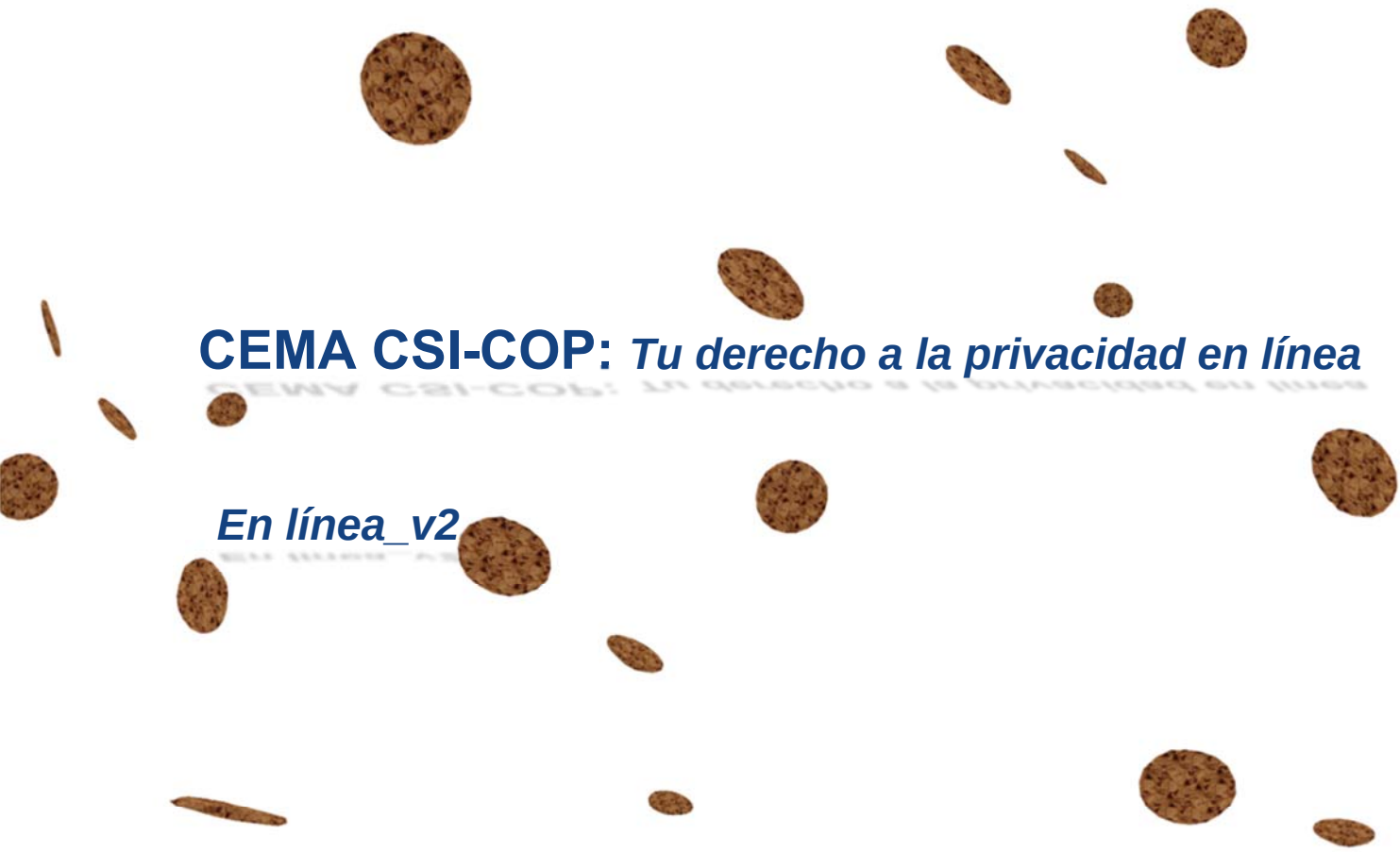
Científicos ciudadanos que investigan el cumplimiento del RGPD en las *cookies* y las aplicaciones



CEMA CSI-COP: *Tu derecho a la privacidad en línea*

En línea_v2

ÍNDICE

CEMA CSI-COP. Curso de educación informal	**Pág. 2**
Detalles del curso	**Pág. 4**
Paso 1: Privacidad	**Pág. 5**
Paso 2: Datos	**Pág. 9**
Paso 3: Rastreo en línea	**Pág. 15**
Paso 4: Derecho a la protección de datos y a la privacidad	**Pág. 22**
Paso 5: Herramientas para proteger tus datos y tu privacidad	**Pág. 26**
Valoración del curso	**Pág. 31**
Evaluación del aprendizaje	**Pág. 32**
Conviértete en un científico ciudadano CSI-COP	**Pág. 33**
Encuesta	**Pág. 34**

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

CEMA

El curso gratuito de aprendizaje informal de CSI-COP (curso en línea masivo y abierto —CEMA—) puede hacerse en línea o descargarse como documento. El tiempo estimado para la realización del mismo es de 2,5 a 3 horas.

Este CEMA trata sobre **tus datos y tu derecho a la privacidad en línea**. En Internet, los datos se recopilan mediante tecnologías digitales de sitios web o aplicaciones (programas de *software* de los dispositivos móviles). Dichas tecnologías incluyen *cookies*; pequeños archivos de texto que se almacenan en los ordenadores de mesa, portátiles o dispositivos inteligentes (tabletas, teléfonos móviles) al visitar una página en Internet. Las *cookies* pueden incluir rastreadores digitales, como el rastreo de la ubicación precisa de un dispositivo. La configuración de la aplicación también puede tener permisos para acceder a tus contactos, cámara, mensajes, micrófono u otros datos presentes en tus dispositivos móviles. La localización de un dispositivo puede identificar a la persona que usa o posee dicho dispositivo, por lo que su rastreo tiene implicaciones en la privacidad y protección de datos.

El proyecto financiado CSI-COP EU Horizon2020 tiene como objetivo principal educar informalmente al gran público en las tecnologías de rastreo en línea y en cómo desactivarlas. Esto puede llevar a este tipo de público a convertirse en «científico ciudadano». Un científico ciudadano (CC) es un miembro de la población en general involucrado en la recopilación y análisis de datos, como parte de un proyecto de colaboración con científicos profesionales. El objetivo de CSI-COP es involucrar a los científicos ciudadanos para que se **unan al equipo del proyecto CSI-COP** para investigar hasta qué punto el rastreo (*tracking*) se realiza de manera *predeterminada* en Internet. El reglamento general de protección de datos (**RGPD**) de 2018 ofrece una lista de verificación con la que se puede evaluar su cumplimiento. El equipo de CSI-COP cree que el enfoque desde la ciencia ciudadana es necesario para forjar la colaboración entre ciudadanos y científicos e investigar hasta qué punto nuestros datos son rastreados en línea a través de los sitios web que visitamos y de las aplicaciones que usamos.

¿Para quién es este curso?
Este curso se adapta a cualquier persona mayor de edad que esté interesada en comprender cómo nuestros datos se recogen a través de Internet y mediante las aplicaciones que utilizamos, y que quiera aprender cómo proteger su privacidad en línea.

¿Qué necesitas para realizar este curso?
Smartphone, tableta u ordenador portátil o de sobremesa con conexión a Internet. Si accedes a la red wifi gratuita de una universidad o biblioteca, ten en cuenta que los beneficios de una red wifi pública y gratuita conllevan el riesgo de que los piratas informáticos accedan a tus datos. Consulta la información de Kaspersky sobre cómo evitar riesgos en las redes wifi públicas aquí: https://bit.ly/3v6thff

Si utilizas Twitter
Al final de cada paso, te hacemos un propuesta de tuit que puedes enviar a terceros para informarles que estás llevando a cabo el curso de educación no formal CSI-COP. Si lo deseas, puedes etiquetar a CSI-COP mediante @cop_csi .

Accede a los detalles del curso en la página 4, y realiza los ejercicios de los pasos 1, 2, 3, 4 y 5 que encontrarás a partir de la página 5.

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

En cada paso se introducen brevemente los objetivos de aprendizaje y el contenido del mismo. Para ampliar información, al final de cada uno de ellos hemos puesto a tu disposición una sección de lectura adicional en la que encontrarás enlaces a una serie de material junto al nombre de su/s autor/es.

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Para mejorar tu aprendizaje y comprensión, responde a la ***pregunta clave*** de cada paso, que te invita a considerar una cuestión sobre un tema antes de aprender sobre él. Puedes discutir la «pregunta clave» (y otras) con tu familia y amigos, o hablar con otras personas en el foro que encontrarás en la web de CSI-COP (necesitarás registrarte previamente en este enlace: https://csi-cop.eu/citizenscientistlogin/).

Después de cada paso, también podrás evaluar tu aprendizaje gracias a una serie de ejercicios relacionados.
Tras el último paso, encontrarás un apartado para revisar todo el curso, así como la información necesaria sobre cómo unirte al equipo CSI-COP para convertirte en científico ciudadano, investigar sobre la privacidad en línea y ser un **defensor de la privacidad**.

¡Que disfrutes del curso!

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

DETALLES DEL CURSO

CEMA CSI-COP: un curso de aprendizaje informal autodidacta	*Tu derecho a la privacidad en línea*
Objetivos del CEMA	El curso en línea gratuito de CSI-COP está diseñado en **cinco pasos.** Completar cada uno de ellos te proporcionará los conocimientos necesarios para tomar decisiones informadas sobre tu derecho a la privacidad en línea y te proveerá de las habilidades necesarias para verificar y bloquear las tecnologías de rastreo en Internet y en las aplicaciones de tus dispositivos Android (por ejemplo, móviles o tabletas Samsung). Una vez completado el curso, podrás solicitar el certificado de aprendizaje informal CSI-COP, y pasar de ser un aprendiz informal a convertirte en un científico ciudadano voluntario, uniéndote al equipo de CSI-COP para investigar hasta qué punto se rastrean tus datos a través de Internet (más información en el paso 5). **https://cordis.europa.eu/project/id/873169**
Qué vas a obtener del curso *(objetivos de aprendizaje)*	—Adquisición de conocimientos sobre la privacidad en virtud de los estatutos de derechos humanos. —Habilidades prácticas (*conocimientos técnicos*) para descubrir las tecnologías de rastreo en línea integradas en sitios web y en aplicaciones de Android. —Información sobre cómo convertirse en un científico ciudadano y cómo unirse al equipo de CSI-COP para investigar el alcance del rastreo en línea a través de las tecnologías de rastreo digital.
Duración del curso	El curso está diseñado para poder ser completado de las formas siguientes: Realización de los cinco pasos en una sola sesión —tanto a nivel teórico como práctico— en unas **2,5 o 3 horas.** A tu propio ritmo.
Detalles del curso de aprendizaje informal	
Título	*Protege tus datos*
Objetivos y resumen	Este curso-taller está diseñado para completarse en medio día y de una sola vez. Sin embargo, puedes escalonar los pasos de aprendizaje para adaptarlos a tu disponibilidad. En este cursillo en línea, comprenderás de manera integral las diferentes facetas de la privacidad y qué relación tiene todo ello con la forma en que tus datos personales pueden ser usados por parte de terceros en tu interacción en línea en sitios web y en el uso de aplicaciones. Asimismo, aprenderás cómo tomar decisiones informadas sobre tus datos personales y cómo verificar la

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	transparencia en la forma en que se recopilan los datos sobre tu persona.
Qué vas a aprender durante el curso *(resultados del aprendizaje)*	**Resultados de aprendizaje previstos para el curso:** —Describir y analizar las diferentes facetas de la privacidad. —Identificar y evaluar la forma en que se recopilan los datos personales durante la navegación por la web y el uso de aplicaciones en dispositivos inteligentes. —Comprender los derechos a la privacidad resultantes de los estatutos para la protección de datos.
Contenido del curso	• La privacidad y sus distintas facetas • ¿Qué son los datos personales? • ¿Cómo se recopilan los datos personales a través de nuestro uso de Internet? • Derecho a la privacidad (ONU; EU; RGPD) • Protección de tus datos personales en línea

