

Chapter 6 / Capítulo 6



The Surnames of Education
ISBN: 978-9915-9928-4-6
DOI: 10.62486/978-9915-9928-4-6.Ch06
Pages: 170-200

© 2026 The authors. This is an open access
book chapter distributed under the terms of
the Creative Commons Attribution (CC BY)
4.0 License.

Digital Education: Autonomy, Judgment and Citizenship in Connected Societies

Educación digital: Autonomía, criterio y ciudadanía en sociedades conectadas

Jerson Ortega Bonfante ¹  

Naun Oseas Onofre Mendoza ²  

Glenda Yamileth Trejo Magaña ³  

¹ Escuela Superior de Administración Pública. Cúcuta, Colombia.

² Universidad Politécnica de El Salvador. San Salvador, El Salvador.

³ Universidad de Sonsonate. San Salvador, El Salvador.

ABSTRACT

Digital education cannot be reduced to access to devices or the instrumental mastery of applications. This chapter examines digital autonomy as the capacity to search, verify, understand, create, participate, and decide within ecosystems mediated by platforms, data, and algorithms. It analyzes the digital divide beyond connectivity by incorporating quality of access, competencies, technological governance, and realistic possibilities for choosing or leaving a service. Information search and evaluation are addressed through criteria of provenance, evidence, currency, and cross-checking, with particular attention to misinformation and biases that favor content consistent with prior beliefs. The chapter also studies the attention economy, recommendation systems, and personalization, showing that platforms are not neutral channels and that their design can shape visibility, time, and behavior. Digital identity, privacy, security, and data protection are examined through individual and institutional risks, including incidents such as Equifax and WannaCry. Creation, participation, authorship, and online coexistence are also considered, together with challenges introduced by generative artificial intelligence. The pedagogical proposal avoids organizing digital education as a list of tools and instead prioritizes transferable capacities: formulating searches, verifying claims, managing permissions, recognizing incentives, documenting sources, and regulating one's own use. Overall, the chapter argues that digital literacy means governing one's participation within systems that also attempt to govern attention, data, and decisions. Digital competence therefore combines technical action with critical judgment, responsibility, and the practical ability to preserve autonomy in connected environments. Digital autonomy does not mean fully controlling the technological environment, but having sufficient criteria and alternatives to act intentionally and responsibly.

Keywords: digital education; digital literacy; platforms; privacy; autonomy

RESUMEN

La educación digital no puede reducirse al acceso a dispositivos ni al dominio instrumental de aplicaciones. Este capítulo examina la autonomía digital como capacidad para buscar, verificar, comprender, crear, participar y decidir dentro de ecosistemas mediados por plataformas, datos y algoritmos. Se analiza la brecha digital más allá de la conectividad, incorporando calidad de acceso, competencias, gobernanza tecnológica y posibilidades reales de elegir o abandonar un servicio. La búsqueda y evaluación de información se abordan mediante criterios de procedencia, evidencia, actualidad y contraste entre fuentes, con especial atención a la desinformación y a los sesgos que favorecen contenidos compatibles con creencias previas. El capítulo estudia además la economía de la atención, los sistemas de recomendación y la personalización, mostrando que las plataformas no son canales neutrales y que su diseño puede orientar visibilidad, tiempo y comportamiento. La identidad digital, la privacidad, la seguridad y la protección de datos se analizan mediante riesgos individuales e institucionales, incluidos incidentes como Equifax y WannaCry. También se consideran la creación, la participación, la autoría y la convivencia en línea, junto con los desafíos introducidos por la inteligencia artificial generativa. La propuesta pedagógica evita organizar la educación digital como una lista de herramientas y prioriza capacidades transferibles: formular búsquedas, verificar afirmaciones, gestionar permisos, reconocer incentivos, documentar fuentes y regular el propio uso. En conjunto, se sostiene que alfabetizar digitalmente significa gobernar la propia participación dentro de sistemas que también intentan gobernar la atención, los datos y las decisiones. La autonomía digital no supone controlar por completo el entorno tecnológico, sino disponer de criterios y alternativas suficientes para actuar con intención y responsabilidad.

Palabras clave: educación digital; alfabetización digital; plataformas; privacidad; autonomía

INTRODUCCIÓN

ESTAR CONECTADO NO SIGNIFICA ESTAR ALFABETIZADO

La vida digital se ha vuelto tan cotidiana que muchas de sus decisiones parecen naturales. Se acepta una política de privacidad sin leerla, se comparte una noticia porque coincide con una intuición, se pulsa una notificación antes de terminar una tarea, se instala una aplicación que solicita permisos excesivos o se produce un texto con una herramienta generativa sin verificar de dónde proviene la información. La familiaridad con dispositivos puede crear una ilusión de dominio. Sin embargo, usar con soltura una interfaz no equivale a comprender los sistemas que organizan la experiencia digital ni a gobernar el propio uso.

