

DIXITALIZACIÓN

Curso: 4º ESO

CIUDADANÍA DIGITAL CRÍTICA

Ciudadanía digital crítica

BRÚJULA DIGITAL

El impacto de la tecnología digital en las sociedades modernas está provocando transformaciones en la forma en que las personas aprenden, trabajan, interaccionan, comercializan o se relacionan con sus administraciones, entre otros aspectos.

En este contexto, la Unión Europea tiene una hoja de ruta para la próxima década, denominada *Brújula digital*, en base a cuatro puntos cardinales:

- Una ciudadanía capacitada y empoderada digitalmente.
- Infraestructuras digitales seguras, sostenibles y eficaces.
- Transformación digital de las empresas.
- Digitalización de los servicios públicos.

Con ello, se aspira a un futuro digital sostenible más próspero y centrado en las personas. Sin embargo, todavía hay muchos desafíos asociados que deben abordarse, como la brecha digital, la desinformación, la protección de datos o la ética de las máquinas.

Las políticas clave para garantizar que se cumplan esos objetivos incluyen tecnologías emergentes como la inteligencia artificial, computación en la nube, impresión 3D, *big data*, IoT, 5G, *block-chain* o *machine learning*.

COMPROMISO ODS

Alrededor del mundo hay millones de personas que se encuentran en situaciones de vulnerabilidad, por lo que necesitan tu ayuda y solidaridad.

- 1  **Averigua** cómo podrías formar parte del cibervoluntariado de alguna de las causas sociales que más te preocupen en este momento.
- 2  **Asamblea de ideas.** El ODS 16 promueve sociedades justas, pacíficas e inclusivas, a través de instituciones públicas sólidas y transparentes. ¿Crees que la digitalización proporciona herramientas que pueden facilitar la transparencia o rendición de cuentas a la ciudadanía?

La sociedad del conocimiento se caracteriza por la capacidad de sus ciudadanos, empresas y Administraciones públicas de obtener, procesar y compartir información, haciendo uso de las tecnologías de la información y la comunicación, con el fin de generar conocimiento.

1.1 Ciudadanos digitales

En la **sociedad actual**, coexisten **dos generaciones** de personas que, aunque comparten una misma tecnología informática, la emplean de forma distinta. Los jóvenes de hoy en día pueden considerarse **nativos digitales**, ya que han nacido y crecido rodeados de ordenadores, pantallas e internet, y están expuestos a ellos desde una edad temprana, por lo que son muy hábiles en su uso. Y, por otra parte, están los **inmigrantes digitales**, que son las personas nacidas antes de la década de los noventa que han sido espectadoras de estos avances tecnológicos y han aprendido a usarlos según han ido surgiendo.

Esta sociedad proporciona muchas oportunidades para interactuar, aprender, trabajar, etc., pero, a medida que aumenta el uso de la tecnología, también ha crecido la **preocupación** por la privacidad de los datos y la ciberseguridad, lo que ha llevado a los Gobiernos a aprobar leyes para proteger a la ciudadanía digital.

1.2 Competencia digital

El continuo desarrollo de las TIC conlleva la aparición de cambios importantes en la sociedad, a los que tiene que adaptarse la ciudadanía.

La **competencia digital** es la capacidad de utilizar las tecnologías de la información y de la comunicación en las tareas de la vida cotidiana.

Uno de los principales retos que plantea la sociedad digital es garantizar que sea inclusiva, sin dejar a nadie atrás. Para ello, es necesario garantizar el acceso a las tecnologías y eliminar las brechas digitales.

La **brecha digital** hace referencia a la situación de desigualdad que se produce entre las personas que pueden tener acceso o conocimiento de las nuevas tecnologías y las que no.

Esta fractura no aparece únicamente como consecuencia de las desigualdades entre los países ricos y pobres, sino entre quienes tienen la capacidad para utilizar la tecnología de forma eficaz y los que no disponen de los conocimientos suficientes. Asimismo, comparando las oportunidades de hombres y mujeres, se desprende la existencia de una **brecha de género digital** que se extiende por todo el mundo.

Algunas de las acciones que es necesario realizar para reducir la brecha digital son **crear infraestructuras** de servicios de internet, aumentar los programas de **alfabetización digital** para mejorar la formación e incrementar la **inversión en digitalización** en todos los ámbitos.

Sabías que...?

En Ghana, el Gobierno utiliza drones, en su programa del sistema público sanitario, con el objetivo de realizar envíos de medicamentos, sangre y vacunas a todo el país.



1.3 Transformación digital desde una perspectiva social

La transformación digital es el fenómeno que incorpora el uso de las nuevas tecnologías de la información y la comunicación en todos sus aspectos. Para garantizar su éxito, sin provocar nuevas brechas digitales, es necesario educar en una cultura digital saludable, responsable y con pensamiento crítico.

