en	—Bases de dades relacionals —Magatzems de dades	—Aplicacions —Bases de dades NoSQL —Magatzems de dades —*data lakes*
Generades per	—Humans o màquines	—Humans o màquines
Aplicacions més freqüents	—Sistemes de reserva de vols —Control d'inventari —Sistemes de gestió de la relació amb els clients —Sistemes de planificació de recursos empresarials	—Processament de textos —*Software* de presentacions —Enviament de correus electrònics als clients —Eines per a la visualització o edició de mitjans
Exemples	—Dates —Números de telèfon —Números de la Seguretat Social —Números de targetes de crèdit —Noms de clients —Adreces postals	—Arxius de text —Informes —Missatges de correu electrònic —Arxius de so —Arxius de vídeo —Imatges —Imatges de càmeres de vigilància

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

	—Noms i referències de productes —Informació sobre transaccions	

Segons Irwin (2021): «En determinades circumstàncies, qualsevol de les següents poden considerar-se *dades personals*»:
—Un nom i cognom
—Una adreça postal
—Una adreça de correu electrònic
—Un número de targeta d'identificació
—Dades de localització
—Una adreça de Protocol d'Internet (IP)
—L'identificador de publicitat del teu telèfon.

Les dades personals són dades que identifiquen una persona «física» (viva).

Pat Walshe de **Privacy Matters** (Afers de Privacitat) diu: «Fem servir els nostres telèfons intel·ligents i ordinadors com mai abans per fer trucades; enviar missatges de text i imatges personals; enviar missatges a la gent a través dels serveis de WhatsApp o Snapchat; comprar aliments o medicines en línia; compartir facetes personals de les nostres vides a les xarxes socials; buscar informació sobre salut mental o física, política, religió o llocs per visitar; navegar per llocs web; deixar comentaris i indicar el que ens agrada i el que no; etc. Ser digital genera una gran quantitat de dades sobre nosaltres, sovint personals i sensibles. Dades que poden permetre que altres ens coneguin millor que nosaltres mateixos» (Privacy Matters).

Podem **oferir dades voluntàriament** quan fem una comanda en línia o agendem una cita mèdica, i també **es poden capturar i observar les nostres dade**s i dels nostres dispositius i comportament en línia (com les pàgines web que visitem, les cançons que escoltem o les pel·lícules que veiem, el tipus de dispositiu que fem servir o la nostra ubicació —essent-ne nosaltres conscients o no—). Les dades es poden **deduir** quan creem un perfil i s'analitza la nostra informació (com ara quin usuari va escoltar una cançó o veure una pel·lícula en línia, la categoria de la cançó o pel·lícula, en quin punt una persona va aturar una cançó o una pel·lícula, juntament amb la data i el moment en què es va fer la pausa i es va reiniciar o es va deixar d'escoltar o mirar, la ubicació en la qual estava —el país, com a mínim...—, etc.); dades, totes elles, que són com una mena d'ombra digital de les activitats en línia (Privacy Matters).

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

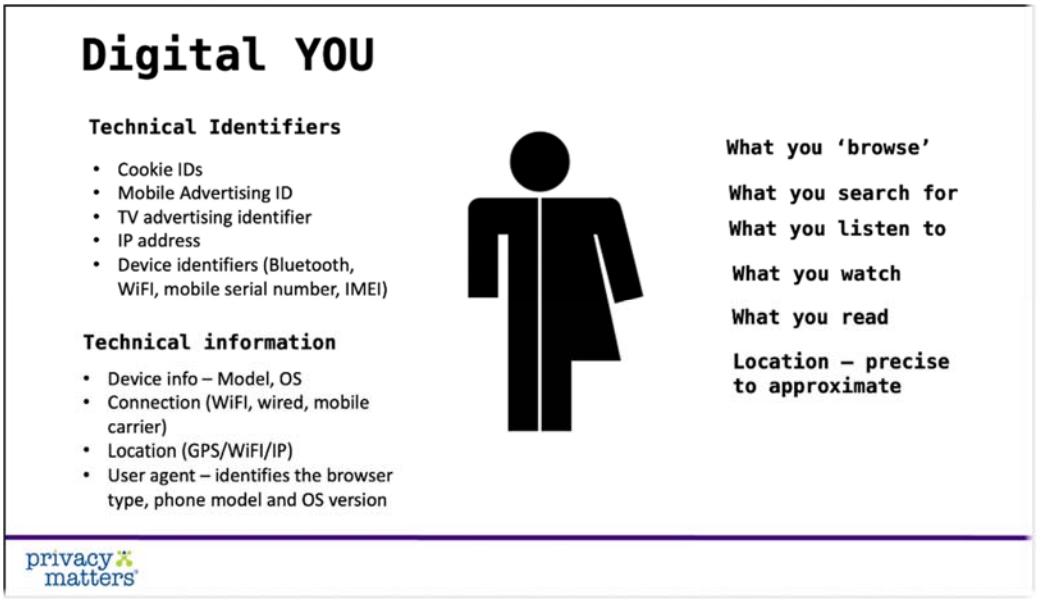
A més de les dades personals, també hi ha **dades personals sensibles**. Segons el reglament general de protecció de dades (RGPD), sobre el qual aprendrem més en el pas 4, les **dades personals confidencials** poden incloure dades que revelin:

- origen racial o ètnic
- creences religioses
- opcions polítiques
- afiliacions sindicals

Les dades personals sensibles també inclouen dades sobre la salut d'una persona (mental o física, per exemple); dades sobre la seva vida sexual o orientació sexual; dades genètiques; dades biomètriques (utilitzades per identificar de forma única a algú) i dades relacionades amb condemnes i delictes penals (Privacy Matters).

L'abril de 2021, Brodkin (2021) va informar que T-Mobile:
«iniciarà un nou programa que utilitzarà algunes de les dades que tenim sobre vostè (...) *incloent-hi la informació que obtenim de les dades d'ús de la web i del seu dispositiu* (com les aplicacions que hi té instal·lades) (...) i de les interaccions amb els nostres productes i serveis, per a ús publicitari propi i de tercers, a no ser que ens indiqui el contrari».

Com et sentiries si el teu operador de telefonia mòbil t'informés que actuaran com T-Mobile? O, si fas servir T-Mobile, com et fa sentir la seva declaració sobre la recopilació i ús de les teves dades?



Traducció de la imatge: EL TEU JO DIGITAL

Identificadors tècnics
—ID de *cookies*
—ID de publicitat mòbil
—ID de publicitat televisiva
—Adreça IP
—Identificador de dispositius (Bluetooth, wifi, número de sèrie del mòbil, IMEI)

Informació tècnica

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

	—Informació de dispositiu (model, sistema operatiu) —Connexió (wifi, cable, operador de telefonia mòbil) —Ubicació (GPS, wifi, IP) —Agent d'usuari (identifica el tipus de navegador, model de telèfon i sistema operatiu) Per on navegues? Què busques? Què escoltes? Què mires? Què llegeixes? On ets? (Ubicació més o menys precisa) <u>Què esperar dels propers passos del curs</u> A l'etapa següent (pas 3), començarem a veure *com es rastregen les nostres dades*. En el pas 4, veurem quins *drets tenim sobre la nostra privacitat* i, en el darrer punt (pas 5), descobrirem quines *eines en línia podem utilitzar per assegurar millor la nostra privacitat i protegir les nostres dades*. <u>Revisa el teu aprenentatge</u> Comprova el que has après en aquest pas responent la pregunta següent i realitzant els 2 exercicis proposats a continuació.
Revisa el teu aprenentatge	Què són les *dades personals*?
Exercicis	**Exercici 1: test curt** Quins dels següents noms es relacionen amb les dades personals? • Leonardo da Vinci • El president Joe Biden • Freddie Mercury • La reina Elizabeth II • Alan Turing • Meghan Markle • Albert Einstein • El Papa • Kim Kardashian (La resposta a aquesta activitat la trobaràs al pas següent) **Exercici 2** Busca i mira les xerrades TED del «tec-sociòleg» **Zeynap Tufekci**. Per exemple, la seva intervenció al TED Global NYC, de setembre de 2017: «Estem construint una distòpia només perquè la gent faci clic als anuncis». Recordatori: Pots compartir els teus punts de vista al fòrum de la web de CSI-COP (https://csi-cop.eu/forum/). Per tal de publicar al fòrum, caldrà que et registris a la web i iniciar sessió mitjançant aquest enllaç: https://csi-cop.eu/citizenscientistlogin/.
Objectiu dels exercicis	Entendre *què són les dades personals.*

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

Proposta de tuit	L'afirmació «no tinc res a amagar, així que no m'importa qui tingui accés a les meves dades» és desencertada.