Esta diferencia entre uso y autonomía constituye el punto de partida del capítulo. El marco DigComp 2.2 organiza la competencia digital alrededor de información y datos, comunicación y colaboración, creación de contenidos, seguridad y resolución de problemas (Vuorikari et al., 2022). Su valor está en desplazar la atención desde el dispositivo hacia capacidades transferibles. Aprender dónde se encuentra una función concreta puede ser útil durante meses; aprender a evaluar una fuente, proteger una cuenta, comprender una recomendación automática o decidir qué información compartir conserva valor cuando cambia la plataforma.

La historia reciente de la educación tecnológica muestra por qué este desplazamiento era necesario. Durante años, muchas políticas midieron avance por número de computadores, conectividad o licencias. Estas condiciones son indispensables, pero no suficientes. La OECD (2023a) insiste en que los ecosistemas de educación digital combinan infraestructura, herramientas, gobernanza y competencias humanas. El Informe GEM 2023 de UNESCO formula una pregunta aún más incisiva: la tecnología en educación debe evaluarse por pertinencia, equidad, escalabilidad y sostenibilidad, y no por novedad. El acceso tecnológico puede ampliar oportunidades y también reproducir desigualdades cuando conectividad, dispositivos, apoyo docente o calidad de recursos están distribuidos de manera desigual.

La brecha digital, por ello, ha cambiado de forma. Van Dijk (2020) distingue acceso motivacional, material, de habilidades y de uso; Helsper (2021) muestra cómo las desigualdades digitales se entrelazan con desigualdades sociales. Una persona puede tener teléfono y datos móviles y, aun así, disponer de una experiencia digital limitada por pantalla pequeña, conexión inestable o escaso repertorio informacional. Otra puede contar con equipos y carecer de criterios para reconocer fraude o manipulación. La pregunta educativa deja de ser quién está conectado y pasa a ser qué puede hacer una persona con esa conexión, bajo qué condiciones y con qué riesgos.

Las plataformas añaden otra complejidad porque no son espacios neutrales. Organizan visibilidad, atención, interacción y datos mediante reglas de diseño y sistemas de recomendación. Gillespie (2018) estudia la moderación como parte de la gobernanza de plataformas; Zuboff (2019) analiza modelos de negocio basados en extracción y predicción de conducta; boyd (2014) muestra cómo los jóvenes negocian identidad, privacidad y públicos en entornos conectados. Estas perspectivas no deben confundirse con un único diagnóstico. Coinciden, sin embargo, en que la vida digital está mediada por arquitecturas que influyen en lo que vemos y hacemos.

La desinformación ha convertido la evaluación de fuentes en competencia cívica. McGrew et al. (2018) y Breakstone et al. (2021) muestran dificultades de estudiantes para juzgar información en línea; McGrew (2020) demuestra que estrategias explícitas como la lectura lateral pueden mejorar esa capacidad. La alfabetización digital deja así de ser una versión moderna de ofimática y se transforma en disciplina del juicio: salir de una página, investigar quién está detrás, comparar fuentes y rastrear una afirmación hasta su origen.

La seguridad introduce una responsabilidad compartida. Casos como WannaCry muestran que un ataque informático no es únicamente resultado de usuarios descuidados: depende de actualizaciones, sistemas heredados, gobernanza y preparación institucional. El National Audit Office británico documentó que el ataque de 2017 afectó de manera amplia al NHS y encontró sistemas sin parches o sin soporte, pese a advertencias previas. La educación digital necesita enseñar hábitos de seguridad y, al mismo tiempo, evitar trasladar toda la carga al usuario.

Algo semejante ocurre con privacidad. El incidente de Equifax de 2017 expuso información personal de aproximadamente 147 millones de personas, según la FTC, y dio lugar a un acuerdo global de cientos de millones de dólares. La lección educativa no es simplemente “use una contraseña fuerte”: el ciudadano no puede controlar completamente cómo una gran organización almacena sus datos. La alfabetización digital debe incorporar derechos, minimización, monitoreo y responsabilidad institucional.

La inteligencia artificial aparece en el capítulo 6 como una extensión del problema de

autonomía digital. El capítulo 11 examina con mayor profundidad sus capacidades, límites, ética y pedagogía. Los sistemas generativos intensifican competencias ya necesarias: verificar, atribuir, proteger datos, reconocer automatización y conservar responsabilidad sobre el juicio. Almatrafi et al. (2024) y UNESCO (2024a) sitúan comprensión, evaluación, creación y ética dentro de la alfabetización en IA. Estas capacidades complementan la educación digital y requieren un tratamiento específico.

El capítulo 6 se organiza en seis acápite. El 6.1 analiza acceso, brechas y autonomía. El 6.2 desarrolla búsqueda, verificación y comprensión de argumentos. El 6.3 estudia plataformas, atención y personalización. El 6.4 aborda identidad, privacidad y seguridad mediante Equifax y WannaCry. El 6.5 relaciona creación, participación, convivencia y bienestar. El 6.6 propone problemas transferibles, criterios de gobernanza y una aplicación ilustrativa de selección tecnológica. El recorrido busca conservar capacidad de juicio dentro de ecosistemas que cambian y que también influyen en nuestras decisiones.