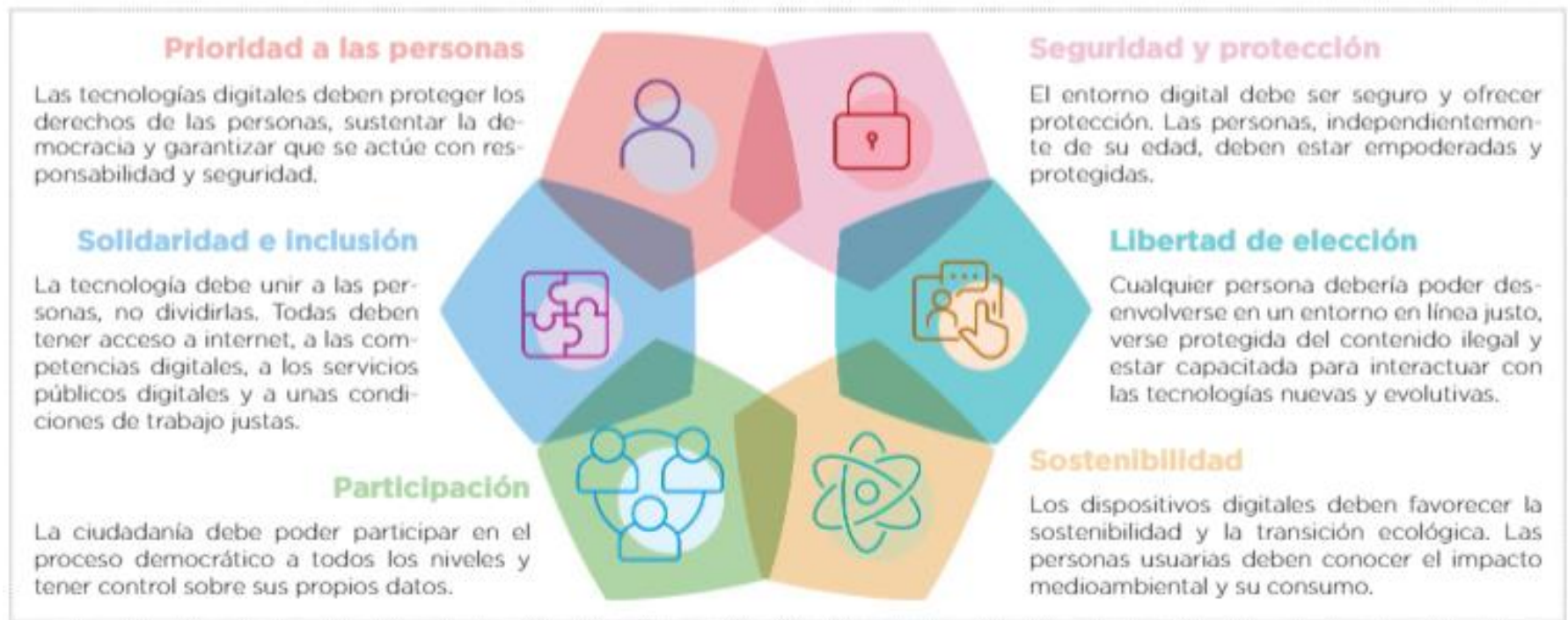
Los países de la Unión Europea se han comprometido a adoptar iniciativas clave para fomentar la conectividad, las tecnologías digitales limpias y las empresas emergentes, con el objetivo de contribuir a la digitalización sostenible. El objetivo es evolucionar hacia una sociedad digital más inclusiva, sostenible y justa.

1.4 Derechos y principios de la ciudadanía digital

Los derechos digitales, muy ligados a la **libertad de expresión** y a la **privacidad**, son aquellos que permiten a las personas acceder, usar, crear y publicar medios digitales, así como acceder y utilizar ordenadores, otros dispositivos electrónicos y redes de comunicaciones.

Los derechos y principios digitales proporcionan un marco de referencia común en la Unión Europea sobre cómo han de aplicarse los valores de la transformación digital y los derechos fundamentales de la ciudadanía en el mundo digital.

Sociedad digital



COMPRENDE, PIENSA, INVESTIGA...

- 1 Describe los objetivos previstos por el Programa Nacional de Algoritmos Verdes.
- 2 La Carta de Derechos Digitales recoge el derecho a la desconexión digital en el ámbito laboral. ¿En qué consiste?
- 3 Averigua si el 5G aumentará la huella de contaminación o, por el contrario, su conectividad será la piedra angular de la sostenibilidad futura.
- 4 Obtén información sobre el Aula del Futuro, su metodología, actividades y equipamiento.

Interactividad en la red

Internet está influyendo en la forma en que las personas se comunican y se relacionan. La cultura participativa que se ofrece ha dado lugar a nuevos escenarios de relaciones digitales en los que evitar conflictos es uno de los retos para lograr una ciberconvivencia igualitaria, segura y saludable, siendo conscientes de **la relevancia que tiene usar y disfrutar de la red con todas sus ventajas**. La libertad de expresión termina donde comienza el derecho de los demás, por lo que es importante adoptar reglas básicas de comportamiento, al igual que se siguen en el mundo real.

2.1 Comunicación en línea

La comunicación en línea hace referencia al intercambio de información y mensajes entre personas o entidades a través de las plataformas o medios que ofrece internet. Se desarrolla a través de redes sociales, mensajería, correo electrónico, foros, chats o cualquier otro medio donde se lleva a cabo el intercambio de información. Una de sus grandes ventajas es que se puede realizar tanto de forma síncrona como asíncrona, por lo que cada interlocutor tiene la posibilidad de participar en cualquier momento y desde cualquier lugar, sin que tenga que ser necesariamente en tiempo real.

Internet no solo ha modificado la forma de comunicarse, también ha propiciado espacios de interacción entre las personas para dialogar, discutir, confrontar y compartir información, potenciando la participación ciudadana y generando una inteligencia colectiva que deriva en una sociedad más activa y empoderada.

2.2 Ciberconvivencia igualitaria, segura y saludable

La red se ha convertido en un espacio de interacción y ciberconvivencia donde las personas desarrollan relaciones entre iguales a través de entornos virtuales, por lo que es preciso ser conscientes de la relevancia que tiene usar y disfrutar de ella, de forma segura y saludable, conociendo los riesgos que puede entrañar.

La ciberconvivencia está basada en unas **reglas y normas de comportamiento**, fundamentadas en el **respeto**, la **educación** y la **tolerancia** hacia los demás, tal y como sucede en la vida real. Cuando no se conocen o aplican, la convivencia digital puede dejar de ser asertiva o, peor aún, verse empañada por conflictos y convertirse en tóxica.

Se suele asumir que todas las personas saben ciberconvivir en los entornos virtuales, pero no tiene por qué ser así, por lo que es importante el conocimiento y uso adecuado de las netiquetas.

2.3 Netiqueta

En 1955 se publicó un documento en inglés, llamado *Request for comments* (RFC 1855), con el propósito de establecer unas reglas de uso de internet. Con el trascurso del tiempo diferentes organizaciones han desarrollado su propia netiqueta.

La netiqueta o etiqueta digital es el conjunto de **normas básicas que fomentan la buena comunicación y comportamiento** en la red, a partir del respeto, la tolerancia y la cortesía.

Este término procede de la conjunción de la palabra inglesa *net*, traducido como red, y de la francesa *étiquette*, referido a etiqueta.

Al igual que existen normas para entornos presenciales, las hay para los entornos virtuales y, aunque la mayoría de las veces no aparecen escritas explícitamente, han pasado a formar parte de la cultura intrínseca del uso de internet, reconocidas y aceptadas por la mayoría de las personas, por lo que deben ser respetadas.