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

PASO 1

Título paso 1:	**Distintas facetas de la privacidad**
En este paso aprenderás a:	1. Describir y analizar las distintas facetas de la privacidad.
Tema	La privacidad y sus distintas facetas
Pregunta clave	*¿La privacidad es un privilegio o un derecho humano?* Pregunta a tus familiares y amigos qué piensan de la **privacidad**. Puedes compartir vuestros puntos de vista (tuyos y de tus contactos) en el foro de la web de CSI-COP aquí: https://csi-cop.eu/forum/ (para publicar en el foro necesitarás registrarte en la web e iniciar sesión mediante este enlace: https://csi-cop.eu/citizenscientistlogin/)
Breve resumen	Jan Holvast (2009) «La discusión sobre cuestiones de privacidad es tan antigua como la humanidad». (Consulta el apartado de lecturas adicionales al final de este paso).
Contenido	**Breve historia de la «privacidad»** Según Jan Holvast (2009), «la discusión sobre cuestiones de privacidad es tan antigua como la humanidad. Empezando por la **protección del cuerpo y el hogar propios**, esta pronto evolucionó hacia el **control de la información personal**».  En 1890, Warren y Brandeis escribieron: «que el individuo debe tener protección total en relación a su persona y a sus propiedades es un principio tan antiguo como el derecho consuetudinario», y también: «en tiempos muy tempranos, la ley solo ofrecía remedio para las injerencias físicas en la vida y la propiedad». Agregaron que «ahora [en 1890], el derecho a la vida ha pasado a significar... el derecho a vivir tranquilo», mientras que «el término "propiedad" ha crecido hasta abarcar todas las formas de posesión, tanto intangibles como tangibles». En 2011, Nissenbaum informó que «el año 2010 fue un gran año para la privacidad en línea. Los informes de errores de privacidad, como por ejemplo los relacionados con Google Buzz o las volubles políticas de privacidad de Facebook, aparecieron en las

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

portadas de los medios de comunicación más destacados. En su sección «**What They Know**» (Lo que saben), *The Wall Street Journal* alertó sobre el rastreo desenfrenado de los individuos para la publicidad conductual y otras razones.

En cuanto a la *ética de la privacidad*, Marijn Sax (2018) se centra en preguntas como: «**¿Cuál es el valor de la privacidad?**» y «**¿Qué normas de privacidad deben respetar los individuos (incluyéndonos a nosotros mismos), la sociedad y el Estado?**».

El 10 de Abril de 2022, el cómico británico John Oliver en su programa de HBO "Last Week Tonight" puso la atención del daño de los "agentes de datos" que capturan y juntan nuestras "migajas de datos digitales" en línea para desanonimizarnos y vender nuestros datos a terceros" (en The Guardian, 11 de Abril de 2022). Oliver informó que los intermediarios de datos son "parte de una industria multimillonaria" que "recoge tu información personal y después la revenden o la comparten con otros" con las "herramientas principales que son las cookies, que permiten a los sitios web recordarte y han evolucionado para incluirte cookies de terceros y que realizan un seguimiento de los sitios visitados en Internet." (The Guardian) Volveremos a las cookies en el paso 3.

Google Chrome

Puede que tengas activado el modo **incógnito** del navegador Chrome de Google para mantener tu privacidad. Sin embargo, parece que Google «recopila en secreto grandes cantidades de datos de Internet, incluso si los usuarios navegan en modo "incógnito" para mantener la privacidad de su actividad de búsqueda» (Nayak y Rosenblatt , 2021) . Una noticia de Bloomberg (2021) informa que «unos consumidores han presentado una "demanda colectiva" alegando que "incluso cuando desactivan la recopilación de datos en Chrome, otras herramientas de Google utilizadas por los sitios web terminan acumulando su información personal"» (Nayak y Rosenblatt, 2021). Puedes obtener más información sobre este caso en el nuevo sitio de Bloomberg aquí: https://bloom.bg/3gFt4vV

Facebook. 533 millones de violaciones de datos de usuarios

Es posible que hayas escuchado las últimas noticias sobre el hecho de que no importa cuánto intentemos mantener nuestra información algo privada, porque, si usamos las redes sociales, quedamos a disposición del propietario de la plataforma y de la competencia para asegurar nuestra privacidad.

Los **datos personales de más de 530 millones de usuarios de Facebook se encontraron disponibles en un sitio web para piratas informáticos en abril de 2021** (Holroyd, 2021). La información personal de los 533 millones incluye usuarios de Facebook en estos países:

—Más de 35 millones en Italia,
—más de 32 millones en EE. UU.,
—casi 20 millones de cuentas en Francia,
—11 millones de usuarios en el Reino Unido y
—6 millones de usuarios en la India.

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Lomas (2021) informa que el volcado de datos (de la información que los usuarios de Facebook han compartido en dicha plataforma) incluye:
—IDs de Facebook,
—nombres completos,
—números de teléfono,
—ubicaciones,
—fechas de nacimiento,
—biografías y
—algunas direcciones de correo electrónico.
Puedes leer más sobre el tema en TechCrunch.

Si eres usuario de Facebook y deseas averiguar si tu información está incluida en esta violación de datos de Facebook, puedes comprobarlo, ya sea con tu correo electrónico, con tu ID de Facebook, o con tu número de teléfono en estos sitios web:

Have I been pwned? (¿He sido engañado?). Aquí: https://haveibeenpwned.com/
Have I been Zucked? (¿He sido «absorbido»?). Aquí: https://haveibeenzucked.com/

También puedes seguir los tuits de The Real Facebook Oversight Board, «hacer que Facebook rinda las cuentas», en Twitter: https://twitter.com/FBoversight.

Quizás haya oído el nombre de Frances Haugen. Es científica de datos y antigua empleada de Facebook. Haugen dio testimonio en el Senado de Estados Unidos el 5 de Octubre de 2021, en el parlamento del Reino Unido el 25 de Octubre de 2021 y en el parlamento europeo el 8 de Noviembre de 2021. Haugen expuso la estrategia de beneficios de Facebook sobre el bienestar de los usuarios (lea más sobre la defensa de Frances Haugen por la "responsabilidad y transparencia en las redes sociales" en su sitio web: https://www.franceshaugen.com/).

La Comisión Irlandesa de Protección de Datos "impuso una multa de 17 millones de euros a Meta Platforms Ireland Limited por una serie de infracciones de datos entre el 7 de Junio de 2018 y el 4 de Diciembre de 2018" (Ver aquí: https://bit.ly/3MmUIKN).

Christopher Wylie, antiguo científico de datos de Cambridge Analytica y autor del libro de 2019 "MindF*ck: Inside Cambridge Analytica's Plot to Break the World" afirma: Facebook tiene demasiado poder sin control" (página 225).

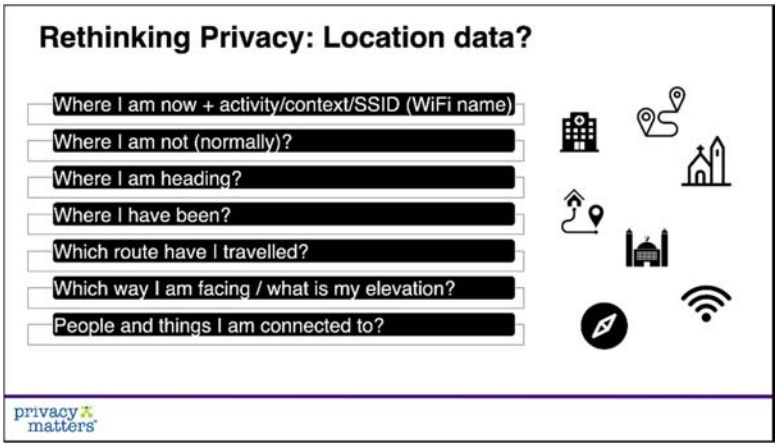
En 2021, el Tribunal de Distrito de Estados Unidos del Distrito Sur de Nueva York presentó una acción civil: Google Digital Advertising Antitrust. El párrafo 175 de la página 64 del documento judicial de EE.UU. dice:
"Google presenta una imagen pública de la preocupación por la privacidad, pero detrás de las escenas Google se coordina estrechamente con las empresas Big Tech

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

para presionar al gobierno para que retrase o destruya las medidas que realmente protejan la privacidad de los usuarios" (de Acción Civil núm.: 1:21-md-03010-PKC documento accesible desde courtlistener.com).

- Carissa Veliz, autora del libro de 2020 'Privacy is Power' advierte:

- Internet se financia principalmente por la recogida, el análisis y el comercio de datos... la economía de los datos" (página 1)
- "Gran parte de estos datos son datos personales: datos sobre ti" (página 1)
- "... teléfono inteligente.... Registrando tu viaje y cuánto tiempo estuviste..." (página 2)
- "La economía de los datos, y cuya vigilancia omnipresente se alimenta, nos cogió por sorpresa" (página 2)



Traducción:
Repensar la privacidad: ¿Qué pasa con los datos de ubicación?
Dónde estoy ahora + actividad / contexto / SSID (identidad de la wifi)
¿Dónde no estoy (normalmente)?
¿A dónde voy?
¿Qué trayecto he recorrido?
¿Con quién y con qué he conectado?

Qué esperar de los próximos pasos del curso

En el siguiente punto (paso 2) empezaremos a fijarnos en la información y los *datos personales*.
En el tercer paso, veremos *cómo se realiza el rastreo de nuestros datos*.
En el cuarto, veremos qué *derechos tenemos sobre nuestra privacidad.*
Y en el último punto de este curso, el paso 5, descubriremos *qué herramientas en línea* podemos utilizar para *asegurar mejor nuestra privacidad y proteger nuestros datos*.

Revisa tu aprendizaje

Comprueba lo que has aprendido en este paso respondiendo a la pregunta siguiente y realizando los ejercicios propuestos a continuación.

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Revisa tu aprendizaje	¿Qué es la *privacidad*?
Ejercicios	**Ejercicio 1** ¿La siguiente afirmación es verdadera o falsa? «El debate sobre la privacidad es nuevo, desde la invención de Facebook». **Ejercicio 2:** Discute el concepto de privacidad con tu familia, amigos, vecinos o compañeros de trabajo. ¿Qué has aprendido de lo que entiendes por privacidad y de lo que piensan otros sobre la misma? Recordatorio: puedes compartir vuestros puntos de vista (tuyos y de tus contactos) en el foro de la web de CSI-COP aquí: https://csi-cop.eu/forum/ (para publicar en el foro necesitarás registrarte en la web e iniciar sesión mediante este enlace: https://csi-cop.eu/citizenscientistlogin/)
Objetivo de los ejercicios	Comprender las *facetas de la privacidad*.
Propuesta de tuit	En la era del acceso móvil a Internet, ¿debería importar más la comodidad que la privacidad?