6.1. DE LA BRECHA DE ACCESO A LA AUTONOMÍA DIGITAL

Conectividad, habilidades, desigualdad y capacidad de elección

La primera desigualdad digital fue no poder conectarse. La siguiente consiste en estar conectado y no poder convertir esa conexión en aprendizaje, participación o protección.

LA BRECHA DIGITAL NO TERMINA CUANDO APARECE UNA SEÑAL DE INTERNET

Las primeras discusiones sobre brecha digital se concentraron en disponibilidad de computadores e internet. Esa dimensión continúa siendo relevante, especialmente en territorios rurales o hogares con recursos limitados, pero resulta insuficiente. Warschauer (2004) mostró que el acceso significativo depende de recursos físicos, contenidos, habilidades y apoyo social. Van Dijk (2020) desarrolla una secuencia donde motivación, acceso material, habilidades y usos se condicionan mutuamente. La conectividad es puerta de entrada, no resultado final.

Esta diferencia fue visible durante la pandemia. Millones de estudiantes pudieron considerarse “conectados” porque tenían un teléfono, pero estudiar desde un dispositivo compartido con datos limitados no era equivalente a disponer de computador, banda ancha y espacio. El GEM Report 2023 de UNESCO subraya que la tecnología puede ampliar acceso y también reforzar desigualdad cuando las condiciones de uso no son equivalentes. La infraestructura necesita interpretarse junto con calidad, costo y continuidad.

Helsper (2021) propone pensar las desigualdades digitales como traducciones de desigualdades sociales. Ingreso, educación, género, edad, discapacidad y territorio influyen en acceso y capacidad de obtener beneficios. El entorno digital puede amplificar ventajas previas porque quienes poseen mayor capital educativo utilizan herramientas para aprender, comparar y producir, mientras otros quedan concentrados en usos de consumo o comunicación. Esta relación no es determinista, pero ayuda a comprender por qué repartir dispositivos no iguala automáticamente resultados.

La autonomía digital requiere, por tanto, repertorio. Una persona que solo conoce una plataforma depende de sus reglas; quien sabe transferir tareas entre herramientas puede elegir. La competencia se manifiesta cuando el usuario distingue qué aplicación conviene, qué datos solicita, qué alternativa existe y qué hacer si el servicio desaparece. Esta flexibilidad es más estable que la instrucción centrada en marcas.

El diseño universal y la accesibilidad añaden otra dimensión. Un recurso puede ser técnicamente disponible y excluir por contraste, navegación, subtítulos o compatibilidad con lectores de pantalla. La accesibilidad no es un complemento posterior; define quién puede participar. La educación digital debe incluir al menos una comprensión básica de que crear contenido implica pensar en usuarios con necesidades distintas.

La calidad del acceso también depende de idioma y pertinencia. Una conexión rápida ofrece poco si la información relevante no está disponible en una lengua comprensible o si los contenidos no responden al contexto. La digitalización puede abrir bibliotecas globales y, al mismo tiempo, concentrar producción en pocos idiomas y plataformas. La alfabetización necesita enseñar a buscar más allá de los resultados más visibles.

La brecha digital termina siendo una pregunta sobre capacidad efectiva. No basta con preguntar quién tiene internet. Conviene preguntar quién puede aprender, trabajar, crear,

reclamar, protegerse y participar mediante ese acceso. Esa formulación desplaza la política desde conteo de dispositivos hacia ecosistemas de oportunidades.

COMPETENCIA DIGITAL: SABER HACER, SABER ELEGIR Y SABER DETENERSE

DigComp 2.2 organiza veintiuna competencias en cinco áreas y propone niveles de dominio. La arquitectura resulta valiosa porque incluye dimensiones que a menudo se separan: localizar información, colaborar, crear, proteger y resolver problemas. Un estudiante que sabe editar video y no puede evaluar una fuente posee una competencia parcial; alguien que verifica información y desconoce cómo proteger una cuenta también. La educación digital necesita equilibrio.

Ng (2012) cuestionó tempranamente la idea de que los llamados nativos digitales dominan automáticamente tecnologías por haber crecido con ellas. La familiaridad cotidiana puede coexistir con debilidades en búsqueda avanzada, evaluación, privacidad o solución de problemas. La etiqueta generacional oculta diferencias de experiencia y puede llevar a que las escuelas dejen de enseñar precisamente a quienes parecen más hábiles.

Eshet-Alkalai (2004) propuso dimensiones como alfabetización foto-visual, reproducción, ramificación, información y socioemocional. Aunque la tecnología ha cambiado, su intuición sigue siendo útil: lo digital exige leer interfaces, navegar estructuras no lineales y comprender normas sociales. Las competencias no son únicamente técnicas.

