Riesgos de la aceleración digital: una mirada desde el *Marco DIGCOMP2.2* y los derechos digitales de la ciudadanía

The risks of digital acceleration: a perspective from *DIGCOMP2.2 Framework* and digital citizen rights

Miguel-Ángel Vera-Baceta; **Gabriel Navarro**; **José-Antonio Gómez-Hernández**

Vera-Baceta, Miguel-Ángel; **Navarro, Gabriel**; **Gómez-Hernández, José-Antonio** (2022). "Riesgos de la aceleración digital: una mirada desde el *Marco DIGCOMP2.2* y los derechos digitales de la ciudadanía". *Anuario ThinkEPI*, v. 16, e16a19.

https://doi.org/10.3145/thinkepi.2022.e16a19

Publicado en *IweTel* el 16 de junio de 2022

Miguel-Ángel Vera-Baceta
https://orcid.org/0000-0003-3912-5882

Fundación Cepaim
Dirección Adjunta de Áreas e Investigación
C/ Estación, s/n.
30570 Murcia, España
verabaceta@cepaim.org

Gabriel Navarro
https://orcid.org/0000-0003-3987-5405

Ayuntamiento de Murcia
Servicio de Juventud
gnc@cop.es

José-Antonio Gómez-Hernández
https://orcid.org/0000-0003-4532-1142

Universidad de Murcia
Facultad de Comunicación y Documentación
Campus de Espinardo, Edificio 3
30100 Murcia, España
jgomez@um.es



Resumen: La pandemia de Covid-19 ha acelerado un proceso de transformación digital que, además, se señala como uno de los principales motores de recuperación. Aunque este proceso es imparable y necesario, la velocidad a la que se están desarrollando los acontecimientos puede atropellar a nuestra sociedad en distintos sentidos. Exclusión digital, infodemia, desinformación, adicciones digitales, hiperconexión, ciberacoso, suplantación de identidad, abusos de la privacidad, robo y perdida de datos, *phishing* o *pharming*… conforman una larga lista de amenazas digitales que crece cada día y que puede poner en riesgo pilares fundamentales de nuestra sociedad como el acceso a derechos, la convivencia, la cohesión social y, en definitiva, la propia democracia. Mediante esta nota se pretende identificar y describir vulnerabilidades y riesgos personales y sociales derivados de la aceleración digital –entre ellos la falta de competencia digital– y cómo pueden afectar al ejercicio de derechos de las personas. Para generar esta propuesta de forma estructurada nos apoyamos en el *Marco europeo de la competencia digital* (*DIGCOMP2.2*) y en la *Carta de derechos digitales* presentada por el Gobierno de España. El abordaje de

los riesgos digitales es complejo dada la amplitud de facetas de la vida a las que afecta y las distintas perspectivas desde las que se puede afrontar, por lo que este ejercicio de síntesis no pretende más que aportar una reflexión crítica que contribuya a un enfoque personal y profesional proactivo del comportamiento y la inclusión digital.

Palabras clave: Riesgos digitales; Competencias digitales; Derechos digitales; Inclusión digital; Brecha digital.

Abstract: The Covid-19 pandemic has accelerated a social digitalization process, which is considered to be one of the main tools for economic recovery. While this process is necessary, its speed could overwhelm our society in different ways. Digital exclusion, the infodemic, disinformation, digital addictions, hyperconnectivity, cyberbullying, identity theft, privacy abuse, data theft and loss, phishing, and pharming make up a long list of digital threats that grows every day and can put fundamental pillars of our society, such as access to rights, coexistence, social cohesion, and, ultimately, democracy itself, at risk. Our goal is to identify and describe personal and social vulnerabilities and risks that arise from digital acceleration –including a lack of digital competence– and how they might limit people's rights. To structure this classification of digital threats, we use the *European Digital Competence Framework* (*DIGCOMP2.2*) and the *Charter of Digital Rights* approved by the Spanish Government. Addressing digital risks is complex given the breadth of facets of life that it affects and the different angles from which it can be approached, so this synthesis exercise only aims to provide a critical reflection that contributes to a proactive personal and professional approach to this problem.

Keywords: Digital divide; Digital competence; Digital rights; Digital inclusion.

1. Introducción

El objetivo de esta nota es identificar y describir vulnerabilidades o riesgos personales y sociales derivados de la aceleración digital, entre ellos la falta de competencia digital, y cómo estos pueden afectar al acceso a derechos de las personas. Para generar esta propuesta de forma estructurada nos apoyamos en el *Marco europeo de la competencia digital* (*DIGCOMP2.2*) (**Vuorikari**; **Kluzer**; **Punie**, 2022) y en la *Carta de derechos digitales de la ciudadanía* (*Gobierno de España*, 2021a). El abordaje de los riesgos digitales es complejo dada la amplitud de facetas de la vida a las que afecta y las distintas perspectivas desde las que se puede afrontar, por lo que este ejercicio de síntesis no pretende más que aportar una reflexión crítica que contribuya a un enfoque personal y profesional proactivo del comportamiento y la inclusión digital.

La pandemia aceleró una transformación digital que supone un cambio cultural global –iniciado hace más de treinta años– y que afecta a trabajo, educación, relaciones sociales, consumo, ocio, trámites administrativos o acceso a los servicios públicos. Somos cada día más dependientes de la tecnología, sus entornos, dispositivos y servicios, por lo que las personas con dificultades para su utilización quedan en riesgo de exclusión no solo digital, también social.

Aunque la sociedad española ha mostrado fortalezas –por ejemplo, una sólida infraestructura de telecomunicaciones que ha podido dar respuesta al rápido incremento de demanda de servicios–, también ha evidenciado carencias, en especial las relacionadas con una parte importante de la ciudadanía que no cuenta con los medios o las capacidades necesarias para enfrentarse al espacio digital en condiciones igualitarias y con las garantías necesarias. En España se estima que 12,4 millones de personas están en riesgo de pobreza (*INE*, 2021a) y 15 millones –una de cada cuatro– no cuentan con competencias digitales básicas, situación que se repite de manera análoga en el resto de Europa (*European Commission*, 2021). Unos datos que ponen de manifiesto el riesgo de dejar atrás a muchas personas en un contexto donde la transformación digital se señala como uno de los principales motores de recuperación económica y social pospandemia. Si además tenemos en cuenta que el porcentaje de la población que utiliza Internet a diario en España es de un 83,1% –con un incremento de más de cinco puntos y medio respecto al año anterior– y que en el último año un 94,5% de las personas utilizaron Internet (*Fundación Telefónica*, 2021), podemos suponer que una parte importante de la ciudadanía está utilizando la tecnología y sus distintas aplicaciones sin las competencias necesarias. Debemos tener en cuenta que

Somos testigos de preocupantes dinámicas vinculadas al mundo digital, que generan una larga lista de amenazas y ponen en peligro pilares fundamentales de nuestra sociedad como el acceso a derechos, la cohesión social o la propia convivencia democrática

el *DIGCOMP2.2* establece que las personas deben contar, al menos, con un nivel intermedio (B1) para alcanzar un dominio autónomo que no requiera de asistencia (**Vuorikari**; **Kluzer**; **Punie**, 2022).

¿Cuáles son los saberes que contribuyen a dar respuesta a las necesidades de una sociedad cada vez más digital? ¿a qué riesgos nos enfrentamos como sociedad derivados de la intensa transformación cultural que vivimos?

En esta situación somos testigos de preocupantes dinámicas vinculadas al mundo digital, que generan una larga lista de amenazas y ponen en peligro pilares fundamentales de nuestra sociedad como el acceso a derechos, la cohesión social o la propia convivencia democrática. Por ejemplo, fenómenos relacionados con la infodemia como sobreinformación, desinformación, polarización o proliferación de discursos populistas y mensajes de odio; problemas derivados del uso incorrecto y excesivo, entre otros, incremento de adicciones digitales, hiperconexión, ciberacoso, *grooming, sexting,* suplantación de identidad y *catfishing*, abusos de la privacidad, *phishing, pharming*, robo, secuestro o perdida de datos; consumo de contenidos inadecuados (violentos o pornográficos...) y un largo etcétera.

Considerando que la aceleración digital es imparable y con la hipótesis de que la brecha digital y el uso generalizado de la tecnología sin las competencias necesarias pueda estar relacionado con los problemas mencionados, debemos preguntarnos una vez más: ¿Cuáles son los saberes que contribuyen a dar respuesta a las necesidades de una sociedad cada vez más digital? ¿A qué riesgos nos enfrentamos como sociedad derivados de la intensa transformación cultural que vivimos? ¿Cómo conectamos la competencia digital con el conjunto de factores psicosociales y económicos que producen vulnerabilidad a las personas en el actual contexto?