Lectures addicionals per al pas 2	Els enllaços a les lectures addicionals esmentades en aquest punt es poden consultar clicant el text subratllat. **Lectures recomanades:** Brodkin, J. (2021). *T-Mobile will sell your web-usage data to advertisers unless you opt o*ut. arsTECHNICA. Pots llegir l'article en anglès aquí: https://bit.ly/3sUdkaQ Irwin, L. (2021). *Personal data vs. sensitive data: what's the difference?* IT Governance. Pots llegir l'article en anglès aquí: https://bit.ly/3vhoRIX Privacy Matters a Twitter: @PrivacyMatters: https://twitter.com/privacymatters?lang=en Llibre en anglès: Weigend, A. (2017). *Data for the people: how to make our post-privacy economy work for you*. Basic Books: New York

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

PAS 3

Títol pas 3:	**Tecnologies de rastreig en línia**
En aquest pas aprendràs a:	1. Descriure i analitzar les diferents facetes de la privacitat. 2. Identificar i avaluar la manera com es recopilen dades personals durant la navegació per Internet i l'ús d'aplicacions en dispositius intel·ligents.
Tema	Com es recopilen les dades gràcies al nostre ús d'Internet?
Pregunta clau	*Com de perilloses poden ser les tecnologies de rastreig en línia?* Pregunta als teus familiars i amics què pensen de les seves dades. Pots compartir els vostres punts de vista (teus i dels teus contactes) al fòrum de la web de CSI-COP (https://csi-cop.eu/forum/). Per tal de publicar al fòrum, caldrà que et registris a la web i iniciar sessió mitjançant aquest enllaç: https://csi-cop.eu/citizenscientistlogin/.
Resum breu	Nigel Warburton (2020): «Sense el teu permís (...), les empreses de tecnologia recopilen les teves dades —la teva ubicació, el que t'agrada, els teus hàbits, les teves pors, les teves malalties, les teves idees polítiques...— i les comparteixen entre elles». (Consulta la secció de lectures addicionals al final d'aquest pas).
Contingut	**Com es recopila la teva informació a Internet** Resum del què hem après en els dos passos anteriors: • En el primer pas hem introduït el concepte de «privacitat». • En el segon pas hem après que l'expressió «dades personals» fa referència a les dades sobre una persona física (i viva). En aquest punt veurem alguna de les eines en línia que recopilen dades mentre fem servir internet. La *product manager* Eliza Crawford (2020) indica que la raó per la qual es recopilen les nostres dades a través d'Internet és per saber com ens comportem quan visitem una web. I això es fa per «obtenir informació sobre com (...) els consumidors fan servir» els llocs web «per, així, proporciona-los una experiència personalitzada en línia i monetitzar l'usuari mostrant-li anuncis dirigits». En explicar per què es produeix el rastreig en línia, Crawford (2020) diu: • «Quan busques un restaurant a Google i el servei et proporciona una llista de restaurants propers, és perquè el motor de cerca sap on et trobes». • «Quan una botiga de comerç electrònic et mostra una llista de productes recomanats, sap el que t'agrada perquè ha fet un rastreig dels ítems que has mirat o comprat prèviament». Pat Walshe (Privacy Matters) recorda que **les dades de comportament** poden incloure: • Les teves **dades de navegació**; és a dir**,** els llocs web que visites, la data i l'hora en què ho fas i el país des d'on ho fas (deduït de la teva adreça IP —una cadena única de caràcters que identifica cada dispositiu que es connecta a Internet i que s'envia automàticament en visitar una pàgina web-—). També cal tenir en compte que, quan s'abandona un lloc web, els propietaris d'aquest lloc podran saber quina web es visita

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

a continuació (i aquests últims saber de quin lloc es ve). Tot això es consideren «dades de comportament de navegació web».

- **Comportament *Clickstream* (flux de clics)**; dades sobre les interaccions d'una persona en un lloc web, que poden incloure on fa clic, per on es desplaça dins el lloc web i què toca en una pantalla tàctil.
- **Motors de cerca** com Google que poden emmagatzemar informació sobre les teves cerques, els resultats en què fas clic o la teva adreça IP, i que poden utilitzar una ID exclusiva de *cookie* per rastrejar-te.
- **Ubicació**; és a dir, la localització i el tipus de llocs que es visiten (supermercat, casino, lloc de culte, hospital ...), o el lloc on s'ha utilitzat l'aplicació, dates i hores, trajecte recorregut, la freqüència d'una visita, etc. Les dades d'ubicació / localització poden ser molt reveladores i de naturalesa conductual.
- **Historial de compres**; pot incloure diferents tipus de subscripcions (membre d'un sindicat, gimnàs, diaris, etc.), reserves a hotels o restaurants que s'hagin realitzat mitjançant la recerca, mapes o assistents virtuals o directament mitjançant els venedors o serveis de tercers.
- **Dades de pagament o informació transaccional**; és a dir, els pagaments que revelen a qui o a quines organitzacions s'ha pagat (fet que pot informar sobre el tipus d'organització receptora —clínica, farmàcia, proveïdor d'alcohol, establiment d'aliments, llibreria, etc.), i quant, quan i amb quina freqüència s'ha fet. Un bon exemple d'això són els pagaments amb targeta «tap & go» (un sistema de validació i pagament amb targeta *contactless*); pensa, per exemple, en el cafè que vas comprar a l'inici d'un viatge, el lloc, la data i l'hora en què ho vas fer, i els pagaments que vas fer al llarg del dia amb la mateixa targeta.
- ***Streaming media*** (flux de continguts multimèdia). «Ets el que mires en *streaming* » (pots llegir els articles en anglès: you are what you stream i They know what You watched Last Night —«Saben què vas mirar ahir a la nit»—) .
  Els mitjans en *streaming* generen **moltes** dades de comportament sobre:
  - la data i l'hora en què vas accedir a un servei de música, àudio o TV / pel·lícules en *streaming* i la ubicació no precisa (nivell de país o nivell de regió) des de la qual hi vas accedir,
  - quin perfil va accedir i va utilitzar el servei (nom + categoria —per exemple: nen—) ,
  - la categoria de música, audiollibre, TV / pel·lícula (per exemple: terror polític, adults),
  - les cerques de contingut,
  - si vas parar una cançó o pel·lícula i durant quant de temps (data I hora incloses)
  - si vas saltar o vas abandonar una cançó o l' àudio d'una pel·lícula o d'un episodi,
  - si vas compartir contingut i amb qui, i les teves interaccions amb altres dins del servei,
  - si vas puntuar una cançó, un programa de televisió o una pel·lícula,
  - les llistes de reproducció o visualització creades,
  - el dispositiu emprat per accedir al servei, l'adreça IP i els identificadors del dispositiu.
- **Dades sobre salut i activitat;** dades sobre l'ús d'aplicacions d'activitat física (com les relacionades amb ciclisme, *running* , senderisme, etc.) o dades sobre la teva salut, com les que es poden obtenir mitjançant les aplicacions dietètiques o de fertilitat.
- **Gràfic de xarxes socials**; són dades que revelen les relacions socials interconnectades entre les persones, la seva naturalesa i els patrons de comunicació.

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

Un estudi de Ghostery (2017) «va revelar que els rastrejadors que recopilen dades sobre el comportament en línia dels usuaris d'Internet estan presents en, com a mínim, el 79% dels llocs web (dominis únics) a nivell mundial. El rastreig web s'ha tornat tan omnipresent que aproximadament el 10% dels llocs web envien les dades recopilades a deu o més empreses diferents (dominis de rastreig únics). En termes de trànsit web, hi ha uns deu (o més) rastrejadors que controlen el 15% de totes les càrregues de pàgines a Internet. Segons l'estudi, els *scripts* de rastreig de Google (60,3% de les càrregues de pàgina) i Facebook (27,1%) són els més freqüents».

Aquest rastreig es realitza mitjançant eines digitals com ara:

Hem sentit a parlar de les galetes al Pas 1, del programa John Oliver, d'HBO, del 10 d'abril de 2022: "Last Week Tonight" on exposava als "Data Brokers".

Cookies: Les *cookies* són petites porcions d'informació que els llocs web emmagatzemen en el dispositiu de l'usuari. Els llocs web solen **utilitzar les *cookies* per recordar les preferències de l'usuari i brindar una experiència personalitzada, així com per obtenir informació amb finalitats publicitàries.** Una vegada que un lloc web ha col·locat una *cookie* a l'ordinador de l'usuari, el proveïdor d'aquesta *cookie* pot seguir accedint-hi. Així és com els llocs web poden utilitzar *cookies* per rastrejar els usuaris d'una pàgina a una altra o d'un lloc a un altre. El temps que una *cookie* pot pot rastrejar un usuari depèn del tipus de *cookie* i aquestes poden ser temporals, persistents, d'origen, de tercers ... (Crawford, 2020).