Lecturas adicionales para el paso 1	Los enlaces a las lecturas adicionales mencionados en este paso se pueden encontrar seleccionando el texto subrayado a continuación: **Lecturas recomendadas** —Lomas, N. (2021). *Answers being sought from Facebook over latest data breach*. Tech Crunch. Puedes leer el artículo en inglés en este enlace: https://tcrn.ch/3xfrTsE —Nayak, M. and Rosenblatt, J. (2021). *Google Must Face Suit Over Snooping on 'Incognito' Browsing* Bloomberg Technology. Puedes leer el artículo en inglés en este enlace: https://bloom.bg/3gFt4vV —The Real Facebook Oversight Board (la cuenta de la Junta de Supervisión de Facebook). Cuenta de Twitter: @Fboversight (https://twitter.com/FBoversight) **Lecturas adicionales** —Holroyd, M. (2021). «Ireland launches data protection inquiry into Facebook hack». *Euronews – Ireland*. Puedes leer el artículo en inglés en este enlace: https://bit.ly/3mOfIOM —Holvast, J. (2009). «History of Privacy». En V. Matyáš et al. (Eds.): *The Future of Identity*, IFIP AICT 298, págs. 13-42, 2009. IFIP International Federation for Information Processing 2009. Puedes leerlo en inglés en ResearchGate: https://www.researchgate.net/publication/225802214_History_of_Privacy

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	—Guardian (2022). *John Oliver on Data Brokers: What they can buy is pretty troubling*. Guardian Culture. 11 April 2022: https://bit.ly/3wzX0j3 —Nissenbaum, H. (2011). «A Contextual Approach to Privacy Online». *Dædalus*, *Journal of the American Academy of Arts & Sciences*, Vol. 140, Nº. 4 (Otoño 2011), págs. 32-48. Puedes leer el artículo en inglés en este enlace: https://www.amacad.org/publication/contextual-approach-privacy-online —Sax, M. (2018). «Privacy from an Ethical Perspective». Capítulo en: B. Van der Sloot & A. De Groot (Eds.), *The Handbook of Privacy Studies: An Interdisciplinary Introduction* (págs. 143-173). Amsterdam: Amsterdam University Press. Puedes leer el artículo en inglés en este enlace: 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, Nº. 5. (Dic. 15, 1890), págs. 193-220. Puedes leer el artículo en inglés siguiendo este enlace: The Right to Privacy on JSTOR

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

PASO 2

Título paso 2:	**Información y datos personales**
En este paso aprenderás a:	1. Describir y analizar las distintas facetas de la privacidad.
Tema	¿Qué son los datos personales?
Pregunta clave	*¿Por qué debería importarme quién tiene acceso a mis datos si no tengo nada que ocultar?* Pregunta a tus familiares y amigos qué piensan acerca de sus datos. Puedes compartir vuestros puntos de vista (tuyos y de tus contactos) en el foro de la web de CSI-COP aquí: https://csi-cop.eu/forum/ (para publicar en el foro necesitarás registrarte en la web e iniciar sesión mediante este enlace: https://csi-cop.eu/citizenscientistlogin/).
Breve resumen	Andreas Weigend (2017): «Cada vez que buscamos algo en Google, contactamos con alguien en Facebook, pedimos un Uber en algún lugar o incluso si simplemente encendemos una luz, creamos datos que las empresas recopilan». (Consulta la sección de lecturas adicionales al final de este paso).
Contenido	**¿Qué son los datos (*data*)?** Recapitulación: en el primer paso hemos introducido el concepto de «privacidad». En esta segunda etapa del curso de educación informal de CSI-COP, comprenderás «qué son los datos (data)» y qué «datos sobre ti» resultan involucrados en diferentes momentos de tu vida en línea; ya sea al comprar por Internet, enviar mensajes a amigos o durante la búsqueda de información, entre otros. En inglés, el singular de «data» (datos) es «datum»: Una única porción de *calidad* o *cantidad* sobre algo. «Data», en inglés, es un nombre colectivo (más que un único ítem): Puntos de información. Por ejemplo, *datos sobre ti*: —Si eres estudiante (tanto si eres estudiante «local» como internacional) —Fecha de nacimiento —Calificaciones para conseguir plaza en la universidad —Dirección postal (del hogar o de la residencia habitual durante el curso) —Número de contacto —… Los datos («data») están en todas partes y se almacenan de distintas formas: *Sin estructurar*: —Visionado de vídeos de YouTube —Consulta de las imágenes de Instagram —Lectura de correos electrónicos

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

—Imágenes por satélite
—Datos meteorológicos
—…

Estructurados:
—Número de identificación del estudiante o personal (cadena de números)
—Número de la Seguridad Social
—Reservas aéreas
—…

	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

Fuente de la imagen: https://bit.ly/2PhkKHa

Traducción de la imagen:

	Datos estructurados	Datos no estructurados
Características	—Modelos de datos predefinidos —Generalmente solo texto —Fáciles de buscar	—Modelos de datos no predefinidos —Puede tratarse de textos, imágenes, archivos de audio o vídeo u otros formatos —Difíciles de buscar
Almacenados en	—Bases de datos relacionales —Almacenes de datos	—Aplicaciones —Bases de datos NoSQL —Almacenes de datos —*data lakes*
Generados por	—Humanos o máquinas	—Humanos o máquinas
Aplicaciones más comunes	—Sistemas de reserva de vuelos	—Procesamiento de textos

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	—Control de inventario —Sistemas de gestión de la relación con los clientes —Sistemas de planificación de recursos empresariales	—*Software* de presentaciones —Envío de correos electrónicos a los clientes —Herramientas para la visualización o edición de medios
Ejemplos	—Fechas —Números de teléfono —Números de la Seguridad Social —Números de tarjetas de crédito —Nombres de clientes —Direcciones postales —Nombres y números de productos —Información sobre transacciones	—Archivos de texto —Informes —Mensajes de correo electrónico —Archivos de sonido —Archivos de vídeo —Imágenes —Imágenes de cámaras de vigilancia

Según Irwin (2021): «En determinadas circunstancias, cualquiera de los siguientes pueden considerarse *datos personales*»:
Un nombre y apellido
Una dirección postal
Una dirección de correo electrónico
Un número de tarjeta de identificación
Datos de localización
Una dirección de Protocolo de Internet (IP)
El identificador de publicidad de tu teléfono.

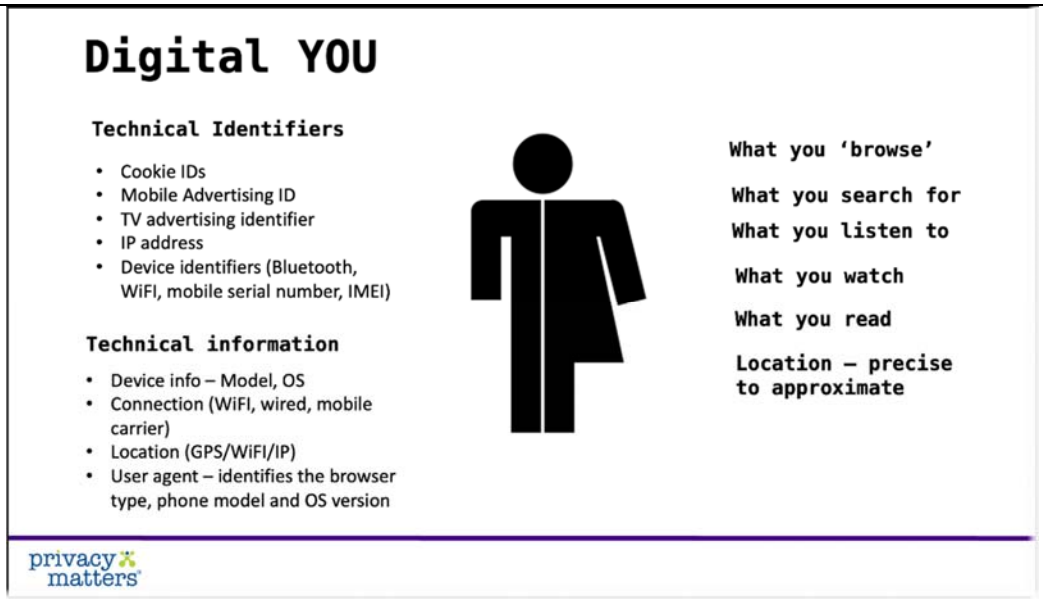
Los datos personales son datos que identifican a una persona «física» (viva).

Pat Walshe de **Privacy Matters** (Asuntos de Privacidad) dice: «Usamos nuestros teléfonos inteligentes y ordenadores como nunca antes para hacer llamadas; enviar

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	mensajes de texto e imágenes personales; enviar mensajes a la gente a través de los servicios de WhatsApp o Snapchat; comprar alimentos o medicinas en línea; compartir facetas personales de nuestras vidas en las redes sociales; buscar información sobre salud mental o física, política, religión o lugares para visitar; navegar por sitios web; dejar comentarios e indicar lo que nos gusta y lo que no; etc. Ser digital genera una gran cantidad de datos sobre nosotros, a menudo personales y sensibles. Datos que pueden permitir que otros nos conozcan mejor que nosotros mismos» (Privacy Matters). Podemos **ofrecer datos voluntariamente** cuando hacemos un pedido en línea o reservamos una cita médica y también se pueden **capturar y observar datos** sobre nosotros y nuestros dispositivos y comportamiento en línea (como los sitios web que visitamos, las canciones que escuchamos o las películas que vemos, el tipo de dispositivo que usamos o nuestras ubicaciones —ya sea que nos demos cuenta o no—). Los datos se pueden **deducir** cuando creamos un perfil y se analiza nuestra información (como qué usuario escuchó una canción o vio una película en línea, la categoría de la canción o película, en qué punto una persona pausó una canción o una película, junto con la fecha y el momento en que se hizo una pausa y se reinició o se dejó de escuchar o mirar, la ubicación en la que estaba —al menos el país—, etc.); datos, todos ellos, que son como una especie de sombra digital de las actividades en línea (Privacy Matters). Además de los datos personales, también hay **datos personales sensibles**. Según el reglamento general de protección de datos (RGPD), sobre el que aprenderemos más en el paso 4, los **datos personales confidenciales** pueden incluir datos que revelen tu/s: origen racial o étnico creencias religiosas opciones políticas afiliaciones sindicales Los datos personales sensibles también incluyen datos sobre la salud de una persona (mental o física, por ejemplo); datos sobre su vida sexual u orientación sexual; datos genéticos; datos biométricos (utilizados para identificar de forma única a alguien) y datos relacionados con condenas y delitos penales (Privacy Matters). En abril de 2021, Brodkin (2021) informó que T-Mobile: «empezará un nuevo programa que utilizará algunos datos que tenemos sobre usted (…) *incluyendo la información que obtenemos de los datos de uso de Internet y de su dispositivo* (como las aplicaciones instaladas en él) (…) y de las interacciones con nuestros productos y servicios, para uso publicitario propio y de terceros, a no ser que nos indique lo contrario». ¿Cómo te sentirías si tu operador de telefonía móvil te informara de que van a actuar como T-Mobile? O, si usas T-Mobile, ¿cómo te hace sentir su declaración sobre la recopilación y uso de tus datos?

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169



Traducción de la imagen: TU YO DIGITAL

Identificadores técnicos
—ID de *cookies*
—ID de publicidad móvil
—ID de publicidad televisiva
—Dirección IP
—Identificador de dispositivos (Bluetooth, wifi, número de serie del móvil, IMEI…)

Información técnica
—Información de dispositivo (modelo, sistema operativo)
—Conexión (wifi, cable, operador de telefonía móvil)
—Ubicación (GPS, wifi, IP)
—Agente de usuario (identifica el tipo de navegador, modelo del teléfono y sistema operativo)

¿Por dónde navegas?
¿Qué buscas?
¿Qué escuchas?
¿Qué miras?
¿Qué lees?
¿Dónde estás? (Ubicación más o menos precisa)

Qué esperar de los próximos pasos del curso

En la siguiente etapa (paso 3), comenzaremos a ver *cómo se rastrean nuestros datos*. En el paso 4, veremos qué *derechos tenemos sobre nuestra privacidad* y, en el punto final (paso 5), descubriremos qué *herramientas en línea podemos utilizar para asegurar mejor nuestra privacidad y proteger nuestros datos*.