La capacidad de elegir una herramienta implica conocer el problema antes del software. Si el objetivo es comparar datos, una hoja de cálculo puede ser adecuada; si se necesita conversación asincrónica, un foro puede funcionar; si la tarea es documentar un proceso, un archivo compartido puede ser suficiente. Empezar por la aplicación invierte la lógica. La educación debería preguntar primero qué se quiere lograr.

Saber detenerse forma parte de la competencia. Una plataforma puede facilitar una tarea y añadir distracción, dependencia o exposición de datos. Elegir no utilizar tecnología puede ser una decisión competente cuando la alternativa analógica es más simple, segura o pedagógicamente adecuada. El GEM Report 2023 insiste en que el uso de tecnología debe responder a propósitos educativos, no a la disponibilidad de la herramienta.

La transferencia es el mejor indicador de autonomía. Un estudiante que aprende a estructurar una búsqueda en un motor y puede trasladar el criterio a bases académicas, bibliotecas o catálogos demuestra comprensión. Lo mismo ocurre con privacidad: entender principios permite adaptarse a nuevas interfaces. La competencia digital profunda no depende de memoria de botones.

Esta concepción cambia también la evaluación. En lugar de preguntar dónde está una función, puede pedirse resolver un problema con restricciones: localizar dos fuentes independientes, producir un documento accesible, configurar privacidad o explicar por qué una herramienta no es apropiada. La tarea muestra juicio y no solo ejecución.

La competencia digital también posee una dimensión metacognitiva. Un usuario experto no es quien siempre resuelve solo, sino quien reconoce qué sabe, qué necesita investigar y cuándo pedir ayuda. Esta calibración evita dos errores: abandonar ante una dificultad menor o continuar improvisando en un problema de seguridad que requiere soporte especializado. La autonomía incluye gestionar límites propios.

Los marcos de competencia pueden convertirse en listas si se enseñan fuera de contexto. DigComp ofrece una taxonomía útil, pero el aprendizaje necesita problemas donde varias competencias aparezcan juntas. Verificar una noticia exige búsqueda, evaluación, comunicación y, si se comparte, creación responsable. Proteger una cuenta involucra seguridad, resolución de problemas y comprensión de datos. La vida digital no separa competencias por columnas.

La transferencia también permite distinguir habilidad de automatismo. Un estudiante que sabe insertar una referencia en un procesador específico puede bloquearse al cambiar de herramienta; quien comprende la estructura de una cita puede adaptarse. El mismo principio vale para compartir pantalla, gestionar permisos o exportar datos. La enseñanza debería variar interfaces lo suficiente para que el estudiante identifique el concepto subyacente.

Las prácticas de archivo ofrecen un ejemplo poco glamoroso y esencial. Nombrar documentos, crear carpetas, mantener versiones y respaldar reduce pérdidas. Estas capacidades suelen darse por supuestas porque no producen un resultado visible inmediato. Sin embargo, una persona que domina herramientas creativas y pierde sistemáticamente su trabajo carece de una parte básica de autonomía.

La resolución de problemas necesita estrategias: leer el mensaje de error, aislar variables, reiniciar con criterio, buscar documentación, comparar versiones y registrar qué se cambió.

Enseñar estas rutinas reduce dependencia de ensayo y error. La alfabetización digital también es una forma de pensamiento diagnóstico.

Saber detenerse adquiere un significado adicional en seguridad. Continuar haciendo clic ante un aviso incomprensible puede agravar un problema. La regla “si no entiendes qué permiso o cambio se solicita, detente y verifica” es transferible. La prudencia técnica es una competencia, no una señal de incapacidad.

La competencia digital madura combina fluidez y fricción deliberada. Automatiza tareas repetitivas cuando conviene y ralentiza decisiones sensibles —privacidad, pagos, publicación, permisos—. Esta asimetría es una de las mejores formas de describir autonomía en entornos que incentivan velocidad.

EL ECOSISTEMA DIGITAL EDUCATIVO: INFRAESTRUCTURA, PLATAFORMAS Y GOBERNANZA

La OECD (2023a) describe los ecosistemas digitales educativos como combinaciones de personas, infraestructura, herramientas de gestión y recursos para enseñanza y evaluación. Esta mirada sistémica es importante porque una plataforma de aprendizaje no funciona de manera aislada. Depende de autenticación, conectividad, soporte, políticas de datos, competencias docentes y decisiones de compra.

La pandemia aceleró la adopción de plataformas, pero también dejó sistemas fragmentados. Una escuela puede utilizar un sistema para calificaciones, otro para contenidos, otro para videoconferencia y varios servicios externos. Cada herramienta añade cuentas, permisos y flujos de datos. La gobernanza digital necesita saber qué información circula, quién administra accesos y qué ocurre cuando cambia un proveedor.

La interoperabilidad es un problema poco visible para estudiantes y muy importante para instituciones. Cuando sistemas no pueden intercambiar datos, aumenta carga administrativa y riesgo de errores. Cuando intercambian demasiado sin controles, crece exposición. La transformación digital requiere equilibrio entre integración y minimización.