Empremtes digitals: La presa d'empremtes digitals és una forma de rastreig de llocs web que utilitza els atributs de el dispositiu o navegador de l'usuari per crear un perfil d'usuari. La informació que s'obté mitjançant les empremtes digitals inclouen el dispositiu, el seu sistema operatiu, la resolució de pantalla, el navegador i la versió de navegador, l'idioma i la zona horària. Crawford (2020) afirma: «Per si sola, cada peça d'informació no és gaire valuosa. Ara bé, quan es té tot junt, proporciona una manera increïblement precisa d'identificar els usuaris. L'Electronic Frontier Foundation (EFF)) manté un lloc web per «tapar les petjades» (es pot veure a l'enllaç: cover your tracks), que analitza el teu navegador per mostrar com d'única és la teva empremta digital en relació amb altres empremtes rastrejades pel lloc web».

Rastreig de correu electrònic: El ***software* de rastreig de correu electrònic** (*e-mail tracking*) **posa un píxel d'imatge invisible als correus electrònics que pot detectar la data i l'hora exactes en què s'obre un correu electrònic.** El motiu d'aquest rastreig és que les empreses estalviïn temps i sàpiguen si un primer correu et resulta prou interessant com per

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

obrir-lo. Si no és el cas, és poc probable que obris els seus futurs correus electrònics de seguiment. En evitar correus electrònics de seguiment innecessaris, el rastreig del correu electrònic estalvia temps tant al venedor com a el destinatari del correu electrònic. De la mateixa manera, si una empresa detecta que un contacte fa clic als enllaços enviats i veu una carta de presentació o una proposta adjunta, sap que aquest contacte la té en ment en aquell moment. Arribar a aquest punt en què hom pugui estar pensant en la proposta d'una empresa (per exemple, comprar una peça de roba) fa que la conversa sigui molt més rellevant (i oportuna per a l'empresa / venedor).

L'estudi de Sivan-Sevilla *et al.* (2020) va descobrir que «empreses de les que mai hem sentit parlar recopilen dades de referència sobre tots els aspectes de les nostres vides: els nostres interessos, compres, estat de salut, ubicacions i més». IAB (Interactive Advertising Bureau; 2019, citat a Sivan-Sevilla *et al.*, 2020). «Aquestes dades de referència es combinen després en perfils de comportament excepcionalment reveladors, que exposen parts íntimes de la nostra identitat i alimenten la indústria de la publicitat multimilionària, que afirma predir el que és probable que consumim per poder orientar-nos amb anuncis» .

Sivan-Sevilla *et al.* (2020) informen, a més, que, quan els anunciants creuen informació sobre problemes mèdics, interessos educatius i hàbits de consum de notícies d' usuaris, estan en condicions de saber millor quan un usuari pot convertir-se en consumidor i prendre decisions de compra que els anunciants no podrien predir d'una altra manera. Els estudis van mostrar de quina manera les dades de diferents llocs web s'agrupen i s'utilitzen per inferir sobre la demografia i els interessos dels usuaris, exposant-los a pràctiques manipuladores que intenten fer-los fer clic a l'anunci «correcte» (personalitzat) en el moment «correcte» (personalitzat).
La indústria de la publicitat havia definit aquests moments com «**moments principals de vulnerabilitat dels consumidors**» (...) en què els usuaris són «excepcionalment receptius». Srinivasan (2020) aclareix que: «L'auge dels anuncis electrònics, àmpliament coneguts avui com a "publicitat programàtica", ha estat paral·lel a l'augment del comerç electrònic en diversos sectors de l'economia (...). La primera empresa de tecnologia publicitària, **Right Media**, va llançar l'"intercanvi publicitari" (**RMX,** per les seves sigles en anglès: Right Media Exchange), el **primer lloc de comerç electrònic per a anuncis.** (...) Avui en dia, una sola empresa, **Google**, gestiona simultàniament l'intercanvi principal així com els intermediaris principals que els editors i anunciants han d'utilitzar per comerciar. (...) Google no només ven espais publicitaris que pertanyen a llocs web de tercers, sinó que ven també espai publicitari que apareix en els seus propis llocs, com el motor de cerca de Google i YouTube».

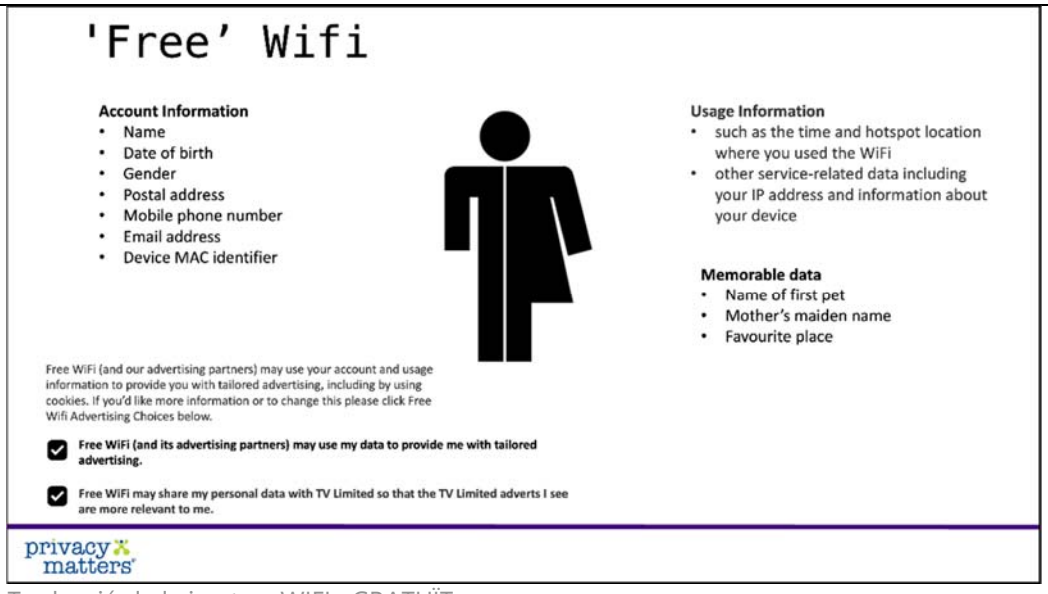
Srinivasan (2020) comenta que «el negoci de la publicitat ha canviat dràsticament en les últimes dues dècades. Avui dia, la categoria de publicitat més important —la publicitat en línia— poques vegades és negociada per persones, ja que els avenços tecnològics permeten que l'espai publicitari es compri i vengui electrònicament a altes velocitats a través de llocs de negociació centralitzats, sense que ningú es reuneixi cara a cara. Així, quan un usuari visita un lloc web, l'espai publicitari d'una pàgina s'enruta instantàniament a un o més d'aquests llocs i, allà, aquest espai publicitari es subhasta en temps real al millor postor. En acabar aquestes subhastes, els anuncis dels anunciants que han obtingut l'espai publicitari es mostren a l'usuari a temps perquè es carregui la pàgina i abans que l'usuari s'adoni que ha passat alguna cosa. L'usuari només veu anuncis dirigits a ell (un de Barclays Bank, per exemple)».

És possible que ara entenguis que cada vegada hi ha una major quantitat de dades capturades, observades i deduïdes per aquells amb qui tens una relació directa, no només

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

	perquè puguin proporcionar-te els serveis bàsics que hagis sol·licitat, sinó cada vegada més per «personalitzar experiències», tant si els ho has demanat com si no, o per enviar-te publicitat dirigida dins i fora dels seus llocs web, aplicacions i serveis. Ara bé, les teves dades no només són capturades, observades i deduïdes per aquells amb qui tens una relació directa, sinó també per tercers de l'ecosistema publicitari que poden estar incrustats en els llocs web que visites o en les aplicacions que utilitzes (per dirigir- publicitat conductual, per exemple). Les teves dades poden ser utilitzades per a seguir-te a través del web i les aplicacions amb finalitats d'orientació conductual (com les ofertes en temps real que permeten als anunciants fer ofertes automàtiques per dirigir-se a un públic concret en funció de criteris específics, com ara un interval d'edat i sexe específics, o tipus de dispositiu mòbil o ubicació). Per tant, les TEVES DADES poden ser molt personals i revelar aspectes íntims de la teva vida. Aquest fet pot afectar-te de maneres que mai havies imaginat, que infringeixin les teves expectatives de privacitat, i que no la respectin ni protegeixin. Per exemple, es va descobrir que l' aplicació Grindr comparteix informació amb una «gran quantitat de tercers» involucrats en la creació de perfils i publicitat. Les dades compartides «inclouen adreça IP, identificador de publicitat, ubicació GPS, edat i sexe». Això va donar lloc a una investigació per part de l'autoritat noruega de protecció de dades que va multar Grindr amb 100 milions de corones (l'equivalent a 8,6 milions de lliures esterlines o uns 10 milions d'euros). Tots els tipus de dades que hem vist fins ara fan referència a dades personals protegides per lleis de protecció de dades, com el RGPD o la llei de privacitat electrònica europea (la de privadesa electrònica —«EPD», per les seves sigles en anglès: ePrivacy Directive—), que discutirem en el següent punt (pas 4) del curs d'aprenentatge informal de CSI-COP. Aquestes lleis imposen obligacions a les organitzacions del sector públic i privat que capturen, observen i dedueixen dades sobre els usuaris i atorguen drets sobre aquest ús. Novament, això també es discutirà en el pas 4 del curs. Però, primer, pren-te un moment i pensa en què diuen les teves dades sobre TU i sobre ALTRES als quals estàs connectat. Així mateix, tingues en compte que, si utilitzes una xarxa wifi gratuïta, et caldrà proporcionar informació personal per accedir a Internet. Observa la imatge següent per veure què es recopila en aquest cas:

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169



Traducció de la imatge: WIFI «GRATUÏT»

Informació de compte
—Nom
—Data de naixement
—Gènere
—Adreça postal
—Número de telèfon mòbil
—Adreça de correu electrònic
—Identificador MAC del dispositiu

Informació d'ús
—Com ara l'hora i la ubicació del punt d'accés o des del qual s'ha accedit a la wifi.
—Altres dades relacionades amb el servei, inclosa la teva adreça IP i informació sobre el teu dispositiu.

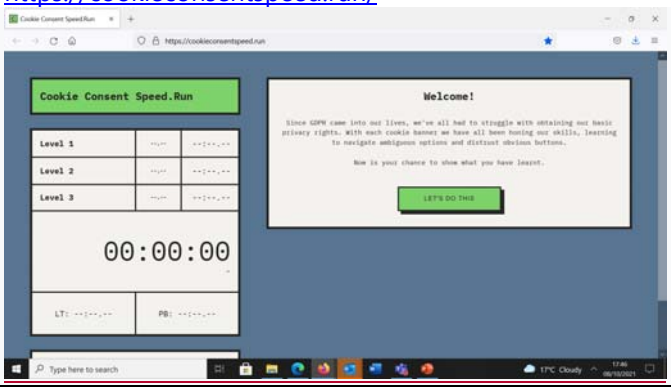
Dades recordatori
—Nom de la primera mascota
—Cognom de la mare
—Lloc favorit
—...

El wifi gratuït (i els nostres socis publicitaris) pot utilitzar el teu compte i la informació d'ús per a mostrar-publicitat personalitzada, fins i tot mitjançant l'ús de *cookies.* Per tal d'obtenir més informació o canviar-ho, fes clic a les opcions de publicitat del wifi gratuït que veuràs a continuació.

* El wifi gratuït i els seus socis publicitaris poden utilitzar les meves dades per proporcionar-me publicitat personalitzada.
* El wifi gratuït pot compartir les meves dades personals amb TV Limited, per tal que els anuncis de TV Limited que vegi siguin més rellevants per a mi.

<u>Què esperar dels propers passos del curs</u>
En el següent punt (pas 4) veurem quins *drets tenim sobre la nostra privacitat.*

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

	Al final d'aquest curs, al pas 5, aprendrem *les eines en línia que* podem emprar per *assegurar* millor *la nostra privacitat i protegir les nostres dades*. <u>Revisa el teu aprenentatge</u> Revisa el que has après en aquesta fase (pas 3). La resposta al primer exercici del pas 2 podràs trobar-la a l'apartat d'exercicis d'aquest cas.
Revisa el teu aprenentatge	Quins són els diferents tipus de *Cookies*? Què és la l'empremta digital? Com funciona el rastreig del correu electrònic?
Exercicis	**Resposta a l'exercici 1 del pas 2** El primer exercici del pas anterior et demanava que identifiquessis quines eren dades personals d'una llista de noms. Atès que les dades personals es refereixen exclusivament a persones físiques (vives), els noms de la llista que fan referència a persones mortes no són dades personals. Ho havies fet bé? Comprova-ho a continuació: • Leonardo da Vinci —no és una dada personal • El president Joe Biden • Freddie Mercury —no és una dada personal • La reina Elizabeth II • Alan Turing —no és una dada personal • Meghan Markle • Albert Einstein —no és una dada personal • El Papa • Kim Kardashian **Pas 3. Exercici 1** 1. Cerca a la web els diferents tipus de *cookies* que es poden incrustar en els llocs web. 2. Quina és la diferència entre la presa d'empremtes digitals i el rastreig de correu electrònic? **Pas 3. Exercici 2** Comenta amb la família, amics, veïns o companys de feina el que enteneu per **«elaboració de perfils de comportament en línia»** i la manera com es fa a través de la web. **Pas 3. Exercici 3** Prova aquest joc en línia gratuït per saber si pots evitar les galetes: https://cookieconsentspeed.run/ 

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

	Recordatori: Pots compartir els vostres punts de vista (teus i dels teus contactes) al fòrum de la web de CSI-COP (https://csi-cop.eu/forum/). Per tal de publicar al fòrum, caldrà que et registris a la web i iniciar sessió mitjançant aquest enllaç: https://csi-cop.eu/citizenscientistlogin/.
Objectiu dels exercicis	Obtenir més informació sobre l'elaboració de perfils de comportament en línia.
Proposta de tuit	Tecnologies de rastreig

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

Lectures addicionals per al pas 3	Els enllaços a les lectures addicionals esmentades en aquest punt es poden consultar clicant el text subratllat. **Lectures recomanades** Crawford, E. (2020). *Website Tracking: Why and How do Websites Track you?* CookiePro Blog: Cookie Compliance. Pots llegir l'article en anglès aquí: https://www.cookiepro.com/blog/website-tracking/ EFF (sense data). *The Electronic Frontier Foundation. The leading non-profit defending digital privacy, free speech, and innovation for 30 years and counting!* Pots llegir l'article en anglès a l'enllaç anterior i consultar la web aquí: https://www.eff.org/ Ghostery (2017). 79 *Percent of Websites Globally Are Secretly Tracking Your Personal Data.* Ghostery. Pots llegir l'article en anglès aquí:https://www.ghostery.com/press/ghostery-global-tracking-study/ Privacy Matters en Twitter: @PrivacyMatters (https://twitter.com/privacymatters?lang=en) **Lectures addicionals** Sivan-Sevilla, I., Chu, W., Liang, X. i Nissenbaum, H. (2020). *Unaccounted Privacy Violation: A Comparative Analysis of Persistent Identification of Users Across Social Contexts*. Federal Trade Commission (FTC) PrivacyCon 2020. Pots llegir l'article en anglès aquí: https://news.cornell.edu/stories/2020/06/study-online-trackers-follow-health-site-visitors Srinivasan, D. (2020). *Why Google Dominates Advertising Markets Competition Policy Could Lean on the Principles of Financial Market Regulation*. 24 STAN. TECH. LAW REV. Pots llegir l'article en anglès aquí: https://law.stanford.edu/publications/why -google-dominates-advertising-markets/ Llibre en anglès: Warburton, N. (2020) coberta interior del llibre de Véliz, C. (2020). *Privacy is Power: Why and how you should take back control of your data*. Penguin Hardback.