La aplicación de las reglas de netiqueta fortalece la comunicación y propicia una interacción agradable entre las personas, contribuyendo al uso adecuado de las herramientas virtuales y evitando conflictos.

Reglas de netiqueta

VIDEOCONFERENCIA

- Vestirse de manera apropiada a la ocasión.
- Identificar un espacio que tenga el fondo apropiado, con buena iluminación y sin ruidos.
- Conectarse a la sesión con antelación a su comienzo.
- Saludar al conectarse.
- Mantener contacto visual con las demás personas.
- No comer con la cámara o micrófono encendido.
- Mantener el micrófono apagado cuando no se habla.
- Solicitar turno con el icono específico para ello.
- Respetar la privacidad no capturando la pantalla.

FORO

- Responder a aportes del foro con argumentos válidos y justificados, citando las fuentes en caso necesario.
- Reconocer y respetar la diversidad de personas, con sus creencias y opiniones.
- Intervenir con un tono adecuado que no pueda ser malinterpretado, incluso cuando se está en desacuerdo.
- Focalizar las intervenciones en el tema y propósito del foro, usando la temática de cada hilo.
- Revisar la ortografía y la gramática antes de publicar.
- Evitar textos completamente en mayúscula.
- Utilizar con moderación los emoticonos.

CORREO ELECTRÓNICO

- Utilizar el correo institucional, si se dispone de él.
- Omitir los mensajes en cadena y no reenviarlos.
- Utilizar los campos Para, CC, CCO y Asunto correctamente.
- Redactar un mensaje claro y conciso, con saludo, despedida y tono adecuado.
- Evitar usar demasiados colores en el texto y emoticonos.
- Revisar la ortografía y la gramática antes de enviar.
- Evitar textos completamente en mayúscula.
- Responder a los mensajes dentro del plazo esperado.
- Informar cuando se adjunten archivos.

MENSAJERÍA INSTANTÁNEA Y CHAT

- Saludar al entrar en una sala y al comenzar a chatear.
- Escribir mensajes breves y significativos.
- Reenviar mensajes únicamente cuando se tenga la seguridad de la autenticidad de su contenido.
- Escuchar la opinión del resto y, en caso de manifestar el desacuerdo hacerlo respetando a los demás.
- Solicitar el consentimiento de cualquier persona antes de añadirla a un grupo de mensajería.
- Revisar la ortografía y la gramática antes de enviar, intentando no utilizar abreviaturas incorrectas.
- Despedirse al retirarse de la conversación.



Sitio web de la campaña *10 pasos para la tolerancia en internet*.

¿Sabías que...?

Cuando se recibe una comunicación en tono insultante, maleducado o que falta el respeto puede afectar al bienestar y a la productividad, por lo que es normal que haga sentir incomodidad o molestia. En este caso, es importante mantener la calma intentando dejar transcurrir un tiempo para reflexionar antes de responder y evitar hacerlo de forma inapropiada o incorrecta.

COMPRENDE, PIENSA, INVESTIGA...

5  Lee la fábula del tigre y el burro. ¿Cómo aplicarías la moraleja que extraes de ella a la comunicación en internet?

6  **Sumamos.** Colabora en la creación de un listado de pautas que ayuden a interactuar en internet de forma saludable.

3.1 Datos personales

En la sociedad de la información y del conocimiento, se registran millones de datos personales en actividades que se realizan a diario, como clasificarse en una carrera, participar en un concurso, publicar contenidos en redes sociales o, simplemente, navegar por internet.

Un **dato** de carácter **personal** es cualquier **información** que permita **identificar** a una persona.

El nombre, los apellidos, la fecha de nacimiento, la dirección postal, el correo electrónico, el número de teléfono, el DNI, las fotografías, los vídeos y muchos otros datos utilizados a diario constituyen información valiosa asociada a una persona y que, por tanto, permiten identificarla.

Los datos personales pueden ser recogidos en **ficheros**, que dependen de las Administraciones públicas, tiendas *online*, compañías de servicios, redes sociales, los centros sanitarios, etc., que los utilizan para **desarrollar** su **actividad**. Las personas deben ser conscientes de que todos estos datos revelan información de la personalidad, los hábitos de consumo, historiales clínicos, etc., que es importante **proteger**.

Los dispositivos almacenan mucha información privada

Uno de los principales motivos para proteger los dispositivos es salvaguardar la información personal y la de aquellos con quienes se mantienen comunicaciones: contactos, fotografías, vídeos, mensajes, audios, etc. Al respecto, algunas recomendaciones son:

- Activar el bloqueo de pantalla.
- Contar con herramientas de seguridad para localizar, bloquear o borrar el dispositivo.
- Descargar aplicaciones únicamente desde tiendas o sitios web oficiales, y revisar los permisos que solicitan.
- Realizar copias de seguridad en la nube.
- Tener instalado un antivirus.
- Evitar las conexiones a redes wifi públicas o abiertas.

3.2 Información y consentimiento

El **derecho fundamental a la protección de datos** garantiza a cada persona la **disposición de toda la información referida a ella y a decidir sobre su uso.**

La protección de las personas, en relación con el tratamiento de los datos personales, es un derecho fundamental, recogido en el artículo 18.4 de la Constitución española, en el Reglamento general sobre protección de datos (RGPD) de la Unión Europea, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD). La **Agencia Española de Protección de Datos (AEPD)** vela por su cumplimiento, siendo el organismo a través del que se puede denunciar su uso inadecuado.

Los datos personales solamente pueden recogerse y emplearse si la persona interesada acepta el uso que se hará de ellos. Normalmente, este consentimiento se otorga al aceptar la información contenida en los **términos del servicio**, las **condiciones de uso**, las **políticas de privacidad**, etc., cada vez que se descarga una aplicación o se realiza un registro en cualquier sitio de internet. Aunque, por lo general, se aceptan sin vacilaciones, **es fundamental leerlos y comprenderlos**, para conocer en qué medida una persona puede quedar expuesta.