La contratación tecnológica también tiene consecuencias pedagógicas. Una plataforma puede orientar prácticas porque facilita ciertos tipos de tarea y dificulta otros. Los docentes terminan adaptándose a plantillas y métricas. Selwyn (2016) advierte que la tecnología educativa debe analizarse socialmente y no como instrumento neutral. La pregunta no es solo qué permite, sino qué normaliza.

La gobernanza de datos escolares merece especial atención. Calificaciones, asistencia, comportamiento y actividad en plataformas crean perfiles que pueden acompañar al estudiante durante años. Las instituciones necesitan criterios de acceso, retención y seguridad. La alfabetización digital del estudiante incluye conocer que sus datos educativos forman parte de sistemas institucionales.

Los ecosistemas también necesitan resiliencia. Si una plataforma cae, ¿puede continuar la enseñanza? Si un proveedor cambia condiciones, ¿pueden recuperarse contenidos? Si un docente pierde acceso, ¿existe soporte? Estas preguntas muestran que autonomía institucional y autonomía individual se reflejan mutuamente.

Comprender el acceso digital requiere una idea ampliada de infraestructura: dispositivos y conexión se combinan con capacidades, reglas, soporte, datos y alternativas. La tabla siguiente distingue estas dimensiones para evitar que una única medida de acceso oculte condiciones relevantes para aprender y participar.

Tabla 13. Dimensiones del acceso digital significativo

Dimensión de acceso	Pregunta central	Riesgo de medirla superficialmente
Conectividad	¿La conexión es estable, suficiente y asequible?	Contar a quien posee datos móviles como plenamente conectado.
Dispositivo	¿El equipo permite realizar la tarea con autonomía?	Equiparar teléfono compartido con computador personal.
Habilidades	¿La persona puede buscar, crear, proteger y resolver problemas?	Suponer competencia por edad o frecuencia de uso.
Soporte	¿Existe ayuda cuando algo falla?	Atribuir todo problema a falta de habilidad individual.
Gobernanza	¿Se conocen reglas, datos y responsabilidades?	Adoptar plataformas sin comprender dependencia y riesgos.

Nota. Síntesis de los criterios desarrollados en este capítulo.

La desigualdad digital puede observarse también en la calidad del tiempo disponible. Dos estudiantes con conexión doméstica no tienen necesariamente las mismas condiciones si uno puede trabajar en un espacio silencioso durante dos horas y otro comparte dispositivo, habitación y responsabilidades de cuidado. La categoría “conectado” oculta estas diferencias. Helsper (2021) insiste en que los beneficios digitales dependen de recursos sociales y materiales más amplios. La educación que ignora estas condiciones corre el riesgo de interpretar como falta de compromiso aquello que es una restricción de contexto.

La calidad del dispositivo importa por su relación con la tarea. Escribir un ensayo de diez páginas, analizar una hoja de cálculo o programar resulta posible desde un teléfono y, en muchos casos, significativamente más difícil. La pantalla pequeña, el teclado táctil y la administración de archivos introducen fricciones que consumen tiempo y atención. Esta diferencia muestra por qué el acceso debe evaluarse funcionalmente: ¿el equipo permite realizar la actividad con una carga razonable?

Los costos de datos pueden condicionar estrategias. Un estudiante puede evitar videos, descargar materiales en horarios específicos o depender de redes públicas. Estas adaptaciones muestran agencia, pero también una desigualdad invisible. Diseñar cursos digitales requiere considerar peso de archivos, posibilidad de descarga y alternativas asincrónicas. La inclusión tecnológica comienza en decisiones de diseño aparentemente pequeñas.

La accesibilidad añade otras fricciones. Un documento escaneado como imagen puede ser ilegible para un lector de pantalla; un video sin subtítulos excluye a parte de la audiencia; una plataforma que requiere precisión motriz puede crear barreras. La competencia digital institucional incluye anticipar estas necesidades. No basta con que el recurso exista: debe poder ser usado.

La brecha de apoyo es menos visible. Algunos estudiantes cuentan con familiares o amigos que resuelven problemas técnicos; otros enfrentan cada error solos. Una contraseña perdida o una actualización puede interrumpir días de trabajo. El soporte constituye infraestructura educativa. Una escuela que introduce tecnología sin definir cómo se obtiene ayuda traslada silenciosamente el costo del fallo al usuario.

Hargittai (2002) habló de una segunda brecha digital relacionada con habilidades. Van Deursen y van Dijk (2014) mostraron que, a medida que el acceso material se expande, las diferencias de uso adquieren mayor importancia. La secuencia es relevante para políticas: resolver una brecha puede hacer visible la siguiente. La alfabetización digital necesita evolucionar junto con el ecosistema.

La autonomía digital requiere, finalmente, opciones. Una persona totalmente dependiente de un único proveedor, formato o dispositivo es vulnerable a cambios de precio, fallas o decisiones comerciales. Enseñar exportación de archivos, formatos interoperables y alternativas básicas amplía independencia. La alfabetización no solo pregunta “¿puedes usarlo?”, sino “¿puedes salir de ahí sin perder tu trabajo?”.