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

PAS 4

Títol pas 4:	**El teu dret a la privacitat**
En aquest pas aprendràs a:	1. Descriure i analitzar les diferents facetes de la privacitat. 2. Identificar i avaluar la manera com es recopilen dades personals durant la navegació per Internet i l'ús d'aplicacions en dispositius intel·ligents. 3. Comprendre els drets a la privacitat resultants dels estatuts per a la protecció de dades.
Tema	Drets a la privacitat: Carta de Drets Humans de l'ONU; Carta de la UE sobre drets humans; RGPD
Pregunta clau	*Quins drets tinc a la privacitat?* Pregunta als teus familiars i amics què en pensen del seu dret a la privadesa. Pots compartir els vostres punts de vista (teus i dels teus contactes) al fòrum de la web de CSI-COP (https://csi-cop.eu/forum/). Per tal de publicar al fòrum, caldrà que et registris a la web i iniciar sessió mitjançant aquest enllaç: https://csi-cop.eu/citizenscientistlogin/.
Resum breu	Estatuts i reglaments que inclouen els drets humans pel que fa la privacitat.
Contingut	**Dret humà a la privacitat** Resumint el què hem après fins ara: • En el primer pas hem vist el concepte de «privacitat». • En el segon pas hem après que les «dades personals» es refereixen a una persona física (viva) . • En el tercer pas hem descobert algunes de les formes en què es poden capturar les nostres dades en línia (a través de les *cookies*, per exemple). En aquest pas explorarem els «drets humans». Pat Walshe, de Privacy Matters, ens recorda que els drets humans han estat importants des de fa molt de temps. Ja el 1689, a Gran Bretanya, per exemple, els drets humans es consideraven quelcom essencial per ser humans, per la nostra dignitat i per protegir els drets i llibertats bàsics (Biblioteca Britànica, 2013). Drets i llibertats que avui donen forma a diferents dimensions de les nostres vides —*offline* i *online*—: des del dret a expressar opinions, a el dret a associar-se lliurement amb altres i a la llibertat de reunió, passant per la llibertat de religió, el dret a l'educació, el dret a un judici just, el dret a contreure matrimoni o el **dret a la privacitat**, per exemple. Els drets humans importen cada dia *offline* i *online*, ja que ens permeten prosperar com a éssers humans. Més tard, el **1948**, els drets humans van adquirir importància global. En resposta a les atrocitats comeses durant la Segona Guerra Mundial, l'Assemblea General de les Nacions Unides va adoptar la Declaració Universal de Drets Humans (**DUDH**) per protegir els drets humans bàsics que totes les persones haurien de tenir. Això inclou la protecció contra la interferència arbitrària en la **privacitat**, la **família**, la **llar** o la **correspondència personal**, segons l'article 12 de la DUDH. El 1949, diversos països europeus van formar el Consell d'Europa (**CoE**), que actualment compta amb 47 estats europeus. El **1950**, el Consell d'Europa va adoptar

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

	el Conveni Europeu de Drets Humans (CEDH), de nou per protegir-nos, en el futur, contra atrocitats com les comeses durant la Segona Guerra Mundial. El CEDH incorpora drets clau que es troben a la DUDH i va entrar en vigor el **1953.** El CEDH és el primer instrument **internacional legalment vinculant** que protegeix els drets humans. Cal destacar que tots els estats membres de la Unió Europea (UE) s'han adherit a CEDH. L'article 8 del CEDH estableix que tota persona té dret al respecte de la seva **vida privada** i **familiar**, així com del seu **domicili** i **correspondència**. És fàcil veure com aquest dret està destinat a protegir els aspectes íntims de la vida d'una persona; aspectes fàcils d'observar *online*. Si bé l'article 8 del CEDH protegeix el dret a la privacitat, també inclou el dret a la protecció de dades, atès que l'ús d'informació personal no només influeix en la privacitat de les persones, sinó també en altres drets i llibertats, com veurem en aquest curs. Per ajudar a protegir les persones, els seus drets i llibertats i, en particular, el dret a la privacitat, el 1981 el **CoE** va adoptar un conjunt de principis i regles que s'apliquen al processament d'informació personal. Aquests principis i regles es coneixen com «Convenció 108». La Convenció es va actualitzar recentment per reflectir els canvis en la tecnologia i l'ús de dades que poden afectar negativament els drets de les persones, i ara es coneix com Convenció 108+. El **2000,** la UE va establir la Carta dels Drets Fonamentals de la UE. La Carta es va convertir en legalment vinculant per als estats membres de la UE el 2009. Tal com el CEDH, la Carta dels Drets Fonamentals de la **UE** estableix que totes les persones tenen dret a el respecte de la seva **vida privada** i i **familiar,** de la seva **llar** i les seves **comunicacions** (article 7). A més, la Carta també estableix que totes les persones tenen dret a la protecció de les seves dades personals (article 8). Els articles 7 i 8 de la Carta, respectivament, estableixen el dret a la privacitat i la protecció de dades com dos drets diferents. Aquests drets es fan efectius mitjançant un **instrument de privacitat electrònica** conegut com la Directiva de privacitat electrònica de la UE (que s'aplica a elements com *cookies* i altres tècniques de rastreig en línia) i un instrument de protecció de dades, el Reglament General de Protecció de Dades de la UE (**RGPD**). Les normes de protecció de dades de la UE i les del **CoE** s'han implementat en la legislació dels estats membres i s'han reforçat per reflectir els canvis en la tecnologia i en l'ús de dades. Avui dia, quan les persones utilitzen els seus telèfons mòbils, ordinadors portàtils, etc., les seves dades poden ser recollides en temps real i compartides entre centenars de tercers (els anunciants, per exemple); sovint, d'una manera de la qual la gent no és realment conscient o sense que es tinguin opcions significatives per evitar-ho. Aquestes dades poden revelar aspectes de la vida privada d'una persona, com la seva ubicació, els seus hàbits de compra, els llocs web que visita o qui són els seus contactes i les seves connexions socials. A la web de l'Oficina del Comissionat d'Informació del Regne Unit (ICO) s'explica que «el reglament general de protecció de dades (RGPD) de 2018 atorga a les persones el dret a ser informades sobre la recopilació i l'ús de les seves dades personals. **Aquest és un requisit clau de transparència**» (es pot veure en el següent enllaç: https://bit.ly/2QxmZH1).

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

	Pat Walshe, de Privacy Matters, afirma: «El dret a la privacitat i a la protecció de dades són més importants que mai, ja que les nostres dades digitals revelen aspectes profundament personals i íntims de nosaltres mateixos i d'aquells amb qui estem connectats».  Traducció de la imatge: La privacitat *online* ~~està morta~~ és el teu dret humà. <u>Què esperar del proper pas del curs</u> En el darrer punt d'aquest curs, pas 5, aprendrem q*uines eines en línia podem utilitzar per tal d'assegurar millor la nostra privadesa i protegir les nostres dades*. <u>Revisa el teu aprenentatge</u> Comprova el que has après en aquest pas responent al miniqüestionari que trobaràs a l'apartat d'exercicis.
Revisa el teu aprenentatge	**Declaració Universal dels Drets Humans de 1948 (DUDH); Article 12**: «Ningú no serà objecte d'intromissions arbitràries en la seva privacitat (...) [o] correspondència». **Carta dels Drets Fonamentals de la UE de 2000 (CEDH); Article 1**: «La dignitat humana és inviolable. Ha de ser respectada i protegida». **El Reglament General de Protecció de Dades (RGPD) de 2018 «estableix un alt estàndard per al consentiment»**; aquest consentiment ***informat*** implica: • «oferir a les persones opcions i control reals», • «que el consentiment genuí ha de posar a les persones al capdavant, generar confiança i compromís».
Exercicis	**Miniqüestionari** sobre les diferents cartes/estatuts i reglaments: ¿Les següents afirmacions són vertaderes o falses? • L'UNHR (United Nations Human Rights) és un nou reglament que atorga el consentiment informat. • La Directiva sobre Privacitat Electrònica es refereix a les *cookies*. • El RGPD no es preocupa per la transparència. Discuteix les teves respostes amb familiars, amics, veïns o companys de treball. Recordatori: Pots compartir els vostres punts de vista (teus i dels teus contactes) al fòrum de la web de CSI-COP (https://csi-cop.eu/forum/). Per tal de publicar al fòrum, caldrà que et registris a la web i iniciar sessió mitjançant aquest enllaç: https://csi-cop.eu/citizenscientistlogin/.

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

Activitat final	Discussió amb altres científics ciutadans sobre la declaració de 1999 del director executiu i cofundador de Sun Microsystems, Scott McNealy: **«De totes maneres, tens zero privacitat ... supera-ho».** Citat a Wired: https://www.wired.com/1999/01/sun-on-privacy-get-over-it/
Proposta de tuit	La privacitat *online* no és un luxe.