Revisa tu aprendizaje

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	Comprueba lo que has aprendido en este paso respondiendo a la pregunta siguiente y realizando los dos ejercicios propuestos a continuación.
Revisa tu aprendizaje	¿Qué son los *datos personales*?
Ejercicios	**Ejercicio 1: test corto** ¿Cuáles de los siguientes nombres se relacionan con los datos personales? • Leonardo da Vinci • El presidente Joe Biden • Freddie Mercury • La reina Elizabeth II • Alan Turing • Meghan Markle • Albert Einstein • El Papa • Kim Kardashian (La respuesta a esta actividad la encontrarás en el siguiente paso). **Ejercicio 2** Busca y mira las charlas TED del «tec-sociólogo» **Zeynap Tufekci**. Por ejemplo, la charla TED Global NYC, de septiembre de 2017: **«Estamos construyendo una distopía solo para que la gente haga clic en los anuncios».** Recordatorio: Puedes compartir tus puntos de vista en el foro de la web de CSI-COP aquí: https://csi-cop.eu/forum/ (para publicar en el foro necesitarás registrarte en la web e iniciar sesión mediante este enlace: https://csi-cop.eu/citizenscientistlogin/
Objetivo de los ejercicios	Comprender *qué son los datos personales*.
Propuesta de tuit	La afirmación «no tengo nada que ocultar, así que no me importa quién tenga acceso a mis datos» es desacertada.

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Lecturas adicionales para el paso 2	Los enlaces para la lectura adicional mencionados en este punto se pueden ver seleccionando el texto subrayado. **Lecturas recomendadas:** Brodkin, J. (2021). *T-Mobile will sell your web-usage data to advertisers unless you opt out.* arsTECHNICA. Puedes leer el artículo en inglés aquí: https://bit.ly/3sUdkaQ Irwin, L. (2021). *Personal data vs. sensitive data: what's the difference?* IT Governance. Puedes leer el artículo en inglés aquí:https://bit.ly/3vhoRlX Privacy Matters en Twitter: @PrivacyMatters: https://twitter.com/privacymatters?lang=en Libro en inglés: Weigend, A. (2017). *Data for the people: how to make our post-privacy economy work for you*. Basic Books: New York

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

PASO 3

Título paso 3:	**Tecnologías de rastreo en línea**
En este paso aprenderás a:	1. Describir y analizar las distintas facetas de la privacidad. 2. Identificar y evaluar la forma en que se recopilan los datos personales mientras se navega por la web y se utilizan aplicaciones en los dispositivos inteligentes.
Tema	¿Cómo se recopilan los datos gracias a nuestro uso de Internet?
Pregunta clave	*¿Cuán peligrosas pueden resultar las tecnologías de rastreo en línea?* Pregunta a tus familiares y amigos qué piensan sobre sus datos. Puedes compartir vuestros puntos de vista (tuyos y de tus contactos) en el foro de la web de CSI-COP aquí: https://csi-cop.eu/forum/ (para publicar en el foro necesitarás registrarte en la web e iniciar sesión mediante este enlace: https://csi-cop.eu/citizenscientistlogin/).
Breve resumen	Nigel Warburton (2020): «Sin tu permiso (…) las empresas de tecnología recopilan tus datos —tu ubicación, lo que te gusta, tus hábitos, tus miedos, tus enfermedades, tus ideas políticas— y los comparten entre ellas». (Consulta la sección de lecturas adicionales al final de este paso).
Contenido	**Cómo se recopila tu información en Internet** Resumen de lo aprendido en los dos pasos anteriores En el paso 1 hemos introducido el concepto de «privacidad». En el paso 2 hemos aprendido que la expresión «datos personales» hace referencia a los datos sobre una persona física (y viva). En este punto vamos a ver algunas de las herramientas en línea que recopilan datos mientas usamos Internet. La *product manager* Eliza Crawford (2020) indica que la razón por la que se recopilan nuestros datos a través de Internet es para saber cómo nos comportamos cuando visitamos una web. Y ello se hace para «obtener información sobre cómo (…) los consumidores usan» los sitios web «para, así, proporcionales una experiencia personalizada en línea y monetizar al usuario mostrándole anuncios dirigidos». Al explicar por qué se produce el rastreo en línea, Crawford (2020) dice: • «Cuando buscas un restaurante en Google y el servicio te proporciona una lista de restaurantes cercanos es porque el motor de búsqueda sabe dónde te encuentras». • «Cuando una tienda de comercio electrónico te muestra una lista de productos recomendados, sabe lo que te gusta porque ha hecho un rastreo de los ítems que has mirado o comprado previamente». Pat Walshe (Privacy Matters) recuerda que **los datos de comportamiento** pueden incluir:

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	• Tus **datos de navegación**; es decir**,** los sitios web que visitas, la fecha y la hora en que lo haces y el país desde donde lo haces (deducido de tu dirección IP —una cadena única de caracteres que identifica cada dispositivo que se conecta a Internet y que se envía automáticamente al visitar una página web—). También hay que tener en cuenta que, cuando se abandona un sitio web, los propietarios de dicho sitio podrán saber qué sitio web se visita a continuación (y estos últimos saber de qué sitio se viene). Todo ello se considera «datos de comportamiento de navegación web». • **Comportamiento *clickstream* (flujo de clics)**; datos sobre las interacciones de una persona en un sitio web, que pueden incluir dónde hace clic, por dónde se desplaza en el sitio y qué toca en una pantalla táctil. • **Motores de búsqueda** como Google, que pueden almacenar información sobre tus búsquedas, los resultados en los que haces clic o tu dirección IP, y que pueden utilizar una ID exclusiva de *cookie* para rastrearte. • **Ubicación**; es decir, la localización y el tipo de lugares que se visitan (supermercado, casino, lugar de culto, hospital…), o el lugar donde se ha utilizado la aplicación, fechas y horas, trayecto recorrido, la frecuencia de una visita, etc. Los datos de ubicación/localización pueden ser muy reveladores y de naturaleza conductual. • **Historial de compras**; esto puede incluir distintos tipos de suscripciones (miembro de un sindicato, gimnasio, periódicos, etc.), reservas en hoteles o restaurantes que se hayan realizado a través de la búsqueda, mapas o asistentes virtuales, o directamente mediante los vendedores o servicios de terceros. • **Datos de pago o información transaccional**; es decir, los pagos que revelan a quiénes o a qué organizaciones se ha pagado (lo que puede informar sobre el tipo de organización receptora —clínica, farmacia, proveedor de alcohol, establecimiento de alimentos, librería, etc.—), y cuánto, cuándo y con qué frecuencia se ha hecho. Un buen ejemplo de ello son los pagos con tarjeta «tap&go» (un sistema de validación y pago mediante tarjeta *contactless*); piensa en el café que compraste al inicio de un viaje, el lugar, la fecha y la hora en la que lo hiciste, y los pagos que hiciste a lo largo del día con la misma tarjeta. • ***Streaming media*** (flujo de contenidos multimedia). «Eres lo que miras en *streaming*» (puedes leer los artículos en inglés: you are what you stream y They know what You Watched Last Night —«Saben lo que miraste anoche»—). o Los medios en *streaming* generan **muchos** datos de comportamiento sobre: o la fecha y la hora en que accediste a un servicio de música, audio o TV / películas en *streaming* y la ubicación no precisa (nivel de país o nivel de región) desde la que accediste, o qué perfil accedió y usó el servicio (nombre + categoría —por ejemplo: niño—), o la categoría de música, audiolibro, TV / película (por ejemplo: terror político, adultos), o las búsquedas de contenido,

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

- si paraste una canción o película y por cuánto tiempo (incluidas la/s fecha/s y la/s hora/s),
- si saltaste / abandonaste una canción o el audio de una película o de un episodio,
- si compartiste contenido y con quién, y tus interacciones con otros dentro del servicio,
- si puntuaste una canción, un programa de televisión o una película,
- las listas de reproducción o visualización creadas,
- el dispositivo utilizado para acceder al servicio, la dirección IP y los identificadores del dispositivo.

- **Datos sobre salud y actividad;** datos sobre el uso de aplicaciones de actividad física (como las relacionadas con ciclismo, *running*, senderismo, etc.) o datos sobre tu salud, como los que se pueden obtener mediante las aplicaciones dietéticas o de fertilidad.
- **Gráfico de redes sociales**; son datos que revelan las relaciones sociales interconectadas entre las personas, su naturaleza y los patrones de comunicación.

Un estudio de Ghostery (2017) «reveló que los rastreadores que recopilan datos sobre el comportamiento en línea de los usuarios de Internet están presentes en al menos el 79% de los sitios web (dominios únicos) a nivel mundial. El rastreo web se ha vuelto tan omnipresente que aproximadamente el 10% de los sitios web envían los datos recopilados a diez o más empresas diferentes (dominios de rastreo únicos). En términos de tráfico web, diez o más rastreadores controlan el 15% de todas las cargas de páginas en Internet. Según el estudio, los *scripts* de rastreo de Google (60,3% de las cargas de página) y Facebook (27,1%) son los más frecuentes».

Hemos oído hablar de las galletas en el Paso 1, del programa John Oliver, de HBO, del 10 de Abril de 2022: "Last Week Tonight" donde exponía a los “Data Brokers”.

Este rastreo se realiza mediante herramientas digitales como:

Cookies: Las *cookies* son pequeñas porciones de información que los sitios web almacenan en el dispositivo del usuario. Los sitios web suelen **utilizar las *cookies* para recordar las preferencias del usuario y brindar una experiencia personalizada, así como para obtener información con fines publicitarios**. Una vez que un sitio web ha colocado una *cookie* en el ordenador del usuario, el proveedor de dicha *cookie* puede seguir accediendo a ella. Así es como los sitios pueden usar *cookies* para rastrear a los usuarios de una página a otra o de un sitio a otro. El tiempo que una *cookie* puede

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	rastrear a un usuario depende del tipo de *cookie* y estas pueden ser temporales, persistentes, de origen, de terceros… (Crawford, 2020). **Huellas digitales**: La toma de huellas digitales es una forma de rastreo de sitios web que utiliza los atributos del dispositivo o navegador del usuario para crear un perfil de usuario. La información que se obtiene mediante las huellas digitales incluye tu dispositivo, el sistema operativo de este, la resolución de pantalla, el navegador y la versión del navegador, el idioma y la zona horaria. Crawford (2020) afirma: «Por sí sola, cada pieza de información no es tan valiosa. Sin embargo, cuando está todo junto, proporciona un modo increíblemente preciso de identificar a los usuarios. La Electronic Frontier Foundation (EFF) mantiene un sitio para «tapar las huellas» (se puede ver en el enlace: cover your tracks), que analiza tu navegador para mostrar cuán única es tu huella digital en relación con otras rastreadas por el sitio». **Rastreo de correo electrónico:** El ***software* de rastreo de correo electrónico** (*e-mail tracking*) **coloca un píxel de imagen invisible en los correos electrónicos que puede detectar la fecha y hora exactas en que se abre un correo electrónico.** El motivo de dicho rastreo es que las empresas ahorren tiempo y sepan si un primer correo te resulta suficientemente interesante como para abrirlo. Si no es el caso, es poco probable que abras futuros correos electrónicos de seguimiento. Al evitar los correos electrónicos de seguimiento innecesarios, el rastreo del correo electrónico ahorra tiempo tanto al vendedor como al destinatario del correo electrónico. Del mismo modo, si una empresa detecta que un contacto hace clic en los enlaces enviados y ve una carta de presentación o una propuesta adjunta, sabe que este contacto la tiene en mente en ese momento. Llegar a este punto en el que uno pueda estar pensando en la propuesta de una empresa (por ejemplo, comprar una prenda de ropa) hace que la conversación sea mucho más relevante (y oportuna para la empresa/vendedor). El estudio de Sivan-Sevilla *et al.* (2020) descubrió que «empresas de las que nunca hemos oído hablar recopilan datos de referencia sobre todos los aspectos de nuestras vidas: nuestros intereses, compras, estado de salud, ubicaciones y más». IAB (Interactive Advertising Bureau; 2019, citado en Sivan-Sevilla *et al.*, 2020). «Estos datos de referencia se combinan luego en perfiles de comportamiento excepcionalmente reveladores, que exponen partes íntimas de nuestra identidad y alimentan la industria de la publicidad multimillonaria, que afirma predecir lo que es probable que consumamos para poder orientarnos con anuncios». Sivan-Sevilla *et al.* (2020) informan, además, de que, cuando los anunciantes cruzan información sobre problemas médicos, intereses educativos y hábitos de consumo de noticias de los usuarios, están en condiciones de saber mejor cuándo un usuario puede convertirse en consumidor y tomar decisiones de compra que los anunciantes no podrían predecir de otra manera. Los estudios mostraron cómo los datos de diferentes sitios web se agrupan y utilizan para inferir sobre la demografía y los intereses de los usuarios, exponiéndolos a prácticas manipuladoras que intentan hacerlos hacer clic en el anuncio «correcto» (personalizado) en el momento «correcto» (personalizado).