La autonomía digital también depende de alfabetización económica mínima sobre servicios en línea. “Gratis” puede significar que el usuario no paga con dinero directo, mientras la empresa obtiene ingresos mediante publicidad, comisiones, datos o servicios complementarios. Comprender el modelo de negocio ayuda a interpretar decisiones de diseño. Una plataforma sostenida por publicidad puede priorizar interacción; una basada en suscripción puede optimizar retención de otra manera. El usuario no necesita conocer balances corporativos para reconocer que la arquitectura responde a incentivos.

Esta comprensión también permite evaluar cambios de condiciones. Un servicio puede comenzar gratuito y después limitar funciones, aumentar precio o introducir publicidad. Si el trabajo de una persona está atrapado dentro de formatos propietarios, la capacidad de salir disminuye. La portabilidad se convierte así en una forma de autonomía económica y técnica.

La sostenibilidad material de lo digital merece atención. Los servicios parecen inmateriales porque la interfaz oculta centros de datos, redes, dispositivos, energía y residuos electrónicos. UNESCO (2023a) incluye sostenibilidad entre criterios para evaluar tecnología educativa. La alfabetización digital puede enseñar que almacenar, transmitir y reemplazar equipos tiene impactos ambientales, en relación con el análisis ambiental del capítulo 4.

La obsolescencia de dispositivos es un buen caso. Un equipo puede seguir funcionando físicamente y quedar fuera de soporte o sin capacidad para nuevas aplicaciones. La decisión de reemplazar tiene dimensiones de seguridad, costo y ambiente. La educación digital no ofrece una fecha universal; enseña a comparar necesidad, soporte y posibilidad de reparación.

El derecho a reparar y la disponibilidad de repuestos muestran cómo una decisión de diseño afecta autonomía. Un dispositivo sellado puede ser más delgado y difícil de mantener. Analizar

estas compensaciones ayuda a comprender que la tecnología materializa prioridades. El usuario puede exigir información sobre reparabilidad y vida útil, aunque no controle toda la cadena.

La inclusión digital, por tanto, también requiere sostenibilidad. Un programa que entrega equipos sin plan de mantenimiento, renovación o soporte puede crear acceso temporal y dependencia posterior. La política digital necesita pensar el ciclo completo de vida del recurso.

La educación digital también necesita reconocer la diferencia entre disponibilidad y apropiación. Un recurso puede estar técnicamente disponible y no formar parte de las prácticas reales de aprendizaje. Esto ocurre cuando el usuario no percibe utilidad, teme equivocarse o encuentra una interfaz que no dialoga con su experiencia. La apropiación implica incorporar la tecnología a un repertorio propio y decidir cuándo sirve. Esa capacidad no se logra únicamente mediante exposición.

La capacitación breve suele concentrarse en procedimientos y deja poco espacio para construir modelos mentales. Un usuario aprende a seguir pasos mientras la interfaz coincide con el tutorial y se desorienta cuando cambia. Enseñar principios —qué es una carpeta, un permiso, una cuenta, un formato o una copia— aumenta transferencia. La educación digital profunda prefiere modelos conceptuales a secuencias rígidas.

Las desigualdades de uso también pueden crecer después de una intervención. Quienes ya poseen mayor experiencia exploran funciones avanzadas y obtienen más beneficios, mientras principiantes usan solo aquello enseñado. Van Deursen et al. (2017) describen la naturaleza compuesta y secuencial de la desigualdad digital. La formación necesita acompañamientos diferenciados para evitar que un mismo recurso amplíe distancias.

La evaluación del acceso debe incluir autonomía de mantenimiento. Un dispositivo puede ser entregado y dejar de ser útil si una batería falla, no existe reparación o el sistema deja de actualizarse. La sostenibilidad del acceso depende de soporte y renovación. Esta observación convierte la política de equipos en política de ciclo de vida.

La conectividad pública ofrece otra capa. Bibliotecas, centros comunitarios y redes escolares pueden compensar falta de acceso doméstico, pero horarios y privacidad condicionan su uso. Realizar un trámite sensible en una red compartida no es equivalente a estudiar un video. La calidad del acceso depende de la tarea y del contexto.

La inclusión digital también necesita considerar confianza. Personas que han sufrido fraude o pérdida de datos pueden evitar servicios útiles. La respuesta no debería ser etiquetarlas como resistentes. Construir confianza exige seguridad, canales de ayuda y experiencias de éxito. La alfabetización puede recuperar agencia cuando permite entender qué ocurrió y cómo reducir riesgos.

Esta perspectiva ayuda a redefinir éxito. Una política digital no triunfa porque aumente usuarios registrados, sino cuando las personas pueden obtener beneficios sin asumir cargas desproporcionadas. La métrica debería observar capacidad, continuidad y control, además de acceso.