2. *Marco Europeo de las Competencias Digitales*

Tradicionalmente, la competencia digital ha estado vinculada a la capacidad de las personas para usar las herramientas tecnológicas enfocadas en buena parte a la empleabilidad y a las necesidades del desempeño profesional. Esta visión ha ido evolucionando de la mano de la propia transición digital, dotándola de una dimensión mucho más amplia adaptada al protagonismo que las tecnologías han ido tomando en nuestras vidas. Así, a esta mirada inicial se fueron incorporando competencias relacionadas con las habilidades que permitieran el aprovechamiento del potencial de la sociedad de la información y sus diferentes aspectos socioculturales (**Cañón-Rodríguez**; **Grande-de-Prado**; **Cantón-Mayo**, 2016; **Van-Dijk**, 2017; 2020; **Cabero-Almenara**; **Ruiz-Palmero**, 2017; **Mihelj**; **Leguina**; **Downey**, 2019) hasta, finalmente, conformar una interpretación holística de la competencia digital vinculada a la necesaria participación de un contexto tecnológico que, cada vez más, influye en el desarrollo de los distintos aspectos de la vida de las personas.

En ese sentido, el *DIGCOMP2.2* hace una propuesta integral que abarca:

- competencias específicas de carácter técnico relacionadas con la dimensión instrumental –por ejemplo, la navegación o la protección de los dispositivos–;
- competencias relacionadas con una dimensión social del contexto digital –como el compromiso ciudadano con las tecnologías digitales–;
- competencias relacionadas con el desarrollo de las capacidades cognitivas –como la creación de contenidos, la comunicación y la gestión de la información–;
- competencias vinculadas a la vigilancia de la seguridad, de la salud o del bienestar de las personas y del medioambiente.

Una concepción amplia de la competencia digital que podría verse complementada en ciertos aspectos por recomendaciones como la *2018/C 189/1* del *Consejo Europeo* (2018) sobre desinformación, alfabetización en información y competencias clave para el aprendizaje permanente, o por el *Plan de Educación Digital 2021-2027* de la *Comisión Europea* (2020) sobre diversidad cultural y creativa (**Gómez-Hernández**; **Vera-Baceta**, 2021).

Con todo, el *DIGCOMP2.2* se ha convertido en un referente internacional utilizado en diferentes campos educativos y de definición de políticas vinculadas a la transformación digital y la capacitación tecnológica (*Gobierno de España*, 2021b). Organizado en cinco áreas competenciales y veintiuna competencias específicas, establece ocho niveles de dominio, donde el primero correspondería al nivel más básico, el octavo al más especializado y el tercero (B1) es el primero que implica un manejo autónomo.

Tabla 1. Resumen del *DIGCOMP 2.2*

Áreas competenciales	Competencias
A. Información y alfabetización de datos	A.1. Navegar, buscar y filtrar de datos, información y contenido digital. A.2. Evaluar datos, información y contenido digital. A.3. Gestionar datos, información y contenido digital.
B. Comunicación y colaboración online	B.1. Interactuar mediante tecnologías digitales. B.2. Compartir mediante tecnologías digitales. B.3. Compromiso ciudadano con tecnologías digitales. B.4. Colaborar a través de tecnologías digitales. B.5. Netiqueta (pautas de comportamiento en la Red). B.6. Gestionar la identidad digital.
C. Creación de contenidos digitales	C.1. Desarrollar contenido digital. C.2. Integrar y reelaborar contenido digital. C.3. *Copyright* y licencias. C.4. Programar.
D. Seguridad en la Red	D.1. Proteger los dispositivos. D.2. Proteger los datos personales y la privacidad. D.3. Proteger la salud y el bienestar. D.4. Proteger el medio ambiente.
E. Resolución de problemas	E.1. Resolver problemas técnicos. E.2. Identificar necesidades y respuestas tecnológicas. E.3. Uso creativo de la tecnología digital. E.4. Identificar brechas digitales.

3. *Carta de derechos digitales*

La rápida evolución de las tecnologías y sus entornos no solo desborda a la ciudadanía; también las propias instituciones y los distintos órganos reguladores sufren una brecha digital relacionada con el tiempo que necesitan para entender las nuevas realidades y adaptar los marcos normativos y legislativos de manera que se pueda seguir garantizando el cumplimiento de derechos y deberes. *Naciones Unidas* (2019) apunta que, en muchos casos, la aplicación de las leyes y tratados de derecho al contexto actual no es obvia ya que están redactados en una era anterior a la digital. Se debe tener en cuenta que el entorno digital no es fiel reflejo del mundo real y altera roles, funciones y reglas. Esta situación crea nuevos contextos y conflictos que deben resolverse mediante la adaptación de la legislación y la reinterpretación del ordenamiento jurídico conforme a nuevas circunstancias (*Gobierno de España*, 2021a). Por ello, el Gobierno de España presentó en julio de 2021 la ya citada *Carta de derechos digitales*, que ofrece un marco de referencia, pionero internacionalmente, sobre los derechos de la ciudadanía que se deben garantizar en la nueva realidad digital.

Aunque sin carácter normativo, la *Carta* recoge un conjunto de principios y derechos que pretenden guiar futuras normas y proteger los derechos individuales y colectivos de las personas en el espacio digital, entre ellos, los derechos de libertad, igualdad, participación y conformación del espacio público, así como del entorno laboral y empresarial. No se trata, por tanto, de la creación de nuevos derechos fundamentales sino del perfilado de los más relevantes en el entorno y los espacios digitales. Para nuestro análisis es relevante el carácter prospectivo de este documento, pues intenta adelantar los contextos y escenarios digitales objeto de conflicto y legitima los principios aplicables, ayudando a articular, de manera ordenada y estructurada, la respuesta dada a los principales retos relacionados con el uso de las tecnologías y el desarrollo de las personas en el contexto digital. Se articula en seis bloques que dan cabida a veintiocho principios (tabla 2).

¿Cómo conectamos la competencia digital con el conjunto de factores psicosociales y económicos que producen vulnerabilidad a las personas en el actual contexto?

Tabla 2. Principios de la *Carta de derechos digitales*

Carta de derechos digitales	
CDD1. Derechos de libertad	CDD1.1. Derechos y libertades en el entorno digital. CDD1.2. Derecho a la identidad en el entorno digital. CDD1.3. Derecho a la protección de datos. CDD1.4. Derecho al pseudonimato. CDD1.5. Derecho de la persona a no ser localizada y perfilada. CDD1.6. Derecho a la ciberseguridad. CDD1.7. Derecho a la herencia digital.
CDD2. Derechos de igualdad	CDD2.1. Derecho a la igualdad y a la no discriminación en el entorno digital. CDD2.2. Derecho de acceso a Internet. CDD2.3. Protección de las personas menores de edad en el entorno digital. CDD2.4. Accesibilidad universal en el entorno digital. CDD2.5. Brechas de acceso al entorno digital.
CDD3. Derechos de participación y conformación del espacio público	CDD3.1. Derecho a la neutralidad de Internet. CDD3.2. Libertad de expresión y libertad de información. CDD3.3. Derecho a recibir libremente información veraz. CDD3.4. Derecho a la participación ciudadana por medios digitales. CDD3.5. Derecho a la educación digital. CDD3.6. Derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas.
CDD4. Derechos del entorno laboral y empresarial	CDD4.1. Derechos en el ámbito laboral. CDD4.2. La empresa en el entorno digital.
CDD5. Derechos digitales en entornos específicos	CDD5.1. Derecho de acceso a datos con fines de archivo en interés público, fines de investigación científica o histórica, fines estadísticos, y fines de innovación y desarrollo. CDD5.2. Derecho a un desarrollo tecnológico y a un entorno digital sostenible. CDD5.3. Derecho a la protección de la salud en el entorno digital. CDD5.4. Libertad de creación y derecho de acceso a la cultura en el entorno digital. CDD5.5. Derechos ante la inteligencia artificial. CDD5.6. Derechos digitales en el empleo de las neurotecnologías.
CDD6. Garantías y eficacia	CDD6.1. Garantía de los derechos en los entornos digitales. CDD6.2. Eficacia.

4. Riesgos sociales y competencia digital

De acuerdo con la *Carta* se pueden identificar dos bloques destacados de derechos. El primero tiene que ver con el derecho de acceso y la necesidad de garantizar tanto los medios como las condiciones de vida que permitan a las personas participar de este entorno. Y el segundo está relacionado con la apropiación personal y comunitaria de los medios digitales de forma relevante; es decir, el proceso de asimilación y adaptación de las personas a los avances de la tecnología y sus consecuencias.