Lectures addicionals per al pas 4	Els enllaços a les lectures addicionals esmentades en aquest punt es poden consultar clicant el text subratllat. **Lectures recomanades** British Library (2013). *Taking Liberties: The struggle for Britain's freedoms and rights. Taking Liberties – Star Items Index – Human Rights.* Pots llegir l'article en anglès aquí: https://bit.ly/2QU4bSa ICO (sense data). *Guide to the General Data Protection Regulation (GDPR): Right to be informed.* UK Information Commissioner's Office (ICO). Pots llegir l'article en anglès aquí: https://bit.ly/3erd79K **Lectures addicionals** EHCR (sense data). *European Convention on Human Rights*. (Convenció Europea dels Drets Humans). Pots consultar-lo en anglès aquí: https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c= ePrivacy Directive (2002). 32002L0058 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. (Directiva 2002/58/EC del Parlament i Consell Europeus de juliol de 2002, relacionada amb el processament de dades personals i la protecció de la privadesa en el sector de les comunicacions electròniques). Pots consultar-la en anglès aquí: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN GDPR (2016). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. (Reglament EU 2016/679 del Parlament i Consell europeus sobre la protecció de les persones físiques en relació amb el processament de dades personals i sobre la lliure circulació d'aquestes dades, que deroga la Directiva 95/46/EC —Reglament General de la Protecció de Dades—). Pots consular-lo en anglès aquí: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN UN (sense data). *United Nations Declaration of Human Rights*. (Declaració dels Drets Humans de les Nacions Unides). Pots consultar-la en anglès aquí: https://www.un.org/en/about-us/universal-declaration-of-human-rights

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

PAS 5

Títol pas 5:	**Com protegir les teves dades en línia**
En aquest pas aprendràs a:	1. Descriure i analitzar les diferents facetes de la privacitat. 2. Identificar i avaluar la manera com es recopilen dades personals durant la navegació per Internet i l'ús d'aplicacions en dispositius intel·ligents. 3. Comprendre els drets a la privacitat resultants dels estatuts per a la protecció de dades.
Tema	Eines per protegir les teves dades en línia.
Pregunta clau	*Com canviar la configuració de navegació web i de les aplicacions per aturar el rastreig en línia?* Quan ho descobreixis, explica-li a la teva família i amics les eines que poden ajudar-los a protegir les seves dades en línia. Pots compartir els vostres punts de vista (teus i dels teus contactes) al fòrum de la web de CSI-COP (https://csi-cop.eu/forum/). Per tal de publicar al fòrum, caldrà que et registris a la web i iniciar sessió mitjançant aquest enllaç: https://csi-cop.eu/citizenscientistlogin/.
Resum breu	**Aplicacions**: Verifica els permisos a l'apartat «Configuració» de les aplicacions existents en els teus dispositius mòbils. Abans de descarregar una aplicació, comprova quins permisos sol·licita: són necessaris per tal l'aplicació funcioni? Per exemple, una aplicació de transport necessitarà accedir a la teva ubicació perquè l'aplicació proporcioni informació precisa. **Llocs web**: Utilitza un navegador amb principi de privacitat en el disseny i per defecte (*privacy-by-design*) o actualitza la configuració per evitar el rastreig i limitar les *cookies* de publicitat i màrqueting de tercers.
Contingut	**Eines en línia que poden ajudar-te a protegir les teves dades i la teva privacitat** Recapitulem el que hem après fins ara: • En el primer pas hem vist el concepte de «privacitat». • En el segon pas hem après que els «dades personals» es refereixen a una persona física viva. • En el tercer pas hem descobert algunes de les formes en què es poden capturar les nostres dades en línia (a través de les *cookies*, per exemple). • En el pas 4 hem vist els diferents estatuts/cartes i reglaments que ens atorguen dret a la privacitat. En aquest pas descobrirem de quines eines en línia disposem per protegir les nostres dades i la nostra privadesa. Pensa en el teu ús d'Internet: sents que controles cada vegada més la teva vida *en línia* ? Pat Walshe (Privacy Matters) assenyala que ens connectem a Internet per: comprar, fer videotrucades, enviar-nos missatges, compartir experiències i pensaments mitjançant les xarxes socials. I també ho fem per demanar cites mèdiques, buscar informació (fins i tot sobre problemes de salut), trobar i seguir indicacions de viatges, per viatjar en transport

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

	públic o en cotxe, bicicleta o a peu. Així mateix, utilitzem la xarxa per escoltar música o àudios i veure pel·lícules o la televisió. Gran part de les nostres vides s'ha tornat digital, però tornar-se digital genera i deixa empremtes, dades digitals que es poden recopilar i utilitzar per crear el nostre perfil i aprendre sobre nosaltres, i així influir en nosaltres de formes que potser no sabem. Cada pàgina web que visites, cada clic que fas, cada trucada o missatge que envies o reps, cada publicació que fas a les xarxes socials, cada lloc que visites o «etiquetes», cada «m'agrada» que publiques, cada cançó que escoltes o cada pel·lícula que mires (i els detalls de quan ho fas, si fas una pausa, si avances la reproducció o et saltes una cançó o pel·lícula)... tot això crea dades sobre tu. I aquestes dades revelen aspectes del teu comportament, aspectes sobre TU i, sovint, aspectes íntims (per exemple, les aplicacions de fertilitat, que et coneixen íntimament). Consulta el següent article (en anglès) de la revista Wired (2018): «Before using birth control apps, consider your privacy» (abans d'usar una aplicació per al control de natalitat, considera la teva privacitat). El pots llegir a: https://bit.ly/3ajCiZz. Addicionalment, en un article de 2020 a *The Guardian*, una organització benèfica sobre privacitat informar que «les aplicacions per al control de la menstruació emmagatzemen informació excessiva». Pots llegir l'article en anglès aquí: https://bit.ly/3aj7IQH. Llavors hi ha les aplicacions que comparteixen aspectes íntims de la sexualitat, religió o ubicació d'una persona, per exemple (i cal tenir en compte que les dades d'«ubicació» ja poden suggerir molt, ja sigui perquè una ubicació indica el lloc d'un tipus específic de culte o una clínica de salut d'un tipus específic). Pots llegir l' informe de Consumer Reports de 2020 sobre aquestes aplicacions aquí: https://bit.ly/3ggUw2x També hi ha aplicacions adreçades a infants i adolescents/adults joves que capturen dades, potser sense el coneixement del nen o adolescent que s'ha descarregat l'aplicació, o sense el coneixement dels pares que podrien haver comprat una aplicació per al seu fill en un dispositiu intel·ligent. Yubo és una "aplicació de xarxes socials" dirigida a infants per ajudar-los a trobar amistats. El diari britànic Sunday Times va informar sobre els problemes de salvaguarda de l'aplicació a la seva edició del 20 de febrer de 2022. Podeu llegir part d'aquest informe del Sunday Times a la imatge següent:

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

Abuse rife on 'Tinder for teens'

Sian Griffiths and Katie Tarrant

Schools have warned parents about a "Tinder for teens" social media app that an investigation found to be exposing children to sexual harassment, racism and bullying.

The platform, Yubo, allows children aged 13 to 17 to match with potential dates, as well as to join "lives" where they are encouraged to interact with about 100 other teenagers in group video calls. In Britain, it has 3.6 million users.

Head teachers at primary and secondary schools have become so concerned that they have shared a safety newsletter which says that "due to the nature of this app, your child may come across content that is not appropriate to them".

James Loten, deputy head at Harwich and Dovercourt High School, Essex, told parents he was concerned that Yubo "could be "exploited by adults for nefarious purposes". Kingsley primary school, in Co Durham, said children should be stopped from downloading it.

A Sunday Times reporter spent ten days on Yubo, posing as a 15-year-old girl called Anne. No age verification was required, with the journalist able to use profile pictures of her 20-year-old self.

She was propositioned for sex and frequently asked to send nude pictures. A message from a 17-year-old boy said: "Let me rail [have sex with] you", while others told girls on a livestream they would "strip you naked and rape you" and "choke you". A black 16-year-old was told by another user: "I'd le you pick my cotton any day." I

Continued on page 4→

NEWMAN'S VIEW

RELAX, WE'RE ALMOST HOME

All the single men...

Tom Calver
Data Projects Editor

Perhaps then, it is no surpr that the area won cult status in 2003 film *Love Actually* when Hu Grant, as the prime minister, w

Més endavant en aquest pas 5 coneixerem les eines en línia gratuïtes que hi ha sota aplicacions com Yubo per saber si hi ha problemes de privadesa de dades en aquesta o en altres aplicacions dirigides als infants.

A més, totes aquestes dades no tan sols revelen aspectes sobre TU MATEIX sinó també aspectes d'ALTRES PERSONES, d'aquells amb qui et comuniques i comparteixes informació, de les teves relacions i patrons de comunicació. Per exemple, una aplicació pot demanar-te que carreguis o li donis accés als «contactes» que tens al teu ordinador o *smartphone* . Però què és un contacte? Un contacte pot incloure el nom d'una persona, la seva foto, el seu número de telèfon mòbil, la seva adreça de correu electrònic, la seva adreça postal, el nom d'usuari de la xarxa social, la seva data d'aniversari...
En ser digitals en línia, potser hem de pensar no només en la nostra pròpia privacitat, sinó també en la privacitat dels altres.

Tal com hem vist en el pas 4, a la UE i el Regne Unit, el dret a la privacitat en línia està protegit per lleis específiques de **privacitat electrònica** i pel Reglament General de Protecció de Dades (**RGPD**); però, tot i que les lleis i la seva aplicació poden fer molt, hi ha coses que tu també pots fer per ajudar a protegir la teva privacitat en línia.