Protección de datos personales

3.3 Tratamiento de los datos

Las reglas aplicables a los datos personales establecen **obligaciones**, para asegurar que la persona o entidad responsable de su tratamiento actúe adecuadamente. Para ello, deben garantizarse los siguientes **principios**:

- **Principio de calidad.** Los datos de carácter personal solo se pueden recoger para su tratamiento cuando sean **adecuados, pertinentes y estén relacionados** con la finalidad para la que han sido obtenidos. Por ejemplo, al instalar una aplicación de *fitness*, sería adecuado autorizar su uso sobre los sensores corporales y la ubicación de la persona que la utiliza, pero no sobre su cámara, contactos o llamadas telefónicas.
- **Principio de seguridad.** Los responsables de su tratamiento deben adoptar las **medidas técnicas y organizativas** necesarias para garantizar su seguridad y evitar la alteración o pérdida, así como el acceso no autorizado. Por ejemplo, la documentación que contenga datos personales, como exámenes o informes médicos, tiene que ser destruida.
- **Principio de secreto.** Es esencial para garantizar el derecho fundamental a la protección de datos. Por ello, quienes intervienen en cualquier fase del tratamiento están obligados a su **custodia**. Así, por ejemplo, las contraseñas se mantienen en secreto y, en caso de pérdida, solo podrán ser restauradas si la persona afectada acredita su identidad.

3.4 Derechos ARCO

Los **derechos ARCO** (acceso, rectificación, cancelación y oposición), regulados por la LOPDGDD, permiten que cualquier persona pueda **ejercer el control** sobre su **información personal**. El RGPD sustituyó el derecho de cancelación por el de supresión, y añadió el de portabilidad de los datos. A continuación, se describen brevemente:

- **Acceso.** Posibilita que una persona pueda solicitar **información** del tratamiento que se está realizando de sus datos, la finalidad, el origen, las comunicaciones realizadas, etc.
- **Rectificación.** Permite, a la persona afectada, pedir la **modificación** de aquellos que sean inexactos o estén incompletos.
- **Supresión.** Garantiza la **cancelación** de los datos personales de la persona interesada sin dilación, siempre que no sean necesarios para su finalidad o cuando se ejerza el derecho a oposición sobre los mismos.
- **Oposición.** Da la opción, a la persona interesada, a oponerse al **tratamiento** de sus datos personales, con fines publicitarios o cualquier otro, para los que no se haya dado su consentimiento.
- **Portabilidad.** Permite **obtener los datos** proporcionados a la entidad responsable de su tratamiento en formato estructurado, de uso común y de lectura mecánica. También implica que estos puedan transmitirse directamente a otra entidad, sin intervención de la persona interesada. Se utiliza, por ejemplo, al cambiar de ISP.

Desde el inicio de los tiempos, la desinformación, las noticias falsas y las mentiras han circulado por la sociedad, pero con las nuevas tecnologías su expansión se ha generalizado, agravada por la saturación de información. Para contrarrestar estas amenazas, las autoridades públicas de numerosos países han puesto en marcha diversas iniciativas legales, tecnológicas y educativas.

4.1 Alfabetización mediática y libertad de expresión

Los medios se han convertido en un espacio de comunicación de libre expresión donde, cada día, millones de personas de todo el mundo crean y comparten millones de mensajes, imágenes y vídeos.

El **derecho** a la **libertad de expresión** y a la **libertad de información** está reconocido en el artículo 19 de la Declaración Universal de los Derechos Humanos. Pero dicha libertad debe ir acompañada de alfabetización mediática para fomentar el empoderamiento de una ciudadanía participativa.

La alfabetización mediática e informacional hace referencia al proceso por el cual se aprenden **habilidades y capacidades** para **desenvolverse** en los **medios actuales** analizando de **forma crítica** la información y **cuestionándose la veracidad** de las fuentes.

4.2 Hábitos, conductas y estrategias comunicativas para el debate crítico en la red

El epicentro de las interacciones en el ecosistema digital son las personas, por lo que su capacidad crítica y analítica frente a la información es fundamental. Para ello, es necesario contar con las habilidades necesarias para el correcto filtrado de los contenidos que se consumen, crean o comparten.

Las estrategias comunicativas son las **tácticas** que utilizan quienes publican en la red **con la finalidad de crear mensajes efectivos** a través de diferentes **canales digitales**. Es importante conocer estas estrategias tanto a la hora de difundir información como al recibirla, para poderla interpretar de forma crítica.

Al analizar la información es importante distinguir entre un **hecho** (algo que se puede demostrar que sucede o ha sucedido) y una **opinión** (punto de vista sobre algo), ya que a veces se confunden estos términos y determinadas opiniones se cree que son hechos. Para ello, se debe seguir la **teoría de las cinco w**, que cobija las preguntas fundamentales que toda información debería responder con rigor: **who, what, when, where and why**.

¿Sabías que...?

Los *youtubers*, *instagrammers* y otros *influencers* que cuentan con gran credibilidad por parte de quienes los siguen están promocionados por marcas que les pagan o regalan productos a cambio de publicidad. Por esta razón, es importante analizar de forma crítica sus publicaciones, ya que su comportamiento o pensamiento puede ser poco objetivo o, incluso, cuestionable.

4.3 Infoxicación

El gran número de personas que publican contenidos en internet, impulsados por la proliferación de medios digitales y redes sociales, ha dado lugar a un **exceso o sobrecarga de información** denominada *infoxicación*.

Su principal **inconveniente** es que el exceso de información exige dedicar **mucho tiempo y esfuerzo a depurarla** para quedarse con la adecuada. A su vez, la rapidez y la facilidad con la que cualquiera puede publicar contenidos que se viralizan velozmente ha contribuido a la propagación de información errónea y de noticias falsas.

Para evitar la infoxicación, se deben utilizar **fuentes de información fiables**, así como **curar** o filtrar los **contenidos**.

4.4 *Fake news* y posverdad

Una ***fake news*** es una **noticia con apariencia real** pero que es **falsa**, inexacta o engañosa creada y difundida para obtener beneficios, influir en el pensamiento de la gente o hacer daño.

Estas noticias son difíciles de identificar porque suelen ocurrir en contexto de posverdad propios de conflictos de intereses, como elecciones, pandemias, guerras, etc., donde existe interés en influir en la opinión pública apelando a sus emociones frente a los hechos reales.

El término **posverdad** se define en la RAE como la **distorsión deliberada de una realidad**, que **manipula creencias y emociones** con el fin de **influir** en la opinión pública y en actitudes sociales.