4.1. Brecha digital de acceso

El primer bloque sobre derechos en el entorno digital tiene una relación directa con la denominada "brecha digital de acceso". Uno de los pasos más evidentes en la cadena de la transición digital es contar con las condiciones, conectividad y equipamiento necesarios para acceder a este entorno, de hecho, su déficit se señala como un factor determinante de exclusión tanto digital como social. Por sus características, esta brecha afecta con mayor rigor a las personas más vulnerables de nuestra sociedad –víctimas o en riesgo de pobreza y exclusión social– a las que, en muchas ocasiones, el entorno digital les es distante (*EAPN*, 2021). Así, estos colectivos no solo se enfrentan a las dificultadas para costear los gastos derivados de la conectividad y los medios tecnológicos necesarios, también suelen tener situaciones personales y laborales complejas que les impiden contar con un espacio –físico y temporal– adecuado que les permita participar de este espacio digital.

Otro de los aspectos fundamentales de la brecha de acceso está relacionado con las diferencias encontradas entre las infraestructuras de distintas zonas geográficas. Existen asimetrías en las formas de acceso a recursos y servicios atendiendo al tamaño de la población de referencia, su localización o su nivel de riqueza (**Rodicio-García** *et al.*, 2020), situación que entra en conflicto con los objetivos de desarrollo sostenible, el desarrollo del medio rural, la lucha contra la despoblación y el reto demográfico.

4.2. Brecha digital de uso

En relación con el segundo bloque de derechos –que hemos denominado de apropiación–, aunque se pueden identificar distintos aspectos y alcances, uno de los mayores retos actuales tiene que ver con la falta de competencia para utilizar la tecnología: la "brecha de uso"–. Así, el *Informe 2020 sobre el*

índice de economía y sociedad digital (DESI) contabiliza 15 millones de personas en España sin competencias digitales básicas, y aproximadamente 3,7 millones que nunca han accedido a Internet.

La brecha digital de uso se convierte, de esta manera, en un problema social que afecta a la ciudadanía española en sentido amplio. La *Agenda España Digital 2025* indica que es clave

> "cerrar las nuevas brechas de desigualdad social por la falta de uso de Internet", pues "la capacidad de uso de redes actúa cada vez más como vector de exclusión social, afectando especialmente a aquellos colectivos más vulnerables" (*Gobierno de España*, 2020).

Además, otros colectivos –no identificados anteriormente como digitalmente vulnerables– están expuestos por la falta de esta competencia y una falta de apropiación tecnológica significativa (**Vera-Baceta**; **Gómez-Hernández**, 2021), entre los que se podrían señalar: sectores de población como personas mayores de 55 años, personas que se dedican a labores del hogar, pensionistas, personas con nivel de estudios inferior a la segunda etapa de secundaria o personas que cuentan con una renta mensual inferior a los 1.600 euros (*ONTSI*, 2021a).

Debemos tener en cuenta que la brecha digital de uso puede alcanzar a personas que disponen de dispositivos móviles y equipos informáticos con conectividad, pero que al no contar con las capacidades para aprovecharlas se están enfrentando al contexto digital sin garantías suficientes

Y, de hecho, esta situación puede llegar a darse incluso entre nativos digitales, como señala el último informe *PISA*, que pone de manifiesto que los estudiantes españoles de 15 años están por debajo de la media europea en habilidades para manejar con eficacia contenidos digitales y que tienen mayores dificultades para detectar textos sesgados o evaluar las fuentes (*OCDE*, 2021). Como argumenta **Álvarez-Sigüenza** (2019), el hecho de que los estudiantes hayan nacido en la era digital no es condición suficiente para suponer que cuentan con las competencias tecnológicas que demanda la sociedad actual.

Por tanto, frente a la "brecha digital generacional" como supuesto paradigma, se ha acreditado una significativa brecha digital intra-generacional: quienes más se benefician del uso de la tecnología digital son los que tienen más capital social, capital humano y capital financiero, independientemente de la edad, observándose una distancia evidente entre las prácticas de los jóvenes desfavorecidos y las expectativas de la sociedad respecto a sus usos digitales. Así, mientras que algunos jóvenes son capaces de elegir sus preferencias entre las diferentes funciones de Internet y de evolucionar en función de las circunstancias, otros se limitan a los "usos limitados" de entretenimiento audiovisual y la comunicación instantánea (**Navarro**, 2013).

Además, debemos tener en cuenta que la brecha digital de uso puede alcanzar a personas que disponen de dispositivos móviles y equipos informáticos con conectividad, pero que al no contar con las capacidades para aprovecharlas se están enfrentando al contexto digital sin garantías suficientes.

Para enumerar e intentar comprender los riesgos digitales derivados de este problema, en los siguientes epígrafes hemos considerado el *Marco DIGCOMP2.2* y sus cinco ámbitos competenciales, y emparejado los riesgos identificados con derechos de la *Carta*.

4.2.1. Riesgos por insuficiente "Información y alfabetización de datos" (Ámbito A de DIGCOMP2.2

Este primer ámbito de la competencia digital identifica las capacidades precisas para:

- articular las necesidades de información;
- localizar y recuperar datos, información y contenidos digitales;
- juzgar la relevancia de las fuentes de información y su contenido;
- almacenar, gestionar y organizar datos, información y contenidos digitales.

Roetzel (2019) señala que descubrir los efectos de la búsqueda, selección, procesamiento y evaluación de la información, sus sesgos y limitaciones es clave en el proceso de comprensión y toma de decisiones de las personas. Y en su definición de "alfabetización informacional", *CILIP* destaca la necesaria capacidad de pensar de forma crítica y emitir opiniones razonadas de manera informada y comprometida como una condición para el desarrollo pleno de las personas y de la sociedad (**Coonan** *et al.*, 2018).

En la vida diaria, la ausencia de competencias informacionales –aun no siendo conscientes de ello o de forma imprecisa– puede conllevar problemas (**Gómez-Hernández**; **Fernández-Rincón**, 2020) como:

- desorientación y navegación improductiva por falta de estrategia o rumbo;
- dificultad para evaluar y seleccionar la información relevante;
- acumulación de información sin valor o "síndrome de Diógenes" digital;
- idealización de las redes como fuente principal de información;

- uso de información descontextualizada desconociendo la credibilidad e intencionalidad de las fuentes;
- vulnerabilidad a noticias falsas;
- exposición a la manipulación política o ideológica;
- difusión de información irrelevante, falsa o de forma indiscriminada, conduciendo todo ello a una probable incapacidad para el pensamiento autónomo y crítico.

Se trata de un ámbito competencial fundamental en una sociedad de la información en la que se da la paradoja de que una sobreexposición a mensajes está produciendo justo el efecto contrario, una *infrainformación* (**Aguaded**, 2014). Según **Eppler** y **Mengis** (2010), cuando el nivel de datos disponible en un sistema supera la capacidad de procesamiento se da el fenómeno de la infodemia, un flujo constante de mensajes de diversos orígenes, recorridos y fines que dan cabida tanto a información rigurosa como a otra cuestionable o errónea que, en cualquier caso, acaba desbordando a las personas.

Cuando el nivel de datos disponible en un sistema supera la capacidad de procesamiento se da el fenómeno de la infodemia

Uno de los aspectos más preocupantes tiene que ver precisamente con la desinformación y la proliferación de rumores, información desvirtuada o directamente falsa. Este fenómeno que puede surgir espontáneamente –a consecuencia de las dinámicas de la comunicación social– es más preocupante cuando se usa de forma intencionada como estrategia de manipulación (**Salaverría** *et al.*, 2020): se ha convertido en una oportunidad para grupos extremistas que aprovechan el ecosistema digital para manipular marcos ideológicos, conductas, establecer agendas y propagar información falsa de manera deliberada. Para ello, hacen un uso estratégico de redes sociales, medios, memes y *bots* y aprovechan las debilidades de los distintos agentes dependientes de las métricas, el sensacionalismo, la novedad y el *clickbait* (**Marwick**; **Lewis**, 2017). Una de las grandes amenazas es la expansión de discursos de odio que en el pasado tenían una difícil difusión en los grandes medios pero que, ahora, han encontrado una oportunidad para llegar a un público más amplio amparados en la horizontalidad de las redes y, paradójicamente, en la democratización de los medios digitales (**Bustos-Martínez** *et al.*, 2019)**.** La profusión de mensajes contradictorios estimulada por estos grupos puede acabar contribuyendo también a disminuir la confianza de las personas e inducir a su desconexión.

Estamos siendo testigos de situaciones extremadamente graves relacionadas con estos fenómenos como, por ejemplo, la denominada por la *Unesco* (2020) "desinfodemia" que incrementó la dificultad de afrontar la compleja pandemia (**Roozenbeek** *et al.*, 2020), los efectos nocivos que determinados usos de la información a través de redes sociales pueden estar teniendo sobre la juventud (**Seetharaman**, 2021), o el asalto al Capitolio, corazón de la democracia estadounidense (**Sulbarán-Lobera**, 2021).

En resumen, fenómenos como infoxicación, desinformación, noticias falsas o posverdad han pasado a formar parte de nuestra cotidianidad. Desafortunadamente, están dejando notar sus efectos, entrando en conflicto con principios fundamentales identificados en la *Carta de Derechos Digitales* como la libertad de información, el derecho a recibir libremente información veraz o la libertad de expresión.