En el tercer pas hem descobert com es rastregen les persones **a través de la web**, fet que inclou el rastreig a través de la tecnologia publicitària (*ad tech*, en anglès), como serien les *cookies* o el rastreig per part del servidor.
Però què pots fer tu per tal de controlar i protegir la teva privacitat en línia? L'autogestió de la privadesa és difícil.
Pots obtenir més informació sobre com es duu a terme el rastreig dels individus **a través de les aplicacions mòbils** (kits de desenvolupament de *software* —SDK—) si llegeixes l'article de Binns *et al.* (2018): *Third Party Tracking in the Mobile Ecosystem*. Pots trobar l'article en anglès aquí: https://arxiv.org/pdf/1804.03603.pdf .

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

Eines per descobrir el rastreig i controlar-lo.

Eines de transparència (web):
Hi ha diverses eines que poden ajudar-te a comprendre quin tipus de rastreig es produeix a les pàgines que visites. Gran part d'aquest rastreig es porta a terme per fer-te arribar publicitat dirigida o per «personalitzar» la teva experiència. Sovint, això inclou compartir dades amb empreses de publicitat de tercers, de vegades centenars d'elles.

Algunes de les eines de transparència web són:
—Webbkoll és una eina que simula el que passa quan un usuari visita una pàgina web usant un navegador típic. Mostra quines *cookies* pròpies i de tercers poden estar presents en la pàgina visitada i també quin rastreig es realitza independentment de les *cookies*, com les sol·licituds realitzades pels servidors.
https://webbkoll.dataskydd.net/en

—Blacklight escaneja un lloc web i en revela les tecnologies clau de rastreig.
https://themarkup.org/blacklight

—Pagexray és una eina d'anàlisi que mostra tots els anuncis i rastrejadors carregats a una pàgina web i presenta els resultats en forma de gràfic d'arbre. Els resultats es poden descarregar com a HTTP Archive (.Har.json) o com a resultats detallats (.json)
https://pagexray.fouanalytics.com/

—Request Map Generator ajuda a identificar quins tercers hi ha en un lloc web i cap on es transmeten les dades. Els resultats es poden descarregar en un fitxer CSV.
https://requestmap.webperf.tools

—Cover Your Tracks és una eina per provar la protecció del teu navegador contra el rastreig i la presa d'empremtes digitals.
https://coveryourtracks.eff.org

Eines de transparència (aplicacions mòbils):
Examinar las aplicacions mòbils no és una tasca fàcil.
O'Flaherty, un periodista un periodista especialitzat en ciberseguretat, afirma que, quan fas servir una aplicació al telèfon, aquesta «pot rastrejar-te a través d'altres aplicacions i llocs web per enviar-te publicitat dirigida. Actualment, això es fa a través d'una cosa anomenada «identificador per anunciants» (**IDFA**, per les sigles en anglès); una eina que rastreja, però sense revelar la teva informació personal».

En tot cas, hi ha algunes eines per ajudar a posar llum sobre l'existència de «rastrejadors» integrats en les aplicacions d'Android.
Una eina clau per Android és **Exodus Privacy** (https://exodus-privacy.eu.org/en/).
Android Studio: https://developer.android.com/studio.

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

	Pat Walshe (Privacy Matters) adverteix que actualment no hi ha una eina equivalent per a les aplicacions iOS d'Apple. No obstant això, Apple ha introduït noves normes de transparència, per la seva botiga i els seus desenvolupadors, amb què s'exigeix l'ús d'etiquetes de privacitat predefinides per revelar quines dades es fan servir i per quin motius. El nou iOS 14.5 d'Apple també requereix als desenvolupadors que «obtinguin el permís de l'usuari abans de rastrejar les seves dades en aplicacions o llocs web propietat d'altres empreses quan sigui amb finalitats publicitàries o per compartir les dades amb corredors de dades (*data brokers*)». Segons Apple, aquesta nova funció de privacitat permet als propietaris de telèfons d'Apple amb aquest sistema operatiu que «cliquin sobre l'informe de privadesa per entendre millor com els llocs web tracten la privacitat dels usuaris» (Apple, 2021). De nou segons Apple, la seva funció de transparència en el rastreig de les aplicacions (App Tracking Transparency —ATT—) «requerirà que totes les aplicacions demanin permís explícit per poder realitzar un rastreig» i «a l'apartat de Configuració, els usuaris podran veure quines aplicacions han demanat permís per dur a terme un rastreig i podran, si ho desitgen, realitzar els canvis que considerin oportuns» (O'Flaherty, 2021). En el Mac OS («Big Sur»), Apple proporciona una eina d'informe de privacitat que apareix com una icona en el navegador Safari, fet que permet als usuaris veure quins rastrejadors hi ha en una pàgina web i quins es bloquegen. El navegador Safari d'Apple «t'ofereix diverses maneres d'ajudar-te a protegir la teva privacitat» (Apple, 2021). La iniciativa de privadesa d'Apple suposa un «punt d'inflexió» segons O'Flaherty (2021). I amb «la mort de les *cookies* de tercers» (Cyphers, 2021), els científics ciutadans podrien convertir-se en la força que impedeixi que qualsevol substitut (com el «nou conjunt de tecnologies de Google per la publicitat dirigida a la web») ens rastregi en línia, la qual cosa comportaria més privadesa a l'hora de navegar en línia. **Recapitulació: Què pots fer per protegir la teva privacitat?** —Navegadors —Bloquejadors d'anuncis —Ús de la configuració de privadesa (en els sistemes operatius, navegadors, aplicacions...) 
Revisa el teu aprenentatge	Revisa el que has après en aquest pas en veure que existeixen maneres de protegir les teves dades i la teva privades quan estàs en línia.
Exercicis	Aprenentatge experiencial: explora els llocs web que visites i les aplicacions que fas servir, i descobreix quins rastrejadors digitals tenen instal·lats, si n'hi ha. **Exercici 1:**

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

	Utilitza una de les eines que hem vist en aquest pas (com webbkoll) per veure què s'amaga sota les pàgines web que acostumes a visitar. Consulta el lloc web per veure a) la seva política de privacitat i b) la seva política de *cookies*. Preguntes —T'ha resultat senzill entendre la política de privacitat? —La política de *cookies* informa sobre alguna d'elles o sobre quantes n'hi ha? —Quines *cookies* incrustades de tercers es donen a conèixer en la política de *cookies*? **Exercici 2** Ves a l'apartat «Configuració» del teu dispositiu mòbil intel·ligent, selecciona qualsevol aplicació i verifica els seus permisos. Preguntes —Quins permisos s'han atorgat a l'aplicació que has consultat? —Quan vas descarregar l'aplicació, eres conscient d'aquests permisos? Recordatori: Pots compartir els vostres punts de vista (teus i dels teus contactes) al fòrum de la web de CSI-COP (https://csi-cop.eu/forum/). Per tal de publicar al fòrum, caldrà que et registris a la web i iniciar sessió mitjançant aquest enllaç: https://csi-cop.eu/citizenscientistlogin/.
Objectiu dels exercicis	Passar de ser un aprenent informal a un científic ciutadà CSI-COP. Comenta la teva opinió sobre aquest curs/taller amb els teus familiars i amics: —Què creus que has guanyat després d'haver seguit els cinc passos de l'aprenentatge informal CSI-COP? —T'agradaria unir-te a l'equip de CSI-COP i convertir-te en un científic ciutadà per investigar el rastreig en línia? —T'interessaria seguir aprenent sobre la protecció de dades, la privacitat, el desenvolupament web i altres temes relacionats?
Proposta de tuit	Protegeixo les meves dades amb eines web.
Lectures recomanades per al pas 5	Cyphers, B. (2021). *Google's FLoC (Federated Learning of Cohorts) is a terrible idea*. Electronic Frontier Foundation. Pots llegir l'article en anglès aquí:https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea O'Flaherty, K. (2021). «Apple's Stunning iOS14 Privacy Move: a game-changer for all iPhone Users». *Forbes*. Pots llegir l'article en anglès aquí: https://bit.ly/3vpOq4v/

Valoració del curs

Els teus comentaris sobre el curs d'aprenentatge informal «CSI-COP: el teu	A l'equip de CSI-COP ens aniria molt bé saber què t'ha semblat aquest curs, així que t'agrairíem que seleccionessis una de les opcions de la llista següent: 5. Molt útil 4. Útil 3. No ho sé 2. Poc útil

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

dret a la privacitat en línia»:	1. Gens útil Afegeix tots els comentaris o suggeriments que puguis tenir sobre el curs i que consideris oportuns:

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

Avalua el teu aprenentatge

Per tal d'avaluar el teu aprenentatge i obtenir un certificat CSI-COP, respon les preguntes següents i envia les respostes a l'Eva (UAB) o a l'Huma (CU) als correus electrònics que trobaràs a continuació. Si obtens un 8/10 o més, rebràs un certificat d'educació informal CSI-COP (pots intentar respondre les preguntes tantes vegades com vulguis):