¿Cuáles son las noticias falsas más repetidas de la historia?

Las temáticas más virales suelen ser la política, ciencia, salud, inmigración, cuestiones de género y aborto. Pero, en la historia, las más repetidas son las que se difunden en tiempos de guerra, incluso algunas, como la campaña de Hearst, provocó la guerra hispano-estadounidense que culminó con la independencia de Cuba. Suele decirse que la primera víctima de una guerra es la verdad.

4.5 Herramientas para detectar noticias falsas y bulos

Las herramientas para detectar noticias falsas y bulos utilizan procesos inherentes a la práctica periodística: **la verificación**.

Existen herramientas que permiten la búsqueda inversa de imágenes y vídeos, analizando sus metadatos (fecha, lugar, fuente) e incluso algunas claves para saber si se han modificado. Además, existen reglas básicas como leer la noticia completa, buscar el titular en Google, comprobar la fecha, examinar la URL, verificar su autoría, contrastar con fuentes oficiales y fijarse en la ortografía.

Algunas redes sociales aplican filtros contra las noticias falsas. También existen **plataformas** dedicadas a la **verificación informativa**, como Maldita.es, Newtral, SOMA o Verificat; incluso algunos medios tradicionales incluyen secciones para ello, como Verifica RTVE o EFE Verifica.

COMPRENDE, PIENSA, INVESTIGA...

- 9  **El espejo.** Averigua de quién es la cita «Una mentira da la vuelta al mundo antes de que la verdad llegue a ponerse las botas». Compara el resultado obtenido con el de tus compañeros y compañeras.
- 10 ¿Cuáles son las 8 P que ayudan a explicar el fenómeno de la desinformación?
- 11  **Grupo nominal.** Las noticias falsas se retuitean un 70% más que las reales, ¿a qué crees que se debe?

Gestiones administrativas en línea

5.1 Servicios públicos en línea

La mayoría de las Administraciones públicas incluyen una sede electrónica en su portal web desde la que es posible acceder al **catálogo de trámites** que ofrecen. Algunos ejemplos de trámites habituales son:

- Solicitar certificados de empadronamiento, vida laboral, afiliación a la Seguridad Social...
- Realizar la inscripción en estudios y pruebas selectivas.
- Comunicar un cambio de domicilio o de estado civil.
- Pedir ayudas, becas y subvenciones.
- Acceder a la búsqueda de empleo y a la oferta de cursos de formación profesional.
- Presentar comunicados por registro electrónico.
- Recibir notificaciones electrónicas de becas, ayudas, infracciones...

Para evitar tener que localizar el sitio web desde el que hacer cada trámite, se puede acceder al **Punto de acceso general** (administracion.gob.es) que facilita su realización desde un portal único, que permite suscribirse y tener acceso a una carpeta ciudadana.

En general, los servicios públicos en línea permiten comunicarse e **interactuar** con cualquier **Administración pública**, utilizando un registro electrónico para presentar las solicitudes. También es posible solicitar cita previa para aquellos trámites que requieran de presencialidad, como pueda ser la expedición del DNI o de un certificado electrónico.

Gestiones administrativas en línea

5.2 Sede electrónica

El derecho de la ciudadanía a relacionarse y comunicarse por medios electrónicos con las Administraciones públicas, como establece la legislación, comporta la necesidad de definir una sede electrónica, para acceder a la información y a sus servicios con las mismas garantías que los efectuados de forma presencial.

La sede electrónica es el **sitio en internet** desde el que se pueden **realizar** los **trámites administrativos** que **requieren identificación** por parte de la ciudadanía o de la Administración.

El acceso se puede realizar en todo momento y desde cualquier lugar, considerando que un trámite realizado en un día inhábil se entenderá efectuado el primer día hábil siguiente. Toda la información viaja cifrada por la red de forma segura.

Para realizar cualquier trámite, se debe utilizar alguno de los sistemas habituales de **autenticación** en las Administraciones públicas, como el DNle, el certificado digital, Clave PIN o Clave permanente.

5.3 Registro electrónico

Un registro electrónico o digital es un punto para la **tramitación** de documentos con **destino** a la **Administración** General del Estado (Ministerios) y sus **organismos públicos**.

Las personas interesadas pueden utilizarlo para presentar solicitudes, comunicaciones, reclamaciones, etc., todos los días del año, durante las 24 horas del día y desde cualquier lugar con acceso a internet.

Cada organismo dispone de su propio registro electrónico, aunque también es posible utilizar el registro electrónico común (REC) o la Oficina de Registro Virtual (ORVE).

Para realizar el registro, se debe acreditar la identidad utilizando el DNI electrónico o un certificado digital reconocido que esté en vigor. A continuación, se rellena una **instancia** con los siguientes datos:

- **Datos personales:** DNI, nombre, apellidos, dirección, teléfono...
- **Organismo destinatario:** Administración estatal, autonómica, local, universidad u otras instituciones.
- **Asunto:** breve descripción de la solicitud.
- **Expone:** explicación sistemática y argumentada de las causas que motivan la solicitud.
- **Solicita:** petición que se realiza al organismo al que va dirigida.
- **Documentos adjuntos:** se pueden aportar archivos en diferentes

Gestiones administrativas en línea

Una vez registrada la solicitud se emite un recibo firmado electrónicamente que contiene el número de registro, fecha y hora de la presentación, así como la copia del escrito y el nombre de los documentos adjuntados. Cuando se inicie su tramitación se recibirá una notificación al medio elegido (SMS o correo electrónico).

Gestiones administrativas en línea

5.4 Carpeta ciudadana

La carpeta ciudadana facilita la relación de la ciudadanía con las Administraciones públicas. Se trata de un **espacio privado en línea**, con el que cuentan muchos organismos, desde el que se puede revisar los datos personales, consultar el **estado de expedientes**, acceder a **notificaciones**, gestionar los **registros** presentados, formular **quejas** o **sugerencias**, entre otros aspectos.

La mayoría de los ayuntamientos cuentan con una sede electrónica a la que se puede acceder desde su página web y donde los habitantes cuentan con una carpeta ciudadana para obtener certificados de empadronamiento, pagar tributos, consultar la agenda cultural, etc.