Tabla 3. Riesgos relacionados con el ámbito competencial "información y alfabetización en datos"

A. Información y alfabetización de datos			
Competencias específicas	**Derechos digitales relacionados**	**Amenazas digitales**	**Riesgos sociales**
A.1. Navegar, buscar y filtrar de datos, información y contenido. A.2. Evaluar datos, información y contenido digital. A.3. Gestionar datos, información y contenido digital.	CDD3. Derechos de participación y de conformación del espacio público: CDD3.1. Derecho a la neutralidad de Internet. CDD3.2. Libertad de expresión y libertad de información. CDD3.3. Derecho a recibir libremente información veraz.	Infoxicación/ Sobreinformación. Desinformación y proliferación de noticias falsas. Proliferación de mensajes populistas / de odio Efecto de cámaras de eco (burbujas filtro)	Problemas de convivencia. Polarización social. Cuestionamiento del sistema democrático. Incremento de conductas violentas, xenófobas y delitos de odio. Baja tolerancia a lo distinto y a las ideas y opiniones de los otros.

4.2.2. Riesgos por falta de o inadecuada "Comunicación y colaboración online" y "Creación de contenidos digitales"

Siguiendo con la revisión del *DIGCOMP2.2*, el ámbito competencial sobre "Comunicación y colaboración online" (B) identifica las capacidades necesarias para:

- interactuar, comunicar y colaborar a través de las tecnologías digitales teniendo presente la diversidad cultural y generacional;
- participar en la sociedad a través de los servicios digitales públicos y privados a través de una ciudadanía participativa;
- gestionar la presencia digital a través de la identidad y reputación online.

De manera específica se señalan competencias sobre normas sociales y cívicas –por ejemplo, diferenciar normas de comportamiento, elegir formas de comunicación y estrategias básicas adaptadas a una audiencia determinada–, competencias relacionadas con la iniciativa ciudadana –como la participación y compromiso de la ciudadanía a través de tecnologías digitales– y algunas competencias más novedosas relacionadas con la construcción de una identidad digital. Adicionalmente, el ámbito "Creación de contenidos digitales" (C) complementa aspectos específicos de la conciencia y expresión culturales como:

- identificación de formas de crear y editar contenidos;
- elección de formas de expresión;
- capacidad de crear contenido original e identificar normas y licencias vinculadas al uso de datos, información y contenidos digitales como los derechos de autor.

Son capacidades y valores en los que se insiste en la mencionada *Recomendación 2018/C 189/01 del Consejo de la Unión Europea sobre competencias clave para el aprendizaje permanente*, entre las que cita (European Commission, 2019):

- capacidad de comunicarse de forma adecuada y eficaz;
- capacidad de trabajar con los demás de forma constructiva;
- empatizar y manejar conflictos en un contexto inclusivo y solidario;
- capacidad de actuar sobre oportunidades e ideas y transformarlas en valores para los demás;
- conciencia y el compromiso con la cultura y el arte, comprendiendo y respetando cómo las ideas se expresan creativamente en todas sus formas y diversidad.

Son dos ámbitos competenciales esenciales para afrontar los retos de una sociedad globalizada, interconectada y dependiente de la tecnología, en la que la comunicación ha difuminado los límites entre emisor y receptor y se ha desencadenado una amplia cultura de la participación (**Marta-Lazo**; **Gabelas-Barroso**; **Marfil-Carmona**, 2019). Si tenemos en cuenta, además, la aceleración digital y el distanciamiento social provocado por la pandemia (**Sá** *et al*., 2021), la posibilidad de utilizar la tecnología como medio de comunicación, de expresión y de colaboración se ha convertido en un factor relacional determinante que puede condicionar nuestras vidas.

¿Qué riesgos se han identificado en este campo? Tenemos en primer lugar usos del espacio digital especialmente preocupantes para los más jóvenes y la construcción de su identidad personal y digital: *Unicef* (2021) describe que el 42% de los adolescentes ha recibido mensajes de contenido sexual, de los que más de la mitad han acabado realizando prácticas de sexting –envío de fotos o videos propios con contenido erótico o sexual– y que uno de cada diez adolescentes ha recibido una propuesta sexual en Internet por parte de un adulto. Situaciones que se pueden ver agravadas por el contacto con extraños –un 57,2% ha aceptado a desconocidos en redes sociales– o la exposición a contenidos violentos, dañinos o pornográficos –un 35,4% han visitado páginas con contenidos eróticos o pornográficos–. Por otra parte, el ciberacoso se sitúa en una tasa del 22,4% –aproximadamente dos de cada diez adolescentes podrían estar siendo víctimas de esta práctica– creando dinámicas perversas en las que la mitad de quienes lo sufren acaban ejerciéndolo. De esta manera, lo que en principio puede tener que ver con dinámicas conductuales acaba derivando en graves problemas para la integridad de las personas más jóvenes.

Fenómenos como infoxicación, desinformación, noticias falsas o posverdad han pasado a formar parte de nuestra cotidianidad y, desafortunadamente entrando en conflicto con principios fundamentales identificados en la Carta de Derechos Digitales como la libertad de información, el derecho a recibir libremente información veraz o la libertad de expresión.

La *Organización Mundial de la Salud* ha alertado sobre un "uso problemático" de la tecnología, Internet y las redes por parte de la adolescencia, que **Rial-Boubeta** *et al.* (2015) cuantificaron en un 33%. En España, un estudio muy reciente del *Centro Reina Sofía* sobre adolescencia y juventud (**Calderón-Gómez**; **Gómez-Miguel**, 2022) muestra que el 79,9% de los jóvenes utiliza las tecnologías digitales para actividades de ocio digital todos los días, sólo por detrás de los usos para comunicación (84,1%)

y búsqueda de información (83,6%), con un promedio de 6,95 horas al día dedicadas al consumo de contenido audiovisual y otras actividades de ocio vinculadas con lo digital. Debemos tener en cuenta de cara a la prevención de riesgos posibles que prácticamente la totalidad de los jóvenes sigue activamente a personas que crean contenido online e *influencers*, sobre todo a través de *Instagram* (81,6%), la red social más popular, junto con *YouTube* (58,9%) y *TikTok* (55,6%).

En segundo lugar, en lo que se refiere a la participación, no contar con una ciudadanía responsable y comprometida que pueda implicarse plenamente en la vida cívica y que comprenda los conceptos y estructuras sociales, económicas, jurídicas y políticas, puede poner en riesgo aspectos tan importantes como la construcción social, la salud democrática y la sostenibilidad global. La importancia de una mayor participación ciudadana se reconoce en el *Tratado de Lisboa* (*Unión Europea*, 2007) y se refuerza en la *Nueva agenda estratégica para la UE 2019-2024* de la *Comisión Europea* (2019), que considera que la contribución ciudadana a través de la creación y la innovación es clave para el desarrollo común y para la construcción de una ciudadanía más unida, más fuerte y democrática. De igual manera, *Naciones Unidas* (2019) declaró en la cumbre sobre los *Objetivos de Desarrollo Sostenible* (*ODS*) que la participación ciudadana era esencial, reclamando a los diferentes estados que la garantizaran de manera amplia. La falta de participación se convierte en un déficit democrático que impide a la ciudadanía formar parte de la toma decisiones, de la actividad pública y, además, aleja a las personas de la construcción social.

Sin competencias en este ámbito estaremos interactuando de forma inadecuada con otras personas, podemos estar atendiendo de forma excesiva a una identidad digital irreal e idealizada o no aprovecharemos las posibilidades digitales para colaborar con otros, participar creativamente o ejercer derechos ciudadanos. Se ponen en riesgo principios de la *Carta* como el derecho a la igualdad y a la no discriminación en el entorno digital, el derecho a la identidad en el entorno digital, el derecho a la participación ciudadana o la libertad de creación y el derecho de acceso a la cultura en el entorno digital.