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	La industria de la publicidad había definido estos momentos como «**momentos principales de vulnerabilidad de los consumidores**» (...) en los que los usuarios son «excepcionalmente receptivos». Srinivasan (2020) aclara que: «El auge de los anuncios electrónicos, ampliamente conocidos hoy como "publicidad programática", fue paralelo al aumento del comercio electrónico en varios sectores de la economía (...). La primera empresa de tecnología publicitaria, **Right Media**, lanzó el "intercambio publicitario" (**RMX**, por sus siglas en inglés Right Media Exchange), el **primer sitio de comercio electrónico para anuncios**. (...) Hoy en día, una sola empresa, **Google**, maneja simultáneamente el intercambio principal así como los intermediarios principales que los editores y anunciantes deben utilizar para comerciar. (...) Google no solo vende espacios publicitarios que pertenecen a sitios web de terceros, vende también espacio publicitario que aparece en sus propios sitios, como el motor de búsqueda de Google y YouTube». Srinivasan (2020) comenta que «el negocio de la publicidad ha cambiado drásticamente en las últimas dos décadas. Hoy en día, la mayor categoría de publicidad —la publicidad en línea— rara vez es negociada por personas, pues los avances tecnológicos permiten que el espacio publicitario se compre y venda electrónicamente a través de sitios de negociación centralizados a altas velocidades, sin que nadie se reúna cara a cara. Y, cuando un usuario visita un sitio web, el espacio publicitario de una página se enruta instantáneamente a uno o más de estos sitios. Allí, el espacio publicitario se subasta en tiempo real al mejor postor. Al terminar estas subastas, los anuncios de los anunciantes que han obtenido el espacio publicitario se muestran al usuario a tiempo para que se cargue la página y antes de que el usuario se dé cuenta de que ha ocurrido algo. El usuario solo ve anuncios dirigidos a él (uno de Barclays Bank, por ejemplo)». Es posible que ahora comprendas que cada vez hay una mayor cantidad de datos capturados, observados y deducidos por aquellos con los que tienes una relación directa, no solo para que puedan proporcionarte los servicios básicos que hayas solicitado, sino cada vez más para «personalizar experiencias», tanto si los has solicitado como si no, y/o para enviarte publicidad dirigida dentro y fuera de sus sitios web, aplicaciones y servicios. Pero tus datos no solo son capturados, observados y deducidos por aquellos con los que tienes una relación directa, sino también por terceros del ecosistema publicitario que pueden estar incrustados en los sitios web que visitas o en las aplicaciones que utilizas (para dirigirte publicidad conductual, por ejemplo). Tus datos pueden ser utilizados para seguirte a través de la web y las aplicaciones con fines de orientación conductual (como las ofertas en tiempo real que permiten a los anunciantes hacer ofertas automáticas para dirigirse a un público concreto en función de criterios específicos, como un rango de edad y sexo específicos, o tipo de dispositivo móvil o ubicación).

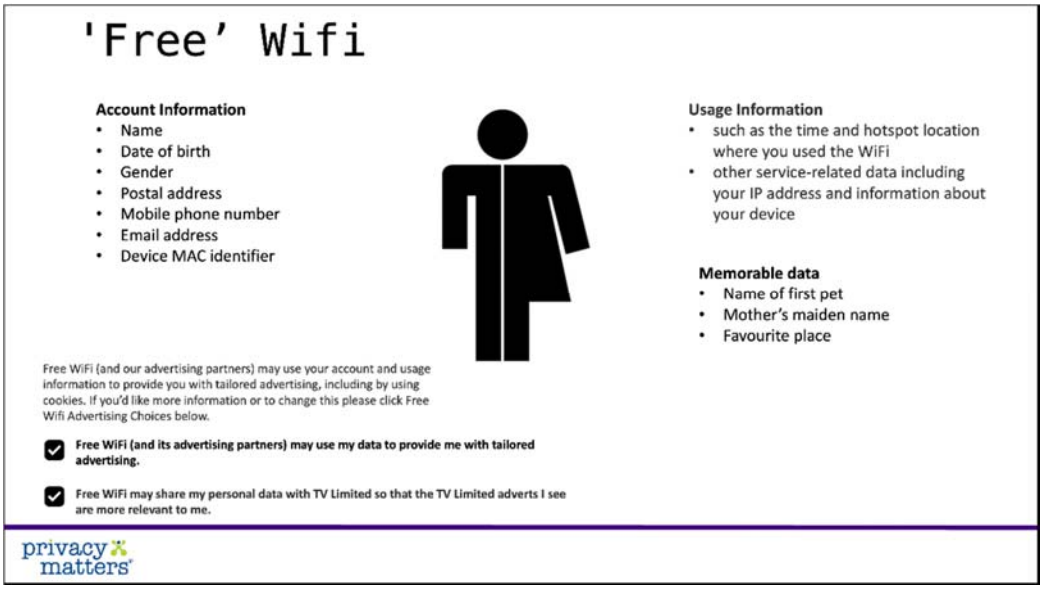
Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Por lo tanto, los datos sobre TI pueden ser muy personales y revelar aspectos íntimos de tu vida. Pueden afectarte de maneras que nunca habías imaginado, que infrinjan tus expectativas de privacidad, y que no la respeten ni protejan. Por ejemplo, se descubrió que la aplicación Grindr comparte información con una «gran cantidad de terceros» involucrados en la creación de perfiles y publicidad. Los datos compartidos «incluyen dirección IP, ID de publicidad, ubicación GPS, edad y sexo». Esto dio lugar a una investigación por parte de la autoridad noruega de protección de datos que multó a Grindr con 100 millones de coronas (el equivalente a 8,6 millones de libras esterlinas o unos 10,11 millones de euros).

Todos los tipos de datos vistos hasta ahora son datos personales protegidos por leyes de protección de datos, como el RGPD o la ley de privacidad electrónica europea (la Directiva de privacidad electrónica — «ePD», por sus siglas en inglés: ePrivacy Directive—), que discutiremos en el siguiente punto (paso 4) del curso de aprendizaje informal de CSI-COP. Estas leyes imponen obligaciones a las organizaciones del sector público y privado que capturan, observan y deducen datos sobre los usuarios y otorgan derechos sobre ese uso. Nuevamente, esto se discutirá en el paso 4 del curso.

Pero, primero, tómate un momento y piensa en lo que dicen tus datos sobre TI y sobre OTROS a los que estás conectado.

Ten en cuenta, también, que, si usas wifi gratuito, tienes que proporcionar información personal para acceder a Internet. Mira la imagen siguiente para ver qué se recopila en este caso:

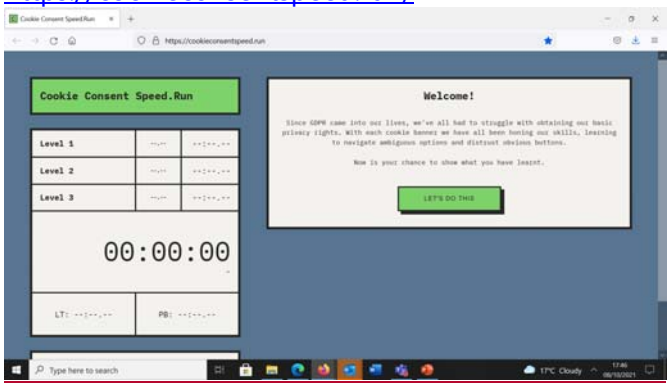


Traducción de la imagen: WIFI «GRATUITO»
Información de cuenta
—Nombre
—Fecha de nacimiento
—Género
—Dirección postal

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	—Número de teléfono móvil —Dirección de correo electrónico —Identificador MAC del dispositivo Información de uso —como la hora y la ubicación del punto de acceso desde el que se ha accedido al wifi —otros datos relacionados con el servicio, incluida tu dirección IP e información sobre tu dispositivo Datos recordatorio —Nombre de la primera mascota —Apellido de la madre —Lugar favorito —… El wifi gratuito (y nuestros socios publicitarios) pueden usar tu cuenta y la información de uso para mostrarte publicidad personalizada, incluso mediante el uso de *cookies*. Si deseas obtener más información o cambiarlo, haz clic en las opciones de publicidad del wifi gratuito que verás a continuación. *El wifi gratuito y sus socios publicitarios pueden usar mis datos para proporcionarme publicidad personalizada *El wifi gratuito puede compartir mis datos personales con TV Limited, para que los anuncios de TV Limited que vea sean más relevantes para mí. <u>Qué esperar de los próximos pasos del curso</u> En el siguiente punto (paso 4) veremos qué *derechos tenemos sobre nuestra privacidad*. Al final de este curso, en el paso 5, aprenderemos *las herramientas en línea que* podemos usar para *asegurar* mejor *nuestra privacidad y proteger nuestros datos*. <u>Revisa tu aprendizaje</u> Revisa lo aprendido en esta fase (paso 3). La respuesta al primer ejercicio del paso 2 podrás encontrarla en el apartado de ejercicios del presente paso.
Revisa tu aprendizaje	¿Cuáles son los distintos tipos de Cookies? ¿Qué es la huella digital? ¿Cómo funciona el rastreo del correo electrónico?
Ejercicios	**Respuesta al ejercicio 1 del paso 2** El primer ejercicio del paso anterior te pedía que identificaras cuáles eran datos personales de una lista de nombres. Dado que los datos personales se refieren exclusivamente a personas físicas (vivas), los nombres de la lista que refieren a personas muertas no son datos personales. ¿Lo hiciste bien? Verifícalo a continuación: 1. Leonardo da Vinci —no es un dato personal 2. El presidente Joe Biden

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	3. Freddie Mercury —no es un dato personal 4. La reina Elizabeth II 5. Alan Turing —no es un dato personal 6. Meghan Markle 7. Albert Einstein —no es un dato personal 8. El Papa 9. Kim Kardashian **Paso 3. Ejercicio 1** 1. Busca en la web los diferentes tipos de *cookies* que se pueden incrustar en los sitios web. 2. ¿Cuál es la diferencia entre la toma de huellas digitales y el rastreo de correo electrónico? **Paso 3. Ejercicio 2** Discute con la familia, amigos, vecinos o compañeros de trabajo lo que entendéis por «**elaboración de perfiles de comportamiento en línea**» y cómo se realiza a través de la web. **Paso 3. Ejercicio 3** Prueba este juego online gratis para saber si puedes evitar las cookies: https://cookieconsentspeed.run/  Recordatorio: Puedes compartir vuestros puntos de vista (tuyos y de tus contactos) en el foro de la web de CSI-COP aquí: https://csi-cop.eu/forum/ (para publicar en el foro necesitarás registrarte en la web e iniciar sesión mediante este enlace: https://csi-cop.eu/citizenscientistlogin/)
Objetivo de los ejercicios	Obtener más información sobre la elaboración de perfiles de comportamiento en línea.
Propuesta de tuit	Tecnologías de rastreo

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Lecturas adicionales para el paso 3	Los enlaces para la lectura adicional mencionados en este punto se pueden ver seleccionando el texto subrayado. **Lecturas recomendadas** Crawford, E. (2020). *Website Tracking: Why and How do Websites Track you?* CookiePro Blog: Cookie Compliance. Puedes leer el artículo en inglés aquí: https://www.cookiepro.com/blog/website-tracking/ EFF (sin fecha). *The Electronic Frontier Foundation. The leading non-profit defending digital privacy, free speech, and innovation for 30 years and counting!* Puedes leer el artículo en inglés en el enlace anterior y consultar la web aquí:https://www.eff.org/ Ghostery (2017). 79 *Percent of Websites Globally Are Secretly Tracking Your Personal Data.* Ghostery. Puedes leer el artículo en inglés aquí:https://www.ghostery.com/press/ghostery-global-tracking-study/ Privacy Matters en Twitter: @PrivacyMatters (https://twitter.com/privacymatters?lang=en) **Lecturas adicionales** Sivan-Sevilla, I., Chu, W., Liang, X. and Nissenbaum, H. (2020). *Unaccounted Privacy Violation: A Comparative Analysis of Persistent Identification of Users Across Social Contexts*. Federal Trade Commission (FTC) PrivacyCon 2020. Puedes leer el artículo en inglés 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. Puedes leer el artículo en inglés aquí: https://law.stanford.edu/publications/why-google-dominates-advertising-markets/ Libro en inglés: Warburton, N. (2020) cubierta interior del libro de Véliz, C. (2020). *Privacy is Power: Why and how you should take back control of your data*. Penguin Hardback.