Comercio electrónico

El comercio electrónico consiste en la **compra y venta de productos a través de internet** utilizando un medio de **pago electrónico**. Este término abarca otras actividades como la banca por internet, subastas en línea, pago de impuestos, etc.

6.1 Estrategias para la detección de fraudes

Las compras en línea pueden entrañar riesgos, por lo que es fundamental utilizar estrategias para detectar o evitar actividades fraudulentas, tales como las siguientes:

- **Identificar tiendas en línea de confianza.** Debe ser una web con certificado de seguridad e incluir sus datos fiscales. Si no es una tienda conocida, se recomienda investigar su reputación en la web.
- **Evitar ser víctima de *phishing*.** No responder a mensajes, enlaces o llamadas que solicitan datos personales o bancarios, ya que su objetivo suele ser usarlos de forma fraudulenta para estafar.
- **No contribuir a delitos contra la propiedad intelectual.** Desconfiar de productos que se venden muy por debajo de su precio habitual, ya que es un indicio de que podrían ser falsificados o robados.
- **No instalar aplicaciones que podrían ser fraudulentas.** Descargar únicamente de sitios oficiales y revisar los permisos que requieren.
- **Usar una forma de pago que garantice la seguridad de la compra.** Especialmente al comprar artículos de segunda mano. Al vender se debe desconfiar de compradores que ofrecen más dinero del que se pide o que se use algún tipo de servicio como Western Union.
- **Utilizar medios de pago a través de plataformas seguras.** Se evita, de este modo, facilitar datos sensibles, como el número de la cuenta corriente o de la tarjeta de crédito, a los vendedores.
- **Actuar con sentido común.** Desconfiar de premios, regalos, etc., que se ofrecen por la red, ya que podrían esconder otros peligros.

6.2 Formas de pago para comprar

Para comprar en la red se pueden utilizar diversas formas de pago:

- **Tarjeta de crédito:** el pago se realiza introduciendo sus datos en la web del comercio o en una pasarela de pago bancaria.
- **Transferencia bancaria:** se envía una cantidad de dinero desde la cuenta bancaria de quien compra a la cuenta de quien vende.
- **Pago contrarrembolso:** se paga al recibir el envío. Aunque es un sistema bastante fiable añade un recargo al coste.
- **Envío de dinero en efectivo:** a través de servicios, como Bizum, con los que únicamente se requiere un número de teléfono.
- **Pago a través de intermediarios:** se usa una tercera empresa de confianza para que gestione el pago, por ejemplo, PayPal.
- **Criptomonedas:** se admite en comercios que estén adheridos a la plataforma de la criptomoneda con la que se desea pagar.

6.3 Criptomonedas

La criptomoneda, también llamada moneda virtual o criptodivisa, es **dinero digital** desarrollado en software libre. Eso significa que no hay monedas ni billetes físicos, ya que **se almacena en monederos o carteras en línea.**

No es una moneda oficial por lo que, aunque cada vez está más regulada, no está respaldada por los Gobiernos y se usa de forma descentralizada, es decir, permite las transacciones directas entre personas, sin necesidad de bancos ni intermediarios. Se suelen utilizar para hacer pagos rápidos, evitar cargos por transacciones o para invertir pese a ser **muy volátil**. Por otra parte, su anonimato ha propiciado que su uso de **soporte a actos delictivos**, razón por la que hay que desconfiar siempre que se solicite un pago en criptomonedas.

Desde la aparición del bitcóin, que fue la primera criptomoneda, no han parado de crearse nuevas, todas ellas basadas en el **blockchain**.

6.4 Facturas digitales

Cada vez que un comercio realiza una venta en línea emite una factura que se debe conservar para hacer valer el derecho de **desistimiento** o de **garantía**, en caso de ser necesario.

Una factura digital es un **documento** que se expide en **formato electrónico**, constituyendo el justificante de la entrega de bienes o la prestación de servicios.

Se trata de una alternativa a la factura tradicional en papel con los mismos efectos legales, pero con el beneficio de eliminar costes de impresión o envío postal y mejorar la lucha contra el fraude.

Las facturas digitales suelen ser generadas automáticamente por los sistemas informáticos de facturación y tramitadas de forma automatizada por los sistemas de contabilidad, gracias al intercambio electrónico de datos.

6.5 Intercambio electrónico de datos

El intercambio electrónico de datos o EDI (*electronic data interchange*) es un estándar para **intercambiar información** entre dos organizaciones de forma electrónica, en lugar de utilizar documentos en papel. La información se traslada directamente entre las aplicaciones informáticas de las organizaciones, para su **procesamiento inmediato** y **sin intervención humana**.

Los datos pueden ser documentos comerciales, administrativos o contables, como presupuestos, albaranes, pedidos, facturas, impuestos, etc. En la mayoría de los casos, estas organizaciones son socios comerciales que intercambian bienes y servicios de forma regular.

Ética en el uso de datos y herramientas digitales

Prueba de Turing



Se creó por Alan Turing en 1950 para determinar si una máquina es capaz de pensar o reaccionar como un ser humano y se ha usado, casi de forma estandarizada, en el mundo de la IA. Se basa en un juego de imitación donde una persona plantea preguntas y debe determinar, a través de las respuestas a las preguntas formuladas, si proceden de una persona o una máquina. Esta prueba fue superada con éxito por un ordenador en 2014, que consiguió hacerse pasar por un chico de 13 años, considerándose un hito histórico de la inteligencia artificial.

La inteligencia artificial está presente, en mayor o menor desarrollo, en casi todos los ámbitos de la vida diaria. A través de herramientas digitales y combinada con el uso de datos decide qué noticias se muestran, controla la energía del hogar o propone rutas alternativas de navegación según el tráfico. Pero, ¿dónde deben fijarse sus límites e implicaciones éticas?

7.1 Implicaciones sociales de la IA

La inteligencia artificial (IA) es la combinación de algoritmos planteados con el propósito de crear **máquinas** que presenten las **capacidades humanas**, como el razonamiento, el aprendizaje y la planificación.

Aunque no es una tecnología reciente, cobra **cada día más importancia** en la **vida cotidiana** de las personas y se puede ver en la cantidad de dispositivos que cuentan con ella. Está presente en la detección facial de los teléfonos, en los asistentes de voz virtuales, en coches autónomos, en la previsión meteorológica, etc.