Tabla 4. Riesgos relacionados con los ámbitos competenciales de "comunicación y colaboración online" y "creación de contenidos digitales"

B. Comunicación y colaboración online y C. Creación de contenidos digitales.			
Competencias específicas	**Derechos digitales relacionados**	**Amenazas digitales**	**Riesgos sociales**
B.1. Interactuar mediante tecnologías digitales. B.2. Compartir mediante tecnologías digitales. B.3. Compromiso ciudadano con tecnologías digitales. B.4. Colaborar a través de tecnologías digitales. B.5. Netiqueta (pautas de comportamiento en la Red). B.6. Gestionar la identidad digital. C.1. Desarrollar contenido digital. C.2. Integrar y reelaborar contenido digital. C.3. Copyright y licencias. C.4. Programar. E.3. Uso creativo de la tecnología digital.	CDD2. Derechos de Igualdad. CDD2.1. Derecho a la igualdad y a la no discriminación en el entorno digital. CDD2.3. Protección de las personas menores de edad en el entorno digital CDD3. Derechos de participación y de conformación del espacio público: CDD3.4. Derecho a la participación ciudadana por medios digitales. CDD3.6. Derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas. CDD5. Derechos digitales en entornos específicos. CDD5.4. Libertad de creación y derecho de acceso a la cultura en el entorno digital.	Distanciamiento de la realidad. Fomento del individualismo. Superficialidad, idealización virtual y flexting. Consumo de contenidos inadecuados. Conductas de comportamiento inapropiados o de contextualizad Frustración ante la incapacidad de realización personal, expresión y participación. *Gaslighting* o abuso emocional. Ciberacoso y ciberbullying. Grooming y sexting. Creación de identidades falsas o catfishing. Rechazo al diferente y falta de empatía. Incapacidad de empatizar	Insolidaridad y aislamiento social. Desapego, falta de pertenencia y falta de cohesión social. Incremento de desigualdades y factores de exclusión. Proliferación de tratos discriminatorios y problemas de convivencia. Estancamiento social. Déficit democrático y degeneración política. Daños al patrimonio, la cultura, el arte y la memoria colectiva. Pederastia y delitos sexuales.

4.2.3. Riesgos por gestión inadecuada de la "Seguridad en la Red" e incapacidad de "Resolución de problemas"

El ámbito "Seguridad en la Red" (D) identifica las competencias específicas necesarias para realizar un uso seguro de la tecnología y las redes que las interconectan, empezando por comprender todos los riesgos y amenazas a los que nos exponemos en los entornos digitales, así como sus consecuencias. Por ello, no solo se consideran competencias a) enfocadas a la protección de los dispositivos, contenidos, datos personales y la privacidad, sino que también se incluyen b) aquellas necesarias para proteger nuestra salud física y psicológica, y c) otras relacionadas con la necesidad de conocer cómo las

tecnologías digitales afectan a la inclusión y el bienestar social, y qué impacto tienen sobre el entorno y el medioambiente –tanto de manera directa como a través de nuestro uso–. Por su parte, el ámbito "Resolución de problemas" (E) señala competencias específicas que, aunque transversales, afectan singularmente a diferentes aspectos de la "Seguridad en la Red":

- capacidad de identificar necesidades y problemas vinculadas al uso de la tecnología;
- resolver problemas conceptuales y situaciones problemáticas en entornos digitales;
- utilizar herramientas digitales para innovar en procesos y productos y para estar al día de la evolución digital.

Proteger los dispositivos, los datos personales y la privacidad

Desde el punto de vista tecnológico, un aspecto fundamental de la seguridad tiene que ver con la protección de los dispositivos y contenidos digitales. Para ello, el *DIGCOMP2.2* señala que es necesario conocer las medidas de seguridad y protección para utilizarlos, y prestar la debida atención a la fiabilidad y la privacidad de sus sistemas y los datos que se generan.

En la actualidad se estima que un 83,1% de la población accede todos los días a Internet y el 81% se conecta varias veces al día (*ONTSI*, 2021b). Esta conexión continuada produce una demanda de servicios digitales –correo electrónico, redes sociales, mensajería instantánea, banca y la administración electrónica, tiendas online, trabajo a distancia, formación en línea, contenidos digitales como música, cine, televisión…– que genera un ritmo frenético de transacciones de gran valor y que, por lo tanto, amplia las oportunidades de fraude. En la encuesta TIC-H (*INE*, 2021b) un 31,5% de los internautas españoles declaró haber sufrido algún incidente de seguridad mientras usaba Internet en el último año, incluyendo esto a los nativos digitales, que tienen dificultades para gestionar la privacidad o garantizar la seguridad en línea (**Álvarez–Sigüenza**, 2019; *OCDE*, 2021). De los incidentes estudiados, los más frecuentes tienen que ver con mensajes fraudulentos o *phishing* (21,1% de los internautas), la redirección a páginas web falsas que solicitan información personal o *pharming* (18,7%) y la utilización fraudulenta de tarjetas de crédito o débito (3,4%). También se estima que durante el año 2020 el 8% de la población española que accedió a Internet desde el móvil perdió datos a consecuencia de virus informáticos, por encima de una media europea del 4%. Entre los ataques más comunes también se identificó el denominado *ransomware* utilizado para el secuestro de datos (*ONTSI*, 2021c). Estas situaciones afectan principalmente a la privacidad y a la integridad de la información (datos, archivos y sistemas) tanto de carácter personal como profesionales, desencadenando distintos tipos de pérdidas.

Otro aspecto importante de la privacidad está relacionado con el marco del *big data*, la inteligencia artificial (IA) y las neurociencias. Deberíamos ser conscientes de las consecuencias reales de la cesión de nuestros datos (**Llaneza**, 2019), que puede conllevar conflictos éticos por usos cuestionables, como el perfilado y la localización con fines comerciales, laborales o políticos, la influencia de los algoritmos en la toma de decisiones y juicios de las personas (**Agudo-Díaz**, 2021) y la discriminación algorítmica por sistemas de IA, la manipulación de datos de salud, etc.

Una investigación llevada a cabo por el *Irish Council for Civil Liberties* (*ICCL*, 2022) desvela que Google escruta datos 436 veces por persona y día de media en España (por encima de la media europea, 376 veces) para obtener información sobre su localización y actividad en Internet con fines de perfilado y comercialización. Otro ejemplo tiene que ver con la utilización de herramientas basadas en la IA y el aprendizaje automático o *machine learning* (ML): según **Yam** y **Skorburg** (2021) cada vez es más común el uso de estas tecnologías aplicadas a la toma de decisiones empresariales, como en procesos selectivos de personal, pudiendo llevar por sus limitaciones a aplicar criterios discriminatorios no permitidos en procesos convencionales.

En el plano sociopolítico, este mismo año hemos podido ser testigos de la estrategia de ciberataques en el contexto de la guerra de Rusia contra Ucrania, llevando al presidente estadounidense Joe Biden a pedir a empresas y organizaciones privadas el cierre de sus puertas digitales (**Tidy**, 2022). O el reciente caso *Pegasus* de espionaje a dispositivos móviles de diferentes gobiernos e importantes mandatorios internacionales ha puesto el foco sobre la importancia de la ciberseguridad y la privacidad (**Sevillano**, 2022).

Todo este conjunto de riesgos vinculados a la "Seguridad en la Red" puede comprometer principios fundamentales de la *Carta de derechos digitales*, relacionados con la propia libertad, con el derecho a la identidad en el entorno digital, el derecho a la protección de datos, el derecho al pseudonimato, el derecho de las personas a no ser localizadas y perfiladas, el derecho a la ciberseguridad, el derecho a la herencia digital o los derechos de las personas ante la IA artificial o el empleo de neurotecnologías.

Tabla 5. Riesgos relacionados con los ámbitos competenciales de "Seguridad en la Red" y "Resolución de problemas"

D. Seguridad en la Red y E. Resolución de problemas			
Competencias específicas	**Derechos digitales relacionados**	**Amenazas digitales**	**Riesgos sociales**
D.1. Proteger los dispositivos. D.2. Proteger los datos personales y la privacidad. E.1. Resolver problemas técnicos. E.2. Identificar necesidades y respuestas tecnológicas. E.4. Identificar brechas digitales.	CDD1. Derechos de libertad: CDD1.2. Derecho a la identidad en el entorno digital CDD1.3. Derecho a la protección de datos. CDD1.4. Derecho al pseudonimato. CDD1.5. Derecho de la persona a no ser localizada y perfilada. CDD1.6. Derecho a la ciberseguridad. CDD1.7. Derecho a la herencia digital. CDD2. Derechos de Igualdad. CDD2.5. Brechas de acceso al entorno digital. CDD5. Derechos digitales en entornos específicos: CDD5.1. Derecho de acceso a datos con fines de archivo en interés público, fines de investigación científica o histórica, fines estadísticos, y fines de innovación y desarrollo. CDD5.5. Derechos ante la inteligencia artificial. CDD5.6. Derechos digitales en el empleo de las neurotecnologías.	Abusos de la privacidad Robo de datos Suplantación de identidad Creación de identidades falsas Pérdida de datos e información significativa. Problemas de ética digital. Delitos contra la propiedad intelectual. Perfilado y localización.	Daños a la propiedad privada e intelectual. Daños a la intimidad. Discriminación y falta de libertades. Manipulación por efecto de la personalización de las respuestas ofrecidas y sistemas automatizados de recomendación

Proteger la salud, el bienestar y el medio ambiente

Por otra parte, aun manteniendo una perspectiva tecnológica de la seguridad, el uso de los entornos digitales puede tener consecuencias no solo en los dispositivos, los datos o la privacidad, sino en aspectos vitales como la protección de la salud o el bienestar. Así, el *DIGCOMP2.2*, en su ámbito "Seguridad en la Red" (D) también hace referencia a competencias específicas que permitan a las personas evitar riesgos y amenazas para la salud física y mental en el uso de tecnologías digitales, protegerse e identificar las que fomenten nuestro bienestar y la inclusión social.