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

PASO 4

Título paso 4:	**Tu derecho a la privacidad**
En este paso aprenderás a:	1. Describir y analizar las distintas facetas de la privacidad. 2. Identificar y evaluar la forma en que se recopilan los datos personales mientras se navega por la web y se utilizan aplicaciones en los dispositivos inteligentes. 3. Comprender los derechos a la privacidad que surgen de los estatutos para la protección de datos.
Tema	Derechos a la privacidad: Carta de Derechos Humanos de la ONU; Carta de la UE sobre derechos humanos ; RGPD
Pregunta clave	*¿Qué derecho tengo a la privacidad?* Pregunta a tus familiares y amigos qué piensan sobre su derecho a la privacidad. Puedes compartir vuestros puntos de vista (tuyos y de tus contactos) en el foro de la web de CSI-COP aquí: https://csi-cop.eu/forum/ (para publicar en el foro necesitarás registrarte en la web e iniciar sesión mediante este enlace: https://csi-cop.eu/citizenscientistlogin/).
Breve resumen	Estatutos y reglamentos que incluyen los derechos humanos con respecto a la privacidad.
Contenido	**Derecho fundamental a la privacidad** Para recapitular lo aprendido hasta ahora: En el primer paso vimos el concepto de «privacidad». En el segundo paso aprendimos que los «datos personales» se refieren a una persona física (viva). En el tercer paso descubrimos algunas de las formas en las que se pueden capturar nuestros datos en línea (a través de las *cookies*, por ejemplo). En este paso exploraremos los «derechos humanos». Pat Walshe, de Privacy Matters, nos recuerda que los derechos humanos importan desde hace mucho tiempo. Ya desde 1689, en Gran Bretaña, por ejemplo, los derechos humanos se consideraban algo esencial para poder considerarnos humanos, para nuestra dignidad y para proteger los derechos y libertades básicos (Biblioteca Británica, 2013). Derechos y libertades que hoy dan forma a diferentes dimensiones de nuestras vidas —*offline* y *online*—: desde el derecho a expresar opiniones, al derecho a asociarse libremente con otros y a la libertad de reunión, pasando por la libertad de religión, el derecho a la educación, el derecho a un juicio justo, el derecho a contraer matrimonio o el **derecho a la privacidad**, por ejemplo. Los derechos humanos importan, todos los días, *offline* y *online*, pues nos permiten prosperar como seres humanos. Más tarde, en **1948**, los derechos humanos adquirieron importancia global. En respuesta a las atrocidades cometidas durante la Segunda Guerra Mundial, la Asamblea General de las Naciones Unidas adoptó la Declaración Universal de

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	Derechos Humanos (**DUDH**) para proteger los derechos humanos básicos que todas las personas deberían tener. Esto incluye la protección contra la interferencia arbitraria en la **privacidad**, la **familia**, el **hogar** o la **correspondencia personal,** según el artículo 12 de la DUDH. En 1949, varios países europeos formaron el Consejo de Europa (**CoE**), que actualmente cuenta con 47 estados europeos. En **1950**, el Consejo de Europa adoptó el Convenio Europeo de Derechos Humanos (CEDH), nuevamente para protegernos, en el futuro, contra atrocidades como las cometidas durante la Segunda Guerra Mundial. El CEDH incorpora derechos clave que se encuentran en la DUDH y entró en vigor en **1953.** El CEDH es el primer instrumento **internacional legalmente vinculante** que protege los derechos humanos. Cabe destacar que todos los estados miembros de la Unión Europea (UE) se han adherido al CEDH. El artículo 8 del CEDH establece que toda persona tiene derecho al respeto de su **vida privada** y **familiar**, así como de su **domicilio** y **correspondencia**. Es fácil ver cómo ese derecho está destinado a proteger los aspectos íntimos de la vida de una persona; aspectos fáciles de observar *online*. Si bien el artículo 8 del CEDH protege el derecho a la privacidad, también incluye el derecho a la protección de datos, dado que el uso de información personal no solo influye en la privacidad de las personas, sino también en otros derechos y libertades, como veremos en este curso. Para ayudar a proteger a las personas, sus derechos y libertades y, en particular, el derecho a la privacidad, en 1981 el **CoE** adoptó un conjunto de principios y reglas que se aplican al procesamiento de información personal. Dichos principios y reglas se conocen como «Convención 108». La Convención se actualizó recientemente para reflejar los cambios en la tecnología y el uso de datos que pueden afectar negativamente los derechos de las personas, y ahora se conoce como Convención 108+. En **2000,** la UE estableció la Carta de los Derechos Fundamentales de la UE. La Carta se convirtió en legalmente vinculante para los estados miembros de la UE en 2009. Al igual que el CEDH, la Carta de los Derechos Fundamentales de la **UE** establece que todas las personas tienen derecho al respeto de su **vida privada** y y **familiar**, su **hogar** y sus **comunicaciones** (artículo 7). Además, la Carta también establece que todas las personas tienen derecho a la protección de sus datos personales (artículo 8). Los artículos 7 y 8 de la Carta, respectivamente, establecen el derecho a la privacidad y la protección de datos como dos derechos distintos. Estos derechos se hacen efectivos mediante un **instrumento de privacidad electrónica** conocido como la Directiva de privacidad electrónica de la UE (que se aplica a elementos como *cookies* y otras técnicas de rastreo en línea) y un instrumento de protección de datos, el Reglamento General de Protección de Datos de la UE (**RGPD**). Las normas de protección de datos de la UE y las del **CoE** se han implementado en la legislación de los estados miembros y se han reforzado para reflejar los cambios en la tecnología y los cambios en el uso de datos. Hoy en día, cuando las personas utilizan sus teléfonos móviles, ordenadores portátiles, etc., sus datos pueden ser recogidos en tiempo real y

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	compartidos entre cientos de terceros (los anunciantes, por ejemplo); a menudo, de un modo en el que la gente no es realmente consciente de ello o sin que tenga opciones significativas para evitarlo. Dichos datos pueden revelar aspectos de la vida privada de una persona, como su ubicación, sus hábitos de compra, los sitios web que visita o quiénes son sus contactos y sus conexiones sociales. En la web de la Oficina del Comisionado de Información del Reino Unido (ICO) se explica que «el reglamento general de protección de datos (RGPD) de 2018 otorga a las personas el derecho a ser informadas sobre la recopilación y el uso de sus datos personales. **Este es un requisito clave de transparencia**» (se puede ver en el siguiente enlace: https://bit.ly/2QxmZH1). Pat Walshe, de Privacy Matters, afirma:«El derecho a la privacidad y a la protección de datos son más importantes que nunca, ya que nuestros datos digitales revelan aspectos profundamente personales e íntimos de nosotros mismos y de aquellos con quienes estamos conectados».  Traducción de la imagen: La privacidad *online* ~~está muerta~~ es tu derecho fundamental. <u>Qué esperar del próximo paso del curso</u> En el último punto de este curso, paso 5, aprenderemos *qué herramientas en línea podemos usar* para *asegurar mejor nuestra privacidad y proteger nuestros datos*. <u>Revisa tu aprendizaje</u> Comprueba lo que has aprendido en este paso respondiendo al minicuestionario que vas a encontrar en el apartado de ejercicios.
Revisa tu aprendizaje	**Declaración Universal de los Derechos Humanos de 1948 (DUDH)**: **Artículo 12**: «Nadie será objeto de injerencias arbitrarias en su privacidad (...) [o] correspondencia». **Carta de los Derechos Fundamentales de la UE de 2000 (CEDH): Artículo 1**: «La dignidad humana es inviolable. Debe ser respetada y protegida». **El Reglamento General de Protección de Datos (RGPD) de 2018 «establece un alto estándar para el consentimiento»**; este consentimiento ***informado*** implica: • «ofrecer a las personas opciones y control reales», • «el consentimiento genuino debe poner a las personas al frente, generar confianza y compromiso».

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Ejercicios	**Minicuestionario** sobre las distintas cartas y reglamentos. ¿Las siguientes afirmaciones son verdaderas o falsas? • El UNHR (United Nations Human Rights) es un nuevo reglamento que otorga el consentimiento informado. • La Directiva sobre Privacidad Electrónica se refiere a las *cookies*. • El RGPD no se preocupa por la transparencia. Discute tus respuestas con familiares, amigos, vecinos o compañeros de trabajo. Recordatorio: Puedes compartir vuestros puntos de vista (tuyos y de tus contactos) en el foro de la web de CSI-COP aquí: https://csi-cop.eu/forum/ (para publicar en el foro necesitarás registrarte en la web e iniciar sesión mediante este enlace: https://csi-cop.eu/citizenscientistlogin/)
Actividad final	Discusión con otros científicos ciudadanos sobre la declaración de 1999 del director ejecutivo y cofundador de Sun Microsystems, Scott McNealy: **«De todos modos, tienes cero privacidad… Supéralo».** Citado en Wired: https://www.wired.com/1999/01/sun-on-privacy-get-over-it/
Propuesta de tuit	La privacidad *online* no es un lujo.