La vertiginosa irrupción de la inteligencia artificial y su **aplicación a la robótica** en la sociedad ha provocado que la Unión Europea desarrolle sus propias leyes de la robótica para regular su uso y evitar, de este modo, posibles problemáticas que puedan surgir en el futuro.

7.2 Aspectos éticos en el manejo del *big data*

La era digital provoca que, para ser competitivos, se deba aprender a gestionar y explotar uno de los **activos** intangibles **más valiosos** que se poseen: **los datos**.

Big data hace referencia al **análisis** de un **gran volumen de datos** cuya **complejidad** y **velocidad de crecimiento** dificultan su captura, gestión y procesamiento utilizando herramientas convencionales, tales como las bases de datos.

Los avances en inteligencia artificial han impulsado el uso del *big data*, debido a su habilidad para procesar ingentes cantidades de datos y proporcionar ventajas en el comercio, la sanidad, la cultura, etc.

Organizaciones de todo tipo recolectan, almacenan, procesan e intercambian grandes volúmenes de información para crear o mejorar sus productos, además de perseguir objetivos como generar mayores beneficios, reducir los costes, consolidar la fidelidad de la clientela y mejorar la toma de decisiones. Por otra parte, ante determinados acontecimientos, como catástrofes o desastres naturales, se pueden usar los datos como un bien social para actuar con rapidez. Pero al mismo tiempo, se enfrentan a importantes retos, tales como gestionar adecuadamente los datos, garantizando la privacidad, la equidad, el respeto, la responsabilidad, la integridad, la calidad, la confiabilidad, la transparencia y la confianza, entre otros.

Ética en el uso de datos y herramientas digitales

Las seis leyes de la robótica de la Unión Europea

- 1 Los robots deberán contar con un interruptor de emergencia para evitar cualquier situación de peligro.
- 2 No podrán hacer daño a los seres humanos. La robótica está expresamente concebida para ayudar y proteger a las personas.
- 3 No podrán generarse relaciones emocionales con los robots.
- 4 Será obligatoria la contratación de un seguro destinado a los de mayor envergadura.
- 5 Sus derechos y obligaciones serán clasificados legalmente.
- 6 Tendrán obligación de pagar impuestos para reducir su impacto en el empleo de las personas.

7.3 Sesgos algorítmicos e ideológicos

Los algoritmos, aunque de manera silenciosa, están **presentes** en la vida de millones de personas, basando su funcionamiento en **software** creado con diferentes fines y cuyo diseño suele heredar sesgos en función de la ideología, la moral o los intereses de quienes lo desarrollan.

Un sesgo algorítmico e ideológico es la **transmisión** de determinados **prejuicios sociales** (de clase, raza, género, ideología, etc.) **a una máquina** o sistema automático.

El análisis y recolección de datos con sesgo ideológico puede provocar efectos adversos en el funcionamiento de dispositivos basados en la inteligencia artificial o *machine learning*. Por ejemplo, los sistemas automatizados con capacidad de aprendizaje intentan reproducir el comportamiento del cerebro humano por lo que, al estar entrenados por personas, también replican aspectos negativos, incluso de forma más agravada por los sesgos que perfilan ese aprendizaje.

Diversos estudios han puesto en relieve que las decisiones que toman estos algoritmos **aumentan la desigualdad**, provocando que sean las máquinas quienes influyan en aspectos tan relevantes como la contratación de personal, concesión de préstamos, popularidad de los candidatos en los procesos electorales, propuestas musicales, etc.

Para evitarlo, el **desafío** que defienden diversas alianzas es incorporar a las máquinas valores, estableciendo **pautas éticas** en el desarrollo de sus algoritmos y, con ello, dando un pequeño salto a la evolución de los sistemas inteligentes para que la inteligencia artificial sea más transparente en su toma de decisiones.

7.4 Soberanía tecnológica y digitalización sostenible

La soberanía tecnológica se basa en el **empoderamiento colectivo** con el fin de tener el conocimiento y la capacidad necesaria **para decidir sobre el uso y consumo de tecnología**. Sus valores se basan en la responsabilidad social, la transparencia, la autogestión y el desarrollo sostenible.

La digitalización y la sostenibilidad debe ser un binomio indivisible, la innovación tecnológica debe satisfacer las necesidades del presente respetando el medioambiente para no comprometer el futuro del planeta. Entre sus finalidades destacan las de contribuir al desarrollo de la economía circular a través de la reutilización de los aparatos al final de su vida útil, **eliminando la obsolescencia programada** y fomentando el acceso universal a la tecnología.

Vocabulario

Machine learning. Disciplina de la inteligencia artificial que dota a las máquinas de la capacidad de aprender a través del reconocimiento de patrones en datos masivos para hacer predicciones. Presente en Netflix, Spotify, Siri, Alexa, etc.

Obsolescencia programada. Vida útil planificada para que un producto se vuelva obsoleto o inservible. No responde a su desgaste habitual sino a una estrategia programada para obligar a comprar dispositivos nuevos. En tecnología suele derivar de la falta de actualizaciones de *software* o del uso de componentes limitados a ciertas horas de uso.

COMPRENDE, PIENSA, INVESTIGA...

16 En 1942, Isaac Asimov enunció en su libro *Círculo vicioso*, las tres leyes fundamentales de la robótica. Enuméralas e indica si consideras que se cumplen.

17  **GCRD.** Enumera dispositivos o aplicaciones que combinen inteligencia artificial con *big data* y puedan tener sesgos algorítmicos.

Activismo en línea

¿Sabías que...?

💡 A través de plataformas como Change.org, Avaaz.org y MoveOn.org, personas y organizaciones de todo el planeta inician campañas, movilizando seguidores para que sus peticiones ayuden a adoptar decisiones para lograr soluciones.



El mundo digital está modificando y determinando la forma en que las personas se comunican y se relacionan. Internet se ha convertido en un espacio propio para que la ciudadanía se empodere y tome conciencia de su capacidad de activismo a través de comunidades y plataformas de iniciativa ciudadana.