Eva (UAB): eva.jove@uab.cat / Huma (CU): ab7778@coventry.ac.uk

Preguntes

a. «La privacitat s'ha convertit en un problema des de l'aparició de Facebook». Aquesta afirmació és vertadera o falsa?
b. «El mode "incògnit" del navegador Google Chrome et permet fer cerques amb total privacitat». Aquesta afirmació és vertadera o falsa?
c. «En utilitzar una xarxa wifi pública es poden compartir les dades de localització». Aquesta afirmació és vertadera o falsa?
d. «Les dades personals sensibles es relacionen amb el teu nom». Aquesta afirmació és vertadera o falsa?
e. «La presa d'empremtes digitals és un tipus de rastreig dels llocs web que utilitza els atributs del teu dispositiu o navegador per construir el teu perfil». Aquesta afirmació és vertadera o falsa?
f. Quina de les següents categories fa referència a dades de comportament? Marca totes les que ho siguin a la llista següent:
    i. Les teves interaccions en un lloc web
    ii. Les teves dades de navegació web
    iii. L'historial de compres en línia
    iv. Quan utilitzes un mapa *en línia*
    v. Quan fas servir una aplicació (per exemple, per controlar la teva salut)
g. «Els drets humans es consideraven quelcom essencial per a la nostra dignitat i per protegir els nostres drets bàsics i les nostres llibertats». Aquesta afirmació és vertadera o falsa?
h. « D'acord amb la Declaració Universal de Drets Humans (DUDH), els teus drets inclouen "protecció contra interferències arbitràries en la privacitat, la família, la llar o la correspondència d'una persona"». Aquesta afirmació és vertadera o falsa?
i. «Segons la convenció europea de drets humans (CEDH): en l'era moderna no tenim dret a esperar una vida privada i familiar a la nostra llar i la nostra correspondència». ¿Aquesta afirmació és vertadera o falsa?
j. De conformitat amb el Reglament General de Protecció de Dades (RGPD), tenim dret a... (selecciona totes les opcions que corresponguin):
    i. Ser informats
    ii. La transparència
    iii. La protecció de dades
    iv. No ser filmats per les càmeres d'altres persones

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

Converteix-te en un científic ciutadà

Esdevenir un científic ciutadà de CSI-COP	Després de completar els cinc passos del curs d'educació informal de CSI-COP i rebre el teu certificat, t'agradaria unir-te a l'equip CSI-COP i investigar l'abast del rastreig en línia? Pots unir-te a l'equip CSI-COP i participar com a científic ciutadà voluntari en el projecte CSI-COP. Si ho demanes, se't proporcionarà informació completa. Aquesta informació inclou: • Full informatiu per als participants sobre el paper dels científics ciutadans. • Full de consentiment informat que compleix amb el Reglament General de Protecció de Dades (RGPD). • Informació sobre com començar a investigar llocs web i aplicacions a la recerca de *cookies*. Pots obtenir més informació a l'apartat 'About' del lloc web de CSI-COP (a l'enllaç següent: https://csi-cop.eu/about/). Si encara no ho has fet, pots apuntar-te al lloc web de CSI-COP creant el teu compte (a l'enllaç següent: https://csi-cop.eu/citizenscientistlogin/). El fòrum del lloc web de CSI-COP, on podràs discutir amb altres científics ciutadans del projecte, el trobaràs a l'enllaç següent: https://csi-cop.eu/forum/ Tot seguit trobaràs una enquesta amb algunes preguntes sobre tu. Això és per ajudar l'equip de CSI-COP a saber qui són els científics ciutadans. No recopilarem cap dada que t'identifiqui com a persona. Moltes gràcies pel teu temps!

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

Interval d'edat: marca amb un cercle l'interval corresponent.	18-39 40-65 66+ Prefereixo no dir-ho
Gènere (selecciona'n un)	—Dona —Home — Intersexual —Paraigua trans — Un altre —Prefereixo no dir-ho
Ubicació (selecciona'n una)	—Urbana (ciutats) —Rural (pobles de menys de 2000 habitants) —Prefereixo no dir-ho
Idiomes 1. Quina és la teva llengua materna o dominant? 2. Parles més d'una llengua? Quines? Pots preferir no dir-ho.	**1.** **2.** Prefereixo no dir-ho
Accessibilitat: Consideres que tens algun problema d'accessibilitat? (per exemple, si fas servir un *software* de conversió de text a veu a causa d'una discapacitat visual?)	Sí No Prefereixo no dir-ho
Feina:	Estudiant (selecciona el nivell d'estudis) —Grau o llicenciatura —Postgrau —Doctorat No estudiant (escull la categoria que millor descrigui la teva situació laboral) —Empleat (36,5 h/setmana o més) —Empleat (1-36h/setmana) —Sense feina (buscant-ne) —Sense feina (sense buscar-ne —Refugiat que busca asil —Jubilat —Amb problemes d'accessibilitat (sense possibilitat de treballar) —Prefereixo no dir-ho
Accés a Internet:	—Amb accés a connexió Internet pròpia (banda ampla domèstica o laboral/ mòbil) —Accés a Internet mitjançant una xarxa pública —Prefereixo no dir-ho

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

Ús d'Internet. Amb quina freqüència utilitzes Internet? (selecciona una opció)	—A diari —2-3 vegades per setmana —Una vegada a la setmana —Menys d'una vegada a la setmana —Mai —Prefereixo no dir-ho
Finalitat de l'ús d'Internet:	—Utilitzo Internet com a part de la meva feina diària —Utilitzo Internet per l'oci (no per la feina) —Utilitzo Internet per l'oci i la feina —Utilitzo Internet de manera limitada (per exemple, en un ordinador d'una biblioteca pública) —Prefereixo no dir-ho
Ús d'aplicacions en ordinadors d'escriptori i portàtils	—Utilitzo aplicacions regularment, per exemple per accedir a eines laborals (com Zoom, MS Teams, etc.). * Si és el cas, indica quines aplicacions utilitzes i amb quina finalitat: —Eines de treball (p.e. Microsoft Office, etc.) —Per jugar (p.e. STEAM). —Aplicacions educatives —Estil de vida (esports, salut...) —Notícies —Entreteniment (com aplicacions en *streaming* tipus Netflix) —Altres —Prefereixo no dir-ho —Rarament utilitzo aplicacions en ordenadors d'escriptori o portàtils. —No utilitzo aplicacions en ordinadors d'escriptori o portàtils. —Prefereixo no dir-ho
Ús d'aplicacions en dispositius mòbils	—Utilitzo aplicacions amb freqüència, per exemple aplicacions per saber l'hora d'arribada del següent tren, bus, etc. * Si és el cas, indica quines aplicacions utilitzes i amb quina finalitat: —Jugar —Aplicacions educatives —Estil de vida (esport, salut...) —Notícies —Entreteniment (com ara *apps* en *streaming* tipus Amazon Prime). —Altres —Prefereixo no dir-ho —Rarament utilitzo aplicacions al telèfon mòbil o la tablet —No utilitzo aplicacions —Prefereixo no dir-ho
Com has conegut el projecte CSI-COP?	—A través del lloc web de CSI-COP —A través d'una universitat —A través d'una associació a la qual pertanyo (p. e. Women in Tech) —A través d'una plataforma de ciència ciutadana com: • SciStarter • Zooniverse • EU-Citizen.Science

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169

	• Una altra plataforma de ciència ciutadana —Navegant per Internet —Gràcies a un voluntariat previ —A través d'una xarxa social (indica quina) —Pel boca-orella —Altres
Has finalitzat el curs/taller d'educació informal en línia i gratuït CSI-COP?	—Sí —No, però tinc intenció de fer-ho —No, prefereixo esperar futurs tallers presencials si es duen a terme a prop del meu lloc de residència
Si has finalitzat el curs/taller, tens intenció d'unir-te a l'equip de CSI-COP com a científic ciutadà voluntari?	—Sí —Potser —Necessito més informació —No
Envia la teva resposta a les preguntes de l'apartat «Avalua el teu aprenentatge», el resultat d'aquesta enquesta, la valoració del curs i qualsevol possible consulta a l'equip CSI-COP de la Universitat de Coventry.	Agrairem que enviïs el document degudament complimentat als membres de l'equip CSI-COP de la Universitat de la Universitat Autònoma de Barcelona: Dra. Eva Jove (eva.jove@uab.cat)

Gràcies per fer el curs d'educació informal de CSI-COP i l'enquesta.

Aquest document està disponible en altres idiomes.

Trobaràs més informació al lloc web de CSI-COP, al següent enllaç: https://csi-cop.eu/

Aquesta comunicació forma part d'un projecte que ha rebut finançament del
programa d'investigació i innovació European Union's Horizon 2020 en virtut de l'acord de subvenció núm. 873169