6.2. BUSCAR, VERIFICAR Y COMPRENDER INFORMACIÓN EN RED

De encontrar resultados a construir confianza

Internet hizo abundante la información y escasa la atención. La competencia decisiva ya no es encontrar algo, sino justificar por qué una fuente merece confianza y qué límites tiene.

BUSCAR NO ES PREGUNTAR A UNA CAJA NEGRA

Los motores de búsqueda suelen percibirse como ventanas neutrales hacia internet. En realidad, indexan, ordenan y personalizan mediante criterios técnicos y comerciales. La posición de un resultado influye fuertemente en qué se consulta. La educación digital necesita enseñar que un ranking no equivale a una jerarquía de verdad. Encontrar primero significa haber sido priorizado por un sistema, no necesariamente ser la mejor fuente.

La búsqueda eficaz empieza por formular la pregunta. Un término amplio produce ruido; uno demasiado específico puede confirmar una intuición. Enseñar operadores, comillas o filtros ayuda, pero la competencia más profunda es reformular. Un estudiante debería poder generar varias búsquedas para una misma cuestión y observar cómo cambian resultados. La discrepancia revela que buscar es construir una ventana.

Caulfield y Wineburg (2023) popularizan prácticas de verificación que coinciden con

la investigación de Civic Online Reasoning: detenerse, investigar la fuente, buscar cobertura y rastrear afirmaciones. McGrew et al. (2018) mostraron que estudiantes con alta habilidad académica podían evaluar mal sitios web cuando permanecían dentro de la página. La solución fue comportarse más como verificadores profesionales: salir y buscar contexto.

La lectura lateral cambia el centro de atención. En lugar de analizar primero diseño, gramática o referencias del sitio, el lector busca quién está detrás y qué dicen fuentes independientes. Metzger et al. (2010) mostraron que usuarios recurren a heurísticas sociales y visuales para juzgar credibilidad. Estas señales pueden ayudar y también ser manipuladas. Una página elegante puede pertenecer a una organización con interés no declarado.

La fuente primaria es otro concepto central. Un artículo periodístico puede resumir un informe; un influencer puede comentar una noticia; una captura puede recortar una tabla. Rastrear la afirmación hacia el documento original permite recuperar contexto. Esto no significa que toda fuente primaria sea confiable por definición: una empresa puede producir un informe interesado. Significa conocer la distancia entre afirmación y evidencia.

La búsqueda también necesita reconocer ausencia. No encontrar evidencia no demuestra que algo sea falso, pero debe reducir confianza si la afirmación es extraordinaria y debería dejar rastros verificables. El estudiante aprende a calibrar, no a clasificar todo como verdadero o falso en segundos.

La educación digital madura convierte búsqueda en investigación mínima. Cada resultado es una pista; la confianza se construye comparando procedencia, evidencia y coincidencia entre fuentes independientes.

La búsqueda también está atravesada por desigualdad lingüística. Muchas consultas producen más resultados, mejores documentos y mayor cobertura en inglés que en otras lenguas. El usuario que domina varios idiomas posee una ventaja informacional. La educación puede enseñar a traducir conceptos clave, buscar equivalentes y comparar cómo diferentes comunidades nombran el mismo problema. Esta práctica amplía el mapa de fuentes.

El sesgo de confirmación puede comenzar en la consulta. Preguntar “por qué X es malo” orienta resultados de forma distinta a “evidencia sobre efectos de X”. Enseñar a formular búsquedas neutrales o simétricas reduce parte de esta tendencia. Una actividad útil consiste en comparar resultados de preguntas cargadas y descriptivas.

La procedencia importa especialmente en estadísticas. Muchos contenidos virales atribuyen cifras a “un estudio” sin enlace. Rastrear el número puede revelar que proviene de una encuesta pequeña, una estimación antigua o una fuente distinta. El estudiante aprende que citar una institución conocida no basta; la afirmación necesita correspondencia exacta con el documento.

Las capturas de pantalla crean una falsa sensación de permanencia. Pueden modificarse, recortarse o perder la URL. Una buena práctica es conservar enlace, fecha y contexto. En investigación escolar, la captura funciona como evidencia auxiliar, no como sustituto de la fuente original.

Los resultados patrocinados añaden otra capa. Un anuncio puede responder mejor a una búsqueda que un resultado orgánico y continuar siendo publicidad. La educación debe enseñar a identificar etiquetas de patrocinio y reconocer que relevancia comercial no equivale a recomendación independiente. Esta distinción es importante en salud, finanzas y consumo.

La búsqueda por imágenes y video necesita técnicas propias. Una fotografía puede haber sido invertida, recortada o reutilizada. La búsqueda inversa ayuda a encontrar versiones anteriores. El análisis de fotogramas clave permite rastrear video. Estas prácticas pueden enseñarse sin exigir herramientas especializadas de periodismo.