Una amplia encuesta de la *Royal Society for Public Health* (2017) de Reino Unido analizó cómo sentían los jóvenes que afectaba a su salud y bienestar (tanto positiva como negativamente) cada una de las plataformas sociales que usaban, concluyendo que éstas influían sustancialmente en:

- la conciencia y comprensión de las experiencias de salud de otras personas;
- el acceso a información de salud experta en la que se puede confiar;
- el apoyo emocional;
- el grado de ansiedad y en la depresión;
- los sentimientos de soledad;
- el sueño;
- la capacidad de autoexpresión de sentimientos o pensamientos;
- la elaboración de la propia identidad;
- la imagen corporal;
- el mantenimiento de relaciones en el mundo real;
- la construcción de comunidad;
- las situaciones de intimidación y en sensaciones *FoMO* (miedo a perderse algo).

Por su parte, la *Fundación Mapfre* (2021) alerta de un amplio número de aspectos en los que la aceleración digital está impactando negativamente sobre la vida de las personas:

- el físico: cansancio visual, sedentarismo, problemas posturales…;
- el social: pérdida de contacto físico con los demás;
- el psicológico: con conductas como la hiperconexión, la dependencia digital o hábitos de consumo compulsivo.

En concreto, la hiperconexión, el tecnoestrés y otros usos abusivos de la tecnología se vinculan a síntomas como la fatiga visual (astenopatía), fatiga neurovisual, trastornos neuromusculoesqueléticos –tórax, extremidades superiores y cervical–, problemas dérmicos, cuadros psicosomáticos o la obesidad. Son conductas que pueden acabar desencadenando trastornos del sueño (insomnio), cambios en el metabolismo (aumento o pérdida de peso, dolores de espalda, de cabeza), trastornos psicológicos (baja autoestima), ruptura de relaciones sociales, pérdida de concentración y pérdida de productividad, depresión mayor, fobia social, agorafobia, o déficit de atención con hiperactividad (**Hernández-Pérez**, 2019).

La preocupación por estos riesgos se está reflejando en distintas iniciativas legislativas españolas como, por ejemplo, la regulación del derecho a la desconexión digital en el ámbito laboral. El artículo 88 de la *Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales* (*España*, 2018) indica que las personas trabajadoras y empleadas públicas tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar. Y de igual manera el *Real Decreto Ley 28/2020, de trabajo a distancia* (*España*, 2020) insiste en sus artículos 16 y 18 en la necesidad de garantizar los tiempos de descanso y de desconexión.

Atendiendo otros aspectos que los riesgos tecnológicos pueden tener sobre la salud, **Cotter** (2019) afirma que en la actualidad preferimos escuchar la voz de otras personas frente a comunicaciones oficiales o comerciales. Esta situación otorga a determinados referentes de canales digitales (por ejemplo, los *influencers*) una voz no contrastada que puede fomentar prácticas dañinas para la salud, tanto personal como pública, hasta tal punto que algunas entidades gubernamentales se han puesto a trabajar de manera coordinada con grandes tecnológicas como *Google* y otros medios sociales para evitar estas prácticas (**Linde**, 2020).

Por último, el ámbito competencial "Seguridad en la Red" hace referencia a la necesidad de reconocer el impacto que la propia tecnología –y el tipo de uso que hacemos de ella– tiene en el medio ambiente. La tecnología está transformando las organizaciones, los procesos de producción, la vida diaria de las personas y, en consecuencia, nuestro propio entorno. El uso intensivo de las tecnologías consume recursos ingentes de energía que, a fecha de hoy, no podrían ser generados con energías renovables. Comprender las implicaciones de ello es fundamental para hacer frente a los desafíos del cambio climático, pues puede impactar en mayor o menor medida en todos los sectores y servicios –alimentario, productivo, industria, edificación, transporte o logística– y este impacto puede ser positivo, pero también negativo (**Andreu-Pinillos**; **Fernández-Mateos**, 2019).

Además, se debe tener en cuenta que la globalización, de la mano del entorno digital, también se caracteriza por incitar a un consumo desmedido donde se persigue satisfacer necesidades y deseos de manera inmediata (**Gómez-Nieto**, 2018). En este contexto la integración de determinados principios –como la sostenibilidad, la economía circular, el consumo saludable y ético o el respeto al medio ambiente– por parte de la ciudadanía es la clave de conductas autónomas que permitan racionalizar el uso y consumo de los recursos (**Andreu-Pinillos**; **Fernández-Fernández**; **Fernández Mateos**, 2019). Por ejemplo, **Bonet** (2021) alerta sobre la plataforma de *e-commerce Shein* que, a través de las redes

Tabla 6. Riesgos relativos a salud, bienestar y medio ambiente

D. Seguridad en la Red y E. Resolución de problemas (segunda parte): Riesgos relativos a salud, bienestar y medio ambiente			
Competencias específicas	**Derechos digitales**	**Amenazas digitales**	**Riesgos sociales**
D.3. Proteger la salud y el bienestar. D.4. Proteger el medio ambiente.	CDD5. Derechos digitales en entornos específicos. CDD5.2. Derecho a un desarrollo tecnológico y a un entorno digital sostenible. CDD5.3. Derecho a la protección de la salud en el entorno digital.	Hiperconexión. Tecnoestrés. Incapacidad de concentración, tendencia a la multitarea y abandono de tareas antes de su finalización. Incapacidad de llevar una vida consciente y orientada al futuro. Sedentarismo, obesidad o problemas visuales y motores. Fomento de hábitos de alimentación y cuidados de la salud inadecuados. Perdida de contacto con otras personas. Fomento de hábitos de consumo inadecuados y compulsivos (consumismo). Dependencia tecnológica y uso excesivo de las TIC Falta de conciencia social y ambiental.	Problemas de salud pública. Empeoramiento de las condiciones de vida y el bienestar (salud física y psicológica). Pérdida de productividad laboral o educativa. Incremento de adicciones digitales. Incremento de enfermedades como la ludopatía y la oniomanía. Incumplimiento de los objetivos de desarrollo sostenible. Calentamiento global y daños al medioambiente.

sociales y la utilización masiva de *influencers*, está fomentando hábitos de consumo compulsivo entre los más jóvenes, consiguiendo un éxito sin precedentes. La amplia demanda y el ritmo de producción que requiere pone en cuestión su estrategia de sostenibilidad suscitando serias dudas sobre los estándares de calidad de sus productos, la procedencia de las materias primas y las condiciones de sus trabajadores. A pesar de ello, la empresa, que solo vende sus prendas a través de Internet, ha conseguido convertirse en la aplicación de compras más descargada en 50 países y acumula ya casi un tercio de las ventas totales de ropa en Estados Unidos, superando la suma de los grupos *H&M* (17%) e *Inditex* (10%).

Estos aspectos pueden afectar a los ODS, como al 3º, *referido* a "Salud y bienestar" que pretende garantizar una vida sana y promover el bienestar para todas las personas, al 12º, relativo a "Producción y consumo responsable" o al 13º: "Adoptar medidas urgentes para combatir el cambio climático y sus efectos" (*Naciones Unidas*, 2015), limitando principios fundamentales señalados en la *Carta de Derechos Digitales*, como el derecho a la protección de la salud en el entorno digital o el derecho a un desarrollo tecnológico y entorno digital sostenible.

5. Reflexiones finales

Exclusión digital, infodemia, desinformación, adicciones digitales, hiperconexión, ciberacoso, suplantación de identidad, abusos de la privacidad, robo y perdida de datos, *phishing o pharming…* conforman una larga lista de amenazas digitales que crece cada día y que puede poner en riesgo pilares fundamentales de nuestra sociedad como el acceso a derechos, la convivencia, la cohesión social y, en definitiva, la propia democracia.

Identificar y clasificar los riesgos digitales es una tarea necesaria, pues permitiría desarrollar programas de capacitación y empoderamiento digital de una forma sistemática o global; pero es un reto complejo pues:

- involucra muy diversos aspectos que se interrelacionan –personales, sociales, educativos o económicos;
- la competencia digital es muy amplia, evolutiva, gradual y contextual, determinando las carencias que podemos tener, los diversos riesgos a los que nos enfrentamos y en qué grado nos puede afectar.

En nuestro caso, partiendo del *DIGCOMP2.2* y de la *Carta de derechos digitales*, hemos intentado ordenar y establecer relaciones temáticas entre derechos, competencias y algunos de los principales problemas sociales derivados del uso inadecuado de la tecnología. Somos conscientes de que los factores que influyen en la vulnerabilidad de las personas van más allá de la mera exclusión digital o la falta de competencias digitales, pero ésta tiene un carácter transversal que incrementa otros muchos factores de vulnerabilidad de las personas.