Lecturas adicionales para el paso 4	Los enlaces para la lectura adicional mencionados en este punto se pueden ver seleccionando el texto subrayado. **Lecturas recomendadas** British Library (2013). *Taking Liberties: The struggle for Britain's freedoms and rights. Taking Liberties – Star Items Index – Human Rights.* Puedes leer el artículo en inglés aquí:https://bit.ly/2QU4bSa ICO (sin fecha). *Guide to the General Data Protection Regulation (GDPR): Right to be informed.* UK Information Commissioner's Office (ICO). Puedes leer el artículo en inglés aquí:https://bit.ly/3erd79K **Lecturas adicionales** EHCR (sin fecha). *European Convention on Human Rights*. (Convención europea de los derechos humanos). Puedes consultarlo en inglés 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 Parlamento y Consejo Europeos de julio de 2002, relacionada con el procesamiento de datos personales y la protección de la privacidad en el sector de las comunicaciones electrónicas). Puedes consultarla en inglés aquí: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	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)*. (Reglamento EU 2016/679 del Parlamento y Consejo europeos sobre la protección de las personas físicas en relación con el procesamiento de datos personales y sobre la libre circulación de dichos datos, derogando la Directiva 95/46/EC —Reglamento General de la Protección de Datos—). Puedes consultarlo en inglés aquí: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN UN (sin fecha). *United Nations Declaration of Human Rights*. (Declaración de los Derechos Humanos de las Naciones Unidas). Puedes consultarla en inglés aquí: https://www.un.org/en/about-us/universal-declaration-of-human-rights

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

PASO 5

Título paso 5:	**Cómo proteger tus datos en línea**
En este paso aprenderás a:	1. Describir y analizar las distintas facetas de la privacidad. 2. Identificar y evaluar la forma en que se recopilan los datos personales mientras se navega por la web y se utilizan aplicaciones en los dispositivos inteligentes. 3. Comprender los derechos a la privacidad que surgen de los estatutos para la protección de datos.
Tema	Herramientas para proteger tus datos en línea
Pregunta clave	*¿Cómo cambiar la configuración de navegación web y de las aplicaciones para detener el rastreo en línea?* Cuando lo descubras, cuéntale a tu familia y amigos las herramientas que pueden ayudarlos a proteger sus datos en línea. Puedes compartir vuestros puntos de vista (tuyos y de tus contactos) en el foro de la web de CSI-COP aquí: https://csi-cop.eu/forum/ (para publicar en el foro necesitarás registrarte en la web e iniciar sesión mediante este enlace: https://csi-cop.eu/citizenscientistlogin/).
Breve resumen	**Aplicaciones**: Verifica los permisos en el apartado «Configuración» de las aplicaciones existentes en tus dispositivos móviles. Antes de descargar una aplicación, comprueba qué permisos solicita: ¿son necesarios para que la aplicación funcione? Por ejemplo, una aplicación de transporte necesitará acceder a tu ubicación para que la aplicación proporcione información precisa. **Sitios web**: Utiliza un navegador con principio de privacidad en el diseño y por defecto (*privacy-by-design*) o actualiza la configuración para evitar el rastreo y limitar las *cookies* de publicidad y marketing de terceros.
Contenido	**Herramientas en línea que pueden ayudarte a proteger tus datos y tu privacidad** Para recapitular lo aprendido hasta ahora: En el primer paso vimos el concepto de «privacidad». En el segundo paso aprendimos que los «datos personales» se refieren a una persona física viva. En el tercer paso descubrimos algunas de las formas en las que se pueden capturar nuestros datos en línea (a través de las *cookies*, por ejemplo). En el paso 4 vimos los distintos estatutos/cartas y reglamentos que te otorgan derecho a la privacidad. En este paso descubriremos de qué herramientas en línea disponemos para proteger nuestros datos y nuestra privacidad. Piensa en tu uso de Internet: ¿sientes que controlas cada vez más tu vida *online*? Pat Walshe (Privacy Matters) señala que nos conectamos a Internet para: comprar, hacer videollamadas, enviarnos mensajes, compartir experiencias y pensamientos

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	mediante las redes sociales. Y también lo hacemos para pedir citas médicas, buscar información (incluso sobre problemas de salud), encontrar y seguir indicaciones de viajes, para viajar en transporte público o en coche, bicicleta o a pie. Asimismo, utilizamos la red para escuchar música o audios y ver películas o la televisión. Gran parte de nuestras vidas se ha vuelto digital, pero volverse digital genera y deja huellas, datos digitales que pueden recopilarse y utilizarse para crear nuestro perfil y aprender sobre nosotros, y así influir en nosotros de formas que quizás no sepamos. Cada página web que visitas, cada clic que haces, cada llamada o mensaje que envías o recibes, cada publicación que haces en las redes sociales, cada lugar que visitas o «etiquetas», cada «me gusta» que publicas, cada canción que escuchas o cada película que miras (y los detalles de cuándo lo haces, si haces una pausa, si adelantas la reproducción o te saltas una canción o película)... todo ello crea datos sobre ti. Dichos datos revelan aspectos de tu comportamiento, aspectos sobre TI y, a menudo, aspectos íntimos sobre ti (por ejemplo, las aplicaciones de fertilidad, que te conocen íntimamente). Consulta el siguiente artículo (en inglés) de la revista Wired (2018): «Before using birth control apps, consider your privacy» (antes de usar una aplicación para el control de natalidad, considera tu privacidad). Lo puedes leer en: https://bit.ly/3ajCyZz. Adicionalmente, en un artículo de 2020 en The Guardian, una organización benéfica sobre privacidad informó que «las aplicaciones para el control de la menstruación almacenan información excesiva». Puedes leer el artículo en inglés aquí: https://bit.ly/3aj7IQH Luego están las aplicaciones que comparten aspectos íntimos de la sexualidad, religión o ubicación de una persona, por ejemplo (y hay que tener en cuenta que los datos de «ubicación» ya pueden sugerir mucho sobre ello, ya sea que una ubicación indique un lugar de un tipo específico de culto o una clínica de salud de un tipo específico). Puedes leer el informe de Consumer Reports de 2020 sobre dichas aplicaciones aquí: https://bit.ly/3ggUw2x También existen aplicaciones dirigidas a niños y adolescentes/adultos jóvenes que capturan datos, quizás sin el conocimiento del niño o adolescente que se ha descargado la aplicación, o sin el conocimiento de los padres que podrían haber comprado una aplicación para su hijo en un dispositivo inteligente. Yubo es una "aplicación de redes sociales" dirigida a niños y niñas para ayudarles a encontrar amistades. El diario británico Sunday Times informó sobre los problemas de salvaguardia de la aplicación en su edición del 20 de febrero de 2022. Puede leer parte de este informe del Sunday Times en la siguiente imagen:

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

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

Más adelante en este paso 5 conoceremos las herramientas online gratuitas que hay bajo aplicaciones como Yubo para saber si hay problemas de privacidad de datos en esta u otras aplicaciones dirigidas a los niños.

Pero todos estos datos revelan no solo aspectos sobre TI, sino también aspectos de OTROS; de aquellos con quienes te comunicas y compartes información, de tus relaciones y patrones de comunicación. Por ejemplo, una aplicación puede pedirte que cargues o le des acceso a los «contactos» que tienes en tu ordenador o *smartphone*. Pero ¿qué es un contacto? Un contacto puede incluir el nombre de una persona, su foto, su número de teléfono móvil, su dirección de correo electrónico, su dirección postal, el nombre de usuario de la red social, su fecha de aniversario... Al ser digitales en línea, quizá debemos pensar no solo en nuestra propia privacidad, sino también en la privacidad de los demás.

Tal como vimos en el paso 4, en la UE y el Reino Unido, el derecho a la privacidad en línea está protegido por leyes específicas de **privacidad electrónica** y por el Reglamento General de Protección de Datos (**RGPD**); pero, aunque las leyes y su aplicación pueden hacer mucho, hay cosas que tú también puedes hacer para ayudar a proteger tu privacidad en línea.

En el tercer paso descubrimos cómo se rastrea a las personas **a través de la web**, lo que incluye el rastreo a través de la tecnología publicitaria (*ad tech*, en inglés), como serían las *cookies* o el rastreo por parte del servidor. Pero ¿qué puedes hacer tú para controlar y proteger tu privacidad en línea? La autogestión de la privacidad es difícil. Puedes obtener más información sobre cómo se realiza el rastreo de los individuos **a través de las aplicaciones móviles** (kits de desarrollo de *software* —SDK—) si lees el

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	artículo de Binns *et al.* (2018): *Third Party Tracking in the Mobile Ecosystem*. Puedes encontrar el artículo en inglés aquí: https://arxiv.org/pdf/1804.03603.pdf . **Herramientas para descubrir y controlar el rastreo:** **<u>Herramientas de transparencia (web):</u>** Hay varias herramientas que pueden ayudarte a comprender qué tipo de rastreo se produce en las páginas que visitas. Gran parte de dicho rastreo se lleva a cabo para hacerte llegar publicidad dirigida o para «personalizar» tu experiencia. A menudo, ello incluye compartir datos con empresas de publicidad de terceros, a veces cientos de ellas. **Algunas de las herramientas de transparencia web son:** **—Webbkoll** es una herramienta que simula lo que sucede cuando un usuario visita una página web usando un navegador típico. Muestra qué *cookies* propias y de terceros pueden estar presentes en la página visitada y también qué rastreo se realiza independientemente de las *cookies*, como las solicitudes realizadas por los servidores. https://webbkoll.dataskydd.net/en **—Blacklight** escanea un sitio web e indica la tecnología de rastreo clave del mismo. https://themarkup.org/blacklight **—Pagexray** es una herramienta de análisis que muestra todos los anuncios y rastreadores cargados en una página web y que presenta los resultados en un gráfico de árbol. Los resultados se pueden descargar como archivo HTTP (.har.json) o como resultados detallados (.json) https://pagexray.fouanalytics.com/ **—Request Map Generator** ayuda a identificar qué terceros hay en un sitio web y dónde se transmiten los datos. Los resultados se pueden descargar en un archivo CSV. https://requestmap.webperf.tools **—Cover Your Tracks** es una herramienta que analiza la protección de tu navegador contra el rastreo y la toma de huellas digitales. https://coveryourtracks.eff.org **<u>Herramientas de transparencia (aplicaciones móviles):</u>**

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Examinar las aplicaciones móviles no es tarea fácil.
O'Flaherty, un periodista especializado en ciberseguridad, afirma que, cuando utilizas una aplicación en tu teléfono, esta «puede rastrearte a través de otras aplicaciones y sitios web para enviarte publicidad dirigida. Actualmente, esto se hace a través de algo llamado identificador para anunciantes (**IDFA**, por sus siglas en inglés), una herramienta que rastrea sin revelar tu información personal».

En todo caso, existen algunas herramientas para ayudar a arrojar luz sobre la existencia de «rastreadores» integrados en las aplicaciones de Android.

Una herramienta clave para Android es **Exodus Privacy** (https://exodus-privacy.eu.org/en/).
Android Studio: https://developer.android.com/studio.

Pat Walshe (Privacy Matters) advierte que actualmente no hay una herramienta equivalente para las aplicaciones iOS de Apple. Sin embargo, Apple ha introducido nuevas normas de transparencia, para su tienda y sus desarrolladores, con las que se exige el uso de etiquetas de privacidad predefinidas para revelar qué datos se utilizan y por qué. El nuevo iOS 14.5 de Apple también requiere a los desarrolladores que «obtengan el permiso del usuario antes de rastrear sus datos en aplicaciones o sitios web propiedad de otras empresas cuando sea con fines publicitarios o para compartir los datos con corredores de datos (*data brokers*)».

Según Apple, esta nueva función de privacidad permite a los propietarios de teléfonos de Apple con este sistema operativo que «cliquen sobre el Informe de Privacidad para entender mejor cómo los sitios web tratan la privacidad de los usuarios» (Apple, 2021). De nuevo según Apple, su función de transparencia en el rastreo de las aplicaciones (App Tracking Transparency —ATT—) «requerirá que todas las aplicaciones soliciten permiso explícito para realizar un rastreo» y «en el apartado de Configuración, los usuarios podrán ver qué aplicaciones han solicitado permiso para realizar un rastreo y podrán realizar los cambios que consideren oportunos» (O'Flaherty, 2021).

En el Mac OS («Big Sur»), Apple proporciona una herramienta de informe de privacidad que aparece como un icono en el navegador Safari, lo que permite a los usuarios ver qué rastreadores hay en una página web y cuáles se bloquean. El navegador Safari de Apple «te ofrece varias maneras de ayudarte a proteger tu privacidad» (Apple, 2021). La iniciativa de privacidad de Apple supone un «punto de inflexión» según O'Flaherty (2021).
Y con «la muerte de las *cookies* de terceros» (Cyphers, 2021), los científicos ciudadanos podrían convertirse en la fuerza que impida que cualquier sustituto (como el «nuevo conjunto de tecnologías de Google para la publicidad dirigida en la web») nos rastree en línea, lo que nos llevaría más cerca de la privacidad a la hora de navegar.