8.1 Plataformas de iniciativa ciudadana

Las personas canalizan su participación a través de diferentes medios, destacando las redes sociales y las plataformas de iniciativa ciudadana. Estas plataformas permiten **compartir información** y **organizarse** para diferentes causas, ya sean locales o globales. Y no solo eso, algunas permiten a cualquier persona u organización lanzar sus propias campañas en línea para recabar apoyos.

8.2 Activismo digital

La expansión de las nuevas tecnologías ha supuesto un punto de inflexión para promover la participación, sin tener que recurrir únicamente a las acciones tradicionales de protesta, manifestaciones, pegadas de carteles, etc.

8.2 Activismo digital

La expansión de las nuevas tecnologías ha supuesto un punto de inflexión para promover la participación, sin tener que recurrir únicamente a las acciones tradicionales de protesta, manifestaciones, pegadas de carteles, etc.

El activismo digital es la **participación activa** de la ciudadanía **en internet** para contactar con personas de todo el mundo, intercambiar información o participar de decisiones colectivas con el objetivo de **movilizar a la sociedad** y de **influir en la toma de decisiones**.

Esto convierte a la ciudadanía en potenciales activistas que pueden participar ejerciendo sus derechos en múltiples causas. Algunos movimientos como #MeToo, 15M o Stop desahucios son ejemplos de casos de éxito de activismo digital.

8.3 Cibervoluntariado

El cibervoluntariado es un medio para dar respuesta a las necesidades, problemas o intereses sociales, desde un **compromiso solidario**, para **mejorar la vida colectiva** y que se desarrolla **a través de las tecnologías de la información y la comunicación**.

La nueva ciudadanía digital genera espacios de construcción de voluntariado, en los que a través del activismo social surgen iniciativas de apoyo a diferentes causas. Las herramientas tecnológicas, como las redes sociales, permiten **dar voz a causas** que en los medios de comunicación tradicionales no alcanzarían la repercusión que se puede lograr a través de **internet**.

Desde el cibervoluntariado se desarrollan actividades tan variadas como promover la participación, difundir campañas solidarias, acompañar en línea a personas vulnerables, formar en competencias digitales, etc.

Activismo en línea

Anonymous: Comunidad virtual, descentralizada, de activistas con ciertas ideas en común y que actúan de manera coordinada en contra de objetivos específicos. Los miembros de esta organización, en su mayoría *hackers*, intentan proteger su anonimato y llevan a cabo acciones que consideran que son a favor de la libertad de expresión y neutralidad de internet, llegando a *hackear* televisiones públicas para mostrar contenidos excluidos por los Gobiernos, entre otros asuntos. Entre sus objetivos están las sociedades de derechos de autoría y los sistemas de censura gubernamentales, por lo que algunas de sus acciones no son legales.

8.4 Comunidades de software libre

El software libre es producto de un proceso de **producción colectiva** que sigue reglas y se organiza en **comunidades**. Estas comunidades están formadas por personas que, aunque no se conozcan físicamente, comparten la ideología de libertad y acceso libre al conocimiento.

Las dinámicas colectivas de comunicación e interacción se dan de manera casi espontánea y generalizada, aunque en general se tiende a usar repositorios de código, foros, wikis, chats y correo electrónico. En estos **espacios virtuales de colaboración**, cada miembro aporta sus habilidades técnicas de programación, diseño, traducción, etc.

Su origen se sitúa en 1983 cuando Richard Stallman fundó el movimiento de software libre con el objetivo de obtener y garantizar las libertades que permiten ejecutar, estudiar, cambiar y redistribuir el software. En la actualidad, el listado es muy amplio, entre las que se encuentran GNU España, ASOLIF, HispaLinux y Ubuntu España.

El software libre está disponible para casi cualquier tarea que se pueda imaginar. Desde sistemas operativos hasta miles de programas, gran parte de ellos recogidos en el directorio de software libre FSF/UNESCO. Millones de personas en todo el mundo lo utilizan.

8.5 Comunidades de hardware libre

Hardware libre es aquel cuyo **diseño** se hace **disponible públicamente** para que cualquier persona pueda **estudiar, construir, modificar o distribuir**, tanto el **original** como productos **derivados**.

Las **fuentes** de los diseños están disponibles en **formatos abiertos** de acceso libre y se fomenta el uso de **materiales** que se pueden conseguir fácilmente, así como procesos de producción **sencillos**.

Tradicionalmente, estos proyectos solo estaban al alcance de profesionales o empresas, aunque fenómenos como la fabricación digital o el **movimiento maker** están ayudando a popularizarlo. Su naturaleza colaborativa y abierta anima a que cualquier persona pueda adoptar un papel más activo, pasando de ser mera consumidora a participar en el desarrollo y la mejora de la tecnología que utiliza.

Las comunidades de desarrollo de hardware libre están formadas por grupos que comparten conocimientos y se enfocan en satisfacer el diseño de productos tecnológicos. Algunas de estas son Hackster.io, Hackaday.io, Instructables o iFixit, que giran en torno a proyectos como Raspberry Pi, Arduino, Open Compute Project, Uzebox o RepRap.



Gracias a la impresión 3D es posible fabricar prótesis, como brazos biónicos, a partir de software y hardware libre.

COMPRENDE, PIENSA, INVESTIGA...

- 18 ¿Has participado en alguna campaña en línea promovida desde alguna plataforma de iniciativa ciudadana? ¿Qué opinas sobre ellas?
- 19 ¿Qué herramientas requiere el cibervoluntariado?

- 20  Localiza algún dispositivo basado en hardware libre que sea de tu interés y veas factible construir. Estudia los pasos para diseñarlo y explícalos a tus compañeros y compañeras.

- 1  **Decálogo de intenciones.** Redacta la netiqueta adecuada para tu red social favorita.
- 2  ¿Consideras que las habilidades sociales propias de la vida real, como la empatía, la asertividad, la gestión de las emociones, el autoconocimiento, la autoestima o el espíritu crítico, también son aplicables para prevenir problemas en internet?
- 3 Consulta la LOPDGDD y responde:
 - a) ¿En qué consiste el derecho al olvido en búsquedas de internet?
 - b) ¿Con qué edad puede una persona menor registrarse en una red social en España?
 - c) Según el artículo 9, ¿qué datos se protegen de manera especial, por su relevancia, para la intimidad y la no discriminación?