La evaluación y categorización de los riesgos digitales debe ir acompañada de un vademécum de metodologías, herramientas y recursos educativos específicos que se pueda utilizar para involucrar a las personas en las estrategias frente a tales riesgos, que puedan aplicarse de forma adaptada tanto en espacios de aprendizaje formales como informales. Ya hay una infinidad de propuestas en sitios web educativos de todo tipo de organizaciones, y tenemos que conseguir integrarlas para su usabilidad; una propuesta que nos parece que va en esa línea es la del *Berkman Klein Center for Internet & Society* de la *Harvard University*, que en su informe *Youth and digital citizenship+ (Plus)* describe 17 áreas vitales para esa ciudadanía digital con ejemplos de recursos educativos que se pueden presentar de manera atractiva (**Cortesi** *et al.*, 2020).

En todo caso, estamos obligados a actuar desde nuestros ámbitos educativos, bibliotecarios y de inclusión social para que las personas tengan en las tecnologías digitales un factor de desarrollo equilibrado y crítico; personas conscientes de sus riesgos y capaces de autorregularse de forma relevante y socialmente solidaria. La educación digital en todas las etapas de la vida es un derecho y una fuente a su vez de derechos y oportunidades. Su ausencia es un factor de exclusión personal y social.

6. Referencias

Aguaded, Ignacio (2014). "Desde la infoxicación al derecho a la Comunicación". *Comunicar*, v. 21, n. 42. *https://doi.org/10.3916/C42-2014-a1*

Agudo-Díaz, Ujué (2021). *La influencia de los algoritmos en las decisiones y juicios humanos. Experimentos en contextos de política, citas y arte.* Tesis doctoral. Facultad de Psicología. Universidad de Deusto. *https://dialnet.unirioja.es/servlet/tesis?codigo=301995*

Álvarez–Sigüenza, Juan-Francisco (2019). "Nativos digitales y brecha digital: una visión comparativa en el uso de las TIC". *Revista de la Asociación Española de Investigación de la Comunicación*, v. 6, n. 11, pp. 203-223. *https://doi.org/10.24137/raeic.6.11.12*

Andreu-Pinillos, Alberto; **Fernández-Mateos, Joaquín** (2019). "La ambivalencia tecnológica para impulsar (¿o no?) los ODS. Los ODS y las nuevas tecnologías". *Telos*, 17 septiembre. *https://telos.fundaciontelefonica.com/ambivalencia-tecnologica-para-impulsar-ods-onu/*

Andreu-Pinillos, Alberto; **Fernández-Fernández, José-Luis**; **Fernández-Mateos, Joaquín** (2019). "Pasado, presente y futuro de los objetivos del desarrollo sostenible (ODS). La tecnología como catalizador (o inhibidor) de la Agenda 2030". *Icade. Revista de la Facultad de Derecho*, n. 108.
https://doi.org/10.14422/icade.i108.y2019.001

Bonet, Inma (2021). "Shein: la voracidad del enigmático grupo textil chino que le está comiendo terreno a *Zara*". *El País*, 9 mayo.
https://elpais.com/economia/negocios/2022-05-21/shein-la-voracidad-del-enigmatico-grupo-textil-chino-que-le-esta-comiendo-terreno-a-zara.html

Bustos-Martínez, Laura; **De-Santiago-Ortega, Pedro-Pablo**; **Martínez-Miró, Miguel-Ángel**; **Rengifo-Hidalgo, Miriam-Sofía** (2019). "Discursos de odio: una epidemia que se propaga en la Red. Estado de la cuestión sobre el racismo y la xenofobia en las redes sociales". *Mediaciones sociales*, v. 18, pp. 25-42.
https://doi.org/10.5209/meso.64527

Cabero-Almenara, Julio; **Ruiz-Palmero, Julio** (2017). "Las Tecnologías de la Información y Comunicación para la inclusión: reformulando la brecha digital". *Ijeri: International journal of educational research and innovation*, v. 9, pp. 16–30.
https://www.upo.es/revistas/index.php/IJERI/article/view/2665

Calderón-Gómez, Daniel; **Gómez-Miguel, Alejandro** (2022). *Consumir, crear, jugar. Panorámica del ocio digital de la juventud*. Madrid: Centro Reina Sofía sobre Adolescencia y Juventud, Fundación FAD Juventud.
https://www.adolescenciayjuventud.org/publicacion/investigacion_ocio_digital

Cañón-Rodríguez, Ruth; **Grande-de-Prado, Mario**; **Cantón-Mayo, Isabel** (2016). "Brecha digital: impacto en el desarrollo social y personal. Factores asociados". *Tendencias pedagógicas*, v. 28.
https://doi.org/10.15366/tp2016.28.009

Comisión Europea (2019). *Una nueva agenda estratégica 2019-2024.*
https://www.consilium.europa.eu/media/39964/a-new-strategic-agenda-2019-2024-es.pdf

Comisión Europea (2020). *Digital education action Plan 2021-2027: Resetting education and training for the digital age.*
https://education.ec.europa.eu/focus-topics/digital-education/action-plan

Consejo Europeo (2018). "Recomendación del Consejo de 22 de mayo de 2018, relativa a las competencias clave para el aprendizaje permanente". *Diario oficial de la Unión Europea*, 4 junio.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018H0604(01)&from=SV

Coonan, Emma; **Geekie, Jacqueline**; **Goldstein, Stéphane**; **Jeskins, Lisa**; **Jones, Rosie**; **Macrae-Gibson, Rowena**; **Secker, Jane**; **Walton, Geoff** (2018). *Cilip definition of information literacy 2018.* Cilip Information Literacy Group, 2018-04.
https://infolit.org.uk/ILdefinitionCILIP2018.pdf

Cortesi, Sandra; **Hasse, Alexa**; **Lombana-Bermúdez, Andrés**; **Kim, Sonia**; **Gasser, Urs** (2020). *Youth and digital citizenship+ (plus): Understanding skills for a digital world.* Youth and Media, Berkman Klein Center for Internet & Society. Universidad de Harvard.
https://cyber.harvard.edu/publication/2020/youth-and-digital-citizenship-plus

Cotter, Kelley (2019). "Playing the visibility game: How digital influencers and algorithms negotiate influence on *Instagram*". *New media & Society*, v. 21, n. 4, pp. 895-913.
https://doi.org/10.1177/1461444818815684

EAPN España (2021). *La brecha digital en la juventud vulnerable. Evaluación de las medidas adoptadas durante la COVID-19.* European Anti-Poverty Network (EAPN).
https://www.eapn.es/ARCHIVO/documentos/documentos/1640621700_eapn_estudio-brecha-digital-en-la-juventud-vulnerable_v4.pdf

Eppler, Martin J.; **Mengis, Jeanne** *(2010).* "The concept of information overload: A review of literature from organization science, accounting, marketing, MIS and related disciplines". *The information society*, v. 20, n. 5, pp. 325–344.
https://doi.org/10.1080/01972240490507974

España (2018). "Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales". *BOE*, n. 294, 6 diciembre.
https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

España (2020). "Real decreto ley 28/2020, de 22 de septiembre, de trabajo a distancia". *BOE*, n. 253, 23 septiembre.
https://www.boe.es/buscar/act.php?id=BOE-A-2020-11043

Fundación Mapfre (2021). *Salud y nuevos hábitos digitales.*
https://www.fundacionmapfre.org/media/publicaciones/destacadas/salud/informe-completo-salud-digital.pdf

Fundación Telefónica (2021). *Sociedad Digital en España: el año en que todo cambió.*
https://www.fundaciontelefonica.com/cultura-digital/publicaciones/sociedad-digital-en-espana-2020-2021/730/

Gobierno de España (2020). *Plan España Digital 2025: conectándonos al futuro.*
https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/230720-Espa%C3%B1aDigital_2025.pdf

Gobierno de España (2021a). *Carta de derechos digitales. Plan de Recuperación, Transformación y Resiliencia.*
https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

Gobierno de España (2021b). *Plan nacional de competencias digitales.*
https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2021/210127_np_digital.pdf

Gómez-Hernández, José-Antonio; **Fernández-Rincón, Antonio-Raúl** (2020). "La sátira gráfica de Calpurnio y El Roto sobre la digitalización social: Un análisis crítico desde la perspectiva de las competencias digitales". *Informação & sociedade: Estudos*, v. 30, n. 4.
https://doi.org/10.22478/ufpb.1809-4783.2020v30n4.57792

Gómez-Hernández, José-Antonio; **Vera-Baceta, Miguel-Ángel** (2021). "Las bibliotecas públicas españolas ante los fondos europeos de recuperación y el *Plan nacional de competencias digitales*". *Anuario ThinkEPI*, v. 15, e15b01.
https://doi.org/10.3145/thinkepi.2021.e15b01