Recapitulación: ¿Qué puedes hacer para proteger tu privacidad?
—Navegadores

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	—Bloqueadores de anuncios —Uso de la configuración de privacidad (en los sistemas operativos, navegadores, aplicaciones…) 
Revisa tu aprendizaje	Revisa lo aprendido en este paso al comprender que existen formas de proteger tus datos y tu privacidad cuando estás en línea.
Ejercicios	Aprendizaje experiencial: explora los sitios web que visitas y las aplicaciones que utilizas, y descubre qué rastreadores digitales tienen instalados, si los hay. **Ejercicio 1:** Utiliza una de las herramientas que hemos visto en este paso (como webbkoll) para ver qué se esconde bajo las páginas web que sueles visitar. Consulta el sitio web para ver su a) su política de privacidad y su b) política de *cookies*. Preguntas —¿Te resulta fácil entender la política de privacidad? —¿La política de *cookies* informa sobre alguna de estas o sobre su cantidad? —¿Qué *cookies* incrustadas de terceros se dan a conocer en la política de *cookies*? **Ejercicio 2** Verifica los permisos de una aplicación en tu dispositivo móvil inteligente. Ve al apartado de «Configuración», selecciona cualquier aplicación y verifica sus permisos. Preguntas —¿Qué permisos se han otorgado a la aplicación que has consultado? —Cuando descargaste la aplicación, ¿eras consciente de estos permisos? Recordatorio: Puedes compartir tus puntos de vista sobre lo aprendido en este punto en el foro de la web de CSI-COP aquí: https://csi-cop.eu/forum/ (para publicar en el foro necesitarás registrarte en la web e iniciar sesión mediante este enlace: https://csi-cop.eu/citizenscientistlogin/).

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Objetivo de los ejercicios	Pasar de ser un aprendiz informal a un científico ciudadano CSI-COP. Comenta tu opinión sobre este curso/taller con tus familiares y amigos: —¿Qué crees que has ganado al seguir los cinco pasos del aprendizaje informal CSI-COP? —¿Te gustaría unirte al equipo de CSI-COP y convertirte en un científico ciudadano para investigar el rastreo en línea? —¿Te interesaría seguir aprendiendo sobre la protección de datos, la privacidad, el desarrollo web y otros temas relacionados?
Propuesta de tuit	Protejo mis datos con herramientas web.
Lecturas recomendadas para el paso 5	Cyphers, B. (2021). *Google's FLoC (Federated Learning of Cohorts) is a terrible idea.* Electronic Frontier Foundation. Puedes leer el artículo en inglés 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*. Puedes leer el artículo en inglés aquí:https://bit.ly/3vpOq4v/

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Valoración del curso

Tus comentarios sobre el curso de educación informal «CSI-COP: tu derecho a la privacidad en línea»:	Al equipo de CSI-COP, nos sería muy útil saber qué te ha parecido este curso, por lo que te agradecemos que selecciones una de las opciones de la lista siguiente: 5. Muy útil 4. Útil 3. No lo sé 2. Poco útil 1. Nada útil No dudes en añadir cualquier otro comentario o sugerencia que puedas tener sobre el curso:

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Evalúa tu aprendizaje

Para evaluar tu aprendizaje y obtener un certificado CSI-COP, responde las preguntas siguientes y envía las respuestas a Eva (UAB) o a Huma (CU) a los correos electrónicos que encontrarás a continuación. Si obtienes 8/10 o más, recibirás un certificado de educación informal CSI-COP (puedes intentar responder a las preguntas tantas veces como desees):

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

Preguntas

a. «La privacidad se ha convertido en un problema desde la aparición de Facebook». ¿Esta afirmación es verdadera o falsa?
b. «El modo "incógnito" del navegador Google Chrome te permite hacer búsquedas con total privacidad». ¿Esta afirmación es verdadera o falsa?
c. «Al usar una red wifi pública se pueden compartir tus datos de localización». ¿Esta afirmación es verdadera o falsa?
d. «Los datos personales sensibles se relacionan con tu nombre». ¿Esta afirmación es verdadera o falsa?
e. «La toma de huellas digitales es un tipo de rastreo de los sitios web que utiliza los atributos de tu dispositivo o navegador para construir tu perfil». ¿Esta afirmación es verdadera o falsa?
f. ¿Cuál de las siguientes categorías refieren a datos de comportamiento? Marca todas las que lo sean en la lista siguiente:
   i. Tus interacciones en un sitio web
   ii. Tus datos de navegación web
   iii. El historial de compras en línea
   iv. Cuando utilizas un mapa *online*
   v. Cuando usas una aplicación (por ejemplo, para controlar tu salud)
g. «Los derechos humanos se consideraban algo esencial para nuestra dignidad y para proteger nuestros derechos básicos y nuestras libertades». ¿Esta afirmación es verdadera o falsa?
h. «De acuerdo con la Declaración Universal de Derechos Humanos (DUDH), tus derechos incluyen "protección contra interferencias arbitrarias en la privacidad, la familia, el hogar o la correspondencia de una persona"». ¿Esta afirmación es verdadera o falsa?
i. «Según la convención europea de derechos humanos (CEDH): en la era moderna no tenemos derecho a esperar una vida privada y familiar en nuestro hogar y nuestra correspondencia». ¿Esta afirmación es verdadera o falsa?
j. De conformidad con el Reglamento General de Protección de Datos (RGPD), tenemos derecho a... (selecciona todas las opciones que correspondan):
   i. Ser informados
   ii. La transparencia
   iii. La protección de datos
   iv. No ser filmados por las cámaras de otras personas

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Conviértete en un científico ciudadano

Convertirse en un científico ciudadano de CSI-COP	Tras completar los cinco pasos del curso de educación informal de CSI-COP y recibir tu certificado, ¿te gustaría unirte al equipo CSI-COP e investigar el alcance del rastreo en línea? Puedes unirte al equipo CSI-COP y participar como científico ciudadano voluntario en el proyecto CSI-COP. Si lo solicitas, se te proporcionará información completa. Dicha información incluye: Hoja informativa para los participantes sobre el rol de los científicos ciudadanos. Hoja de consentimiento informado que cumple con el Reglamento General de Protección de Datos (RGPD). Información sobre cómo empezar a investigar sitios web y aplicaciones en busca de *cookies*. Puedes obtener más información en el apartado 'About' del sitio web de CSI-COP (en el siguiente enlace: https://csi-cop.eu/about/). Si todavía no los has hecho, puedes apuntarte en el sitio web de CSI-COP creando tu cuenta (en el siguiente enlace: https://csi-cop.eu/citizenscientistlogin/). El foro del sitio web de CSI-COP, en el que podrás discutir con otros científicos ciudadanos del proyecto, lo encontrarás en el siguiente enlace: https://csi-cop.eu/forum/ Seguidamente, encontrarás una encuesta con algunas preguntas sobre ti. Esto es para ayudar a CSI-COP a saber quiénes son los científicos ciudadanos. No recopilaremos ningún dato que te identifique como persona. ¡Muchas gracias por tu tiempo!

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Rango de edad: marca con un círculo el rango correspondiente	18-39 40-65 66+ Prefiero no decirlo
Género (selecciona uno)	—Mujer —Hombre —Intersexual —Paragua trans —Otro —Prefiero no decirlo
Ubicación (selecciona una)	—Urbano (ciudades) —Rural (pueblos de menos de 2000 habitantes) —Prefiero no decirlo
Idiomas 1. ¿Cuál es tu lengua materna o dominante? 2. ¿Hablas más de un idioma de manera fluida? ¿Cuál/es? Puedes preferir no decirlo	**1.** **2.** Prefiero no decirlo
Accesibilidad: ¿Consideras que tienes algún problema de accesibilidad? (Por ejemplo, ¿usas un *software* de conversión de texto a voz debido a una discapacidad visual?)	Sí No Prefiero no decirlo
Empleo:	Estudiante (selecciona el nivel de estudios) —Grado o licenciatura —Posgrado —Doctorado No estudiante (elige la categoría que mejor describa tu situación laboral) —Empleado (36,5 h/semana o más) —Empleado (1-36h/semana) —Sin empleo (buscando trabajo) —Sin empleo (sin buscar trabajo) —Refugiado que busca asilo —Jubilado —Con problemas de accesibilidad (sin posibilidad de trabajar) —Prefiero no decirlo

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

Acceso a Internet:	—Con acceso a conexión Internet propia (banda ancha doméstica o labora/ móvil) —Acceso a internet mediante red pública —Prefiero no decirlo
Uso de Internet. ¿Con qué frecuencia utilizas Internet? (selecciona una opción)	—A diario —2-3 veces por semana —Una vez por semana —Menos de una vez por semana —Nunca —Prefiero no decirlo
Finalidad del uso de Internet:	—Uso Internet como parte del trabajo diario —Uso Internet para el ocio (no como parte del trabajo) —Uso Internet para el ocio y el trabajo —Uso Internet de manera limitada (por ejemplo, al usar un ordenador de una biblioteca pública) —Prefiero no decirlo
Uso de aplicaciones en ordenadores de sobremesa y portátiles	—Uso aplicaciones regularmente, por ejemplo para autenticar el acceso a las herramientas de trabajo (como Zoom, MS Teams, etc.). * En este caso, indica algunas de las aplicaciones que usas y la finalidad con qué lo haces: —Herramientas de trabajo (p.e. Microsoft Office, etc.) —Para jugar (p.e. STEAM). —Aplicaciones educativas —Estilo de vida (deportes, salud…) —Noticias —Entretenimiento (como aplicaciones en *streaming* tipo Netflix) —Otras —Prefiero no decirlo —Raramente utilizo aplicaciones en ordenadores de sobremesa o portátiles —No uso aplicaciones en ordenadores de sobremesa o portátiles —Prefiero no decirlo
Uso de aplicaciones en dispositivos móviles	—Uso aplicaciones con frecuencia, por ejemplo aplicaciones de transporte para saber cuándo llega el próximo tren o autobús. * En este caso, indica algunas de las aplicaciones que usas y la finalidad con qué lo haces: —Jugar —Aplicaciones educativas —Estilo de vida (deporte, salud…) —Noticias —Entretenimiento (como aplicaciones en *streaming* tipo Amazon Prime).

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169

	—Otras —Prefiero no decirlo —Raramente utilizo aplicaciones en el teléfono móvil o la tablet —No utilizo aplicaciones —Prefiero no decirlo
¿Cómo conociste el proyecto CSI-COP?	—A través del sitio web de CSI-COP —A través de una universidad —A través de una asociación a la que pertenezco (p.e. Women in tech) —A través de una plataforma de ciencia ciudadana como: SciStarter Zooniverse EU-Citizen.Science Otra plataforma de ciencia ciudadana —Navegando por Internet —Gracias a un trabajo voluntario previo —A través de una red social (indicar cuál) —Por el boca a boca —Otros
¿Has completado el curso/taller de educación informal en línea y gratuito CSI-COP?	—Sí —No, pero pretendo hacerlo —No, prefiero esperar a futuros talleres presenciales si se llevan a cabo cerca de donde vivo
Si has completado el curso/taller, ¿tienes intención de unirte al equipo CSI-COP como científico ciudadano voluntario?	—Sí —Quizás —Necesito más información —No
Envía tu respuesta a las preguntas del apartado «Evalúa tu aprendizaje», el resultado de esta encuesta, la valoración del curso y cualquier posible consulta al equipo CSI-COP de la Universidad de Coventry.	Te agradecemos que envíes el documento cumplimentado al miembro del equipo CSI-COP de la Universitat Autònoma de Barcelona: Prof. Dra. Eva Jove (eva.jove@uab.cat)
Gracias por completar el curso de educación informal de CSI-COP y la encuesta. **Este documento está disponible en otros idiomas.** **Para más información, consulta el sitio web de CSI-COP en el siguiente enlace: https://csi-cop.eu/**	

Esta comunicación forma parte de un proyecto que ha recibido financiación del
programa de investigación e innovación European Union's Horizon 2020 en virtud del acuerdo de subvención Nº873169