Gómez-Nieto, Begoña (2018). "El influencer: herramienta clave en el contexto digital de la publicidad engañosa". *Methaodos*, v. 6, n. 1, pp. 149-156.
https://doi.org/10.17502/m.rcs.v6i1.212

Hernández-Pérez, Francisco (2019). "Los riesgos de las tecnologías de la información y la comunicación". *Revista Conamed*, v. 24, n. 4, pp. 184-199.
https://www.medigraphic.com/cgi-bin/new/resumen.cgi?IDARTICULO=90243

INE (2021a). *Encuesta de Condiciones de Vida. Año 2020.* Instituto Nacional de Estadística.
https://www.ine.es/prensa/ecv_2020.pdf

INE (2021b). *Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares. Año 2021. Instituto Nacional de Estadística.*
https://www.ine.es/prensa/tich_2021.pdf

ICCL (2022). *The biggest data breach. Irish Council for Civil Liberties.*
https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf

Llaneza, Paloma (2019) *Datanomics*. Ediciones Deusto. ISBN: 978 8423430208

Linde, Pablo (2020). "'Influencers' nocivas para la salud". *El País*, 9 enero.
https://elpais.com/sociedad/2020/01/08/actualidad/1578509328_514133.html

Marwick, Alice; Lewis, Rebecca (2017). *Media manipulation and disinformation online*. Data & Society Research Institute.
http://www.chinhnghia.com/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf

Marta-Lazo, Carmen; **Gabelas-Barroso, José-Antonio**; **Marfil-Carmona, Rafael** (2019). "El factor relacional y el ecosistema 3.0: nuevas conectividades, nuevas saturaciones". En: Romero-Rodríguez, Luis-Miguel; Rivera-Rogel, Diana-Elizabeth (coords.). *La comunicación en el escenario digital. Actualidad, retos y prospectivas*. Pearson, pp. 535-569. ISBN: 978 607 32 4859 4
https://digibug.ugr.es/handle/10481/61272

Mihelj, Sabina; **Leguina, Adrian**; **Downey, John** (2019). "Culture is digital: Cultural participation, diversity and the digital divide". *New media & society*, v. 21, n. 7, pp. 1465-1485.
https://doi.org/10.1177/1461444818822816

Naciones Unidas (2019). *The age of digital interdependence: report of the UN Secretary-General's High-Level Panel on Digital Cooperation.*
https://digitallibrary.un.org/record/3865925

Naciones Unidas (2015). *Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible.*
https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=S

Navarro, Gabriel 2013). "Un matiz sobre jóvenes y brecha digital". *Gabriel Navarro*, 9 enero.
http://www.gabrielnavarro.es/2013/01/09/un-matiz-sobre-jovenes-y-brecha-digital

OCDE (2021). *21st-Century readers: Developing literacy skills in a digital world*. Paris: OECD.
https://www.oecd.org/publications/21st-century-readers-a83d84cb-en.htm

ONTSI (2021a). *Competencias digitales de los internautas. Análisis de datos INE 2020*. Observatorio Nacional de Tecnología y Sociedad, ONTSI.
http://www.ontsi.es/sites/ontsi/files/2021-10/competenciasdigitalesinternautas2020.pdf

ONTSI (2021b). *Indicadores sobre confianza digital y ciberseguridad en España y la Unión Europea. Octubre 2021.* Observatorio Nacional de Tecnología y Sociedad, ONTSI.
https://n9.cl/q6e7j

ONTSI (2021c). *Cómo se protege la ciudadanía ante los ciberriesgos: estudio sobre percepción y nivel de confianza en España. Edición diciembre 2021.* Observatorio Nacional de Tecnología y Sociedad, ONTSI.
https://www.observaciber.es/sites/observaciber/files/media/documents/ciberriesgos_informe_diciembre2021.pdf

Rial-Boubeta, Antonio; **Gómez-Salgado, Patricia**; **Isorna-Folgar, Manuel**; **Araujo-Gallego, Manuel**; **Valera-Mallou, Jesús** (2015). "EUPI-a: Escala de uso problemático de Internet en adolescentes. Desarrollo y validación psicométrica". *Adicciones*, v. 27, n. 1, pp. 47-63.
https://www.adicciones.es/index.php/adicciones/article/view/193/0

Rodicio-García, María-Luisa; Ríos-de-Deus, María-Paula; Mosquera-González, María-José; Penado-Abilleira, María (2020). "La brecha digital en estudiantes españoles ante la crisis de la Covid-19". *Revista internacional de educación para la justicia social*, v. 9, n. 3, pp. 103-125.
https://doi.org/10.15366/riejs2020.9.3.006

Roetzel, Peter-Gordon (2019). "Information overload in the information age: a review of the literature from business administration, business psychology, and related disciplines with a bibliometric approach and framework development". *Business research*, v. 12, n. 2, pp. 479-522.
https://doi.org/10.1007/s40685-018-0069-z

Roozenbeek, Jon; **Schneider, Claudia R.**; **Dryhurst, Sarah**; **Kerr, John**; **Freeman, Alexandra L. J.**; **Recchia, Gabriel**; **Van-Der-Bles, A. M.**; **Van-Der-Linden, S.** (2020). "Susceptibility to misinformation about Covid-19 around the world. *Royal Society open science*, v. 7, n. 10, 201199.
https://doi.org/10.6084/m9.figshare.c.5170488

Royal Society for Public Health (2017). *#StatusOfMind Social media and young people's mental health and wellbeing*. RSPH-YHM Social Media & Mental Health Report 2017.
https://www.rsph.org.uk/our-work/campaigns/status-of-mind.html

Sá, María-José; **Santos, Ana-Isabel**; **Serpa, Sandro**; **Ferreira, Carlos-Miguel** (2021). "Digitainability—Digital Competences Post-COVID-19 for a sustainable society". *Sustainability*, v. 13, 9564.
https://doi.org/10.3390/su13179564

Salaverría, Ramón; **Buslón, Nataly**; **López-Pan, Fernando**; **León, Bienvenido**; **López-Goñi, Ignacio**; **Erviti, María-Carmen** (2020*).* "Desinformación en tiempos de pandemia: tipología de los bulos sobre la Covid-19". *Profesional de la información*, v. 29, n. 3, e290315.
https://doi.org/10.3145/epi.2020.may.15

Seetharaman, Deepa (2021). "Instagram boss to testify in congress on child safety issues". *Wall Street Journal*, 24 November.
https://www.wsj.com/articles/instagram-boss-to-testify-in-congress-on-child-safety-issues-11637783654

Sevillano, E. G. (2022). "Gobiernos de todo el mundo han ordenado rastreos internos por la amenaza de Pegasus". *El País*, 2 mayo.
https://elpais.com/internacional/2022-05-02/gobiernos-de-todo-el-mundo-han-ordenado-rastreos-internos-por-la-amenaza-de-pegasus.html

Sulbarán-Lobera, Patricia (2021). "Asalto al Capitolio". *BBC News*, 7 enero.
https://www.bbc.com/mundo/noticias-internacional-55568588

Tidy, Joe (2022). "Rusia y Ucrania: los 3 ciberataques rusos que más teme Occidente". *BBC News*, 24 marzo.
https://www.bbc.com/mundo/noticias-60850173

Unesco (2020). *Combatiendo la desinfodemia: trabajando por la verdad en la época del COVID-19.*
https://es.unesco.org/covid19/disinfodemic

Unicef (2021). *Impacto de la tecnología en la adolescencia: relaciones, riesgos y oportunidades*.
https://www.unicef.es/publicacion/impacto-de-la-tecnologia-en-la-adolescencia

Unión Europea (2007). "Tratado de Lisboa". *Revista de las Cortes Generales*, n. 70-72, pp. 703-1166.
https://doi.org/10.33426/rcg/2007/70-72/1337

Van-Dijk, Jan A. G. M. (2017). "Digital divide: Impact of access". *The international encyclopedia of media effects*, 8 March.
https://doi.org/10.1002/9781118783764.wbieme0043

Van-Dijk, Jan A. G. M. (2020). *The digital divide.* Polity Press. ISBN: 978 1509534456

Vera-Baceta, Miguel-Ángel; **Gómez-Hernández, José-Antonio** (2021). "Espacios de ciudadanía digital en las bibliotecas públicas: una propuesta para su integración en el marco del Plan nacional de competencias digitales". *Anuario ThinkEPI*, n. 15, e15b02.
https://doi.org/10.3145/thinkepi.2021.e15b02

Vuorikari, Rina; **Kluzer, Stefano**; **Punie, Yves** (2022). *DigComp 2.2: The digital competence framework for citizens. With new examples of knowledge, skills and attitudes*. Publications Office of the European Union.
https://doi.org/10.2760/490274

Yam, Josephine; **Skorburg, Joshua-August** (2021). "From human resources to human rights: Impact assessments for hiring algorithms". *Ethics and information technology*, n. 23, pp. 611–623.
https://doi.org/10.1007/s10676-021-09599-7