La competencia de búsqueda se completa cuando el estudiante puede explicar cómo cambió su pregunta durante la investigación. Una búsqueda profunda rara vez sigue una consulta inicial intacta. Reformular a partir de nueva información es señal de aprendizaje, no de indecisión.

DESINFORMACIÓN, MOTIVACIÓN Y EL PROBLEMA DE CREER LO QUE QUEREMOS CREER

La desinformación no prospera únicamente por falta de conocimiento. Las personas evalúan contenidos desde identidades, emociones y preferencias previas. Kahne y Bowyer (2017) mostraron cómo el razonamiento motivado afecta evaluación de afirmaciones en temas políticos y cómo la alfabetización mediática puede ayudar. El hallazgo es transferible: verificar resulta más difícil cuando una información confirma aquello que deseamos creer.

Esta dificultad obliga a una regla incómoda: verificar especialmente lo favorable. Muchos usuarios aplican escrutinio intenso a fuentes contrarias y tolerancia a fuentes afines. Una rutina

puede exigir buscar una fuente independiente incluso cuando el contenido coincide con nuestras expectativas. La alfabetización digital se vuelve una práctica de autocontrol cognitivo.

Wardle y Derakhshan (2017) distinguen entre información errónea, desinformación e información dañina según falsedad e intención. La clasificación es útil porque evita llamar “fake news” a todo contenido problemático. Un error compartido de buena fe necesita corrección; una campaña deliberada puede requerir respuesta diferente; una información verdadera difundida para causar daño plantea otra cuestión.

Las imágenes añaden dificultad porque producen una sensación de evidencia directa. Sin embargo, pueden ser antiguas, recortadas o generadas. La verificación básica incluye búsqueda inversa, fecha, lugar y fuente. La expansión de contenido sintético aumenta la importancia de procedencia. La capacidad estable no es detectar visualmente una falsificación perfecta, sino buscar contexto externo.

La velocidad de circulación es parte del problema. Compartir requiere segundos; verificar puede tomar minutos. Las plataformas reducen fricción para amplificar y suelen añadir menos fricción para comprobar. La educación puede introducir una pausa deliberada: si el contenido provoca indignación o urgencia, suspender el envío y buscar una segunda fuente.

Breakstone et al. (2021) encontraron dificultades importantes entre estudiantes de secundaria de Estados Unidos al evaluar información cívica en línea. McGrew (2020) mostró que una intervención explícita podía mejorar el desempeño. La conclusión pedagógica es importante: la evaluación crítica no aparece espontáneamente con más tiempo de pantalla; necesita enseñanza.

La desinformación se convierte así en problema de hábitos, motivación y arquitectura. Educar implica combinar técnicas de verificación con conciencia sobre los impulsos que nos hacen compartir antes de pensar.

El razonamiento motivado es especialmente difícil porque opera incluso entre personas informadas. Kahne y Bowyer (2017) encontraron que la sofisticación política no inmuniza contra el sesgo. La educación necesita procedimientos, no exhortaciones. Una técnica consiste en pedir qué evidencia haría cambiar de opinión antes de mostrar nuevos datos. Esta pregunta obliga a definir un criterio de falsación personal.

Otra técnica es la inversión de posición: evaluar un argumento sin conocer de qué grupo proviene o reescribir de manera justa la posición contraria. El objetivo no es fingir neutralidad total, sino separar temporalmente contenido e identidad. Esta práctica puede reducir el rechazo automático a una fuente por afinidad partidaria o cultural.

El humor y la sátira complican la clasificación. Un contenido falso puede no pretender engañar y ser compartido fuera de contexto. Wardle y Derakhshan (2017) recuerdan que intención y falsedad son dimensiones distintas. La educación debe preguntar qué función cumple la pieza antes de etiquetarla.

La corrección también tiene una dimensión social. Señalar un error públicamente puede provocar resistencia si amenaza identidad. En grupos de clase, enseñar cómo corregir —con fuente, sin humillar y reconociendo buena fe cuando corresponde— convierte la alfabetización en convivencia. La verdad importa y también la forma de reconstruir confianza.

Los sistemas generativos añaden un tipo nuevo de plausibilidad. Un texto puede estar bien escrito y contener referencias inventadas. La regla de verificación no cambia: una cita necesita existir y sostener la afirmación. La fluidez es una característica de estilo, no una garantía epistemológica. Esta idea será central en el capítulo 11, dedicado a educación para la inteligencia artificial.

La sobrecarga informativa puede llevar al cinismo: si todo puede ser manipulado, parece imposible saber algo. La alfabetización debe evitar este extremo. Las fuentes tienen grados de confiabilidad, las instituciones producen registros y la evidencia puede contrastarse. El objetivo no es desconfiar de todo, sino confiar con razones.

La capacidad de declarar incertidumbre protege frente a ambos extremos. Un estudiante puede concluir que una afirmación está bien respaldada, es dudosa o no puede verificarse con la información disponible. Esta escala es más realista que un detector binario de verdad.

DE LA FUENTE AL ARGUMENTO: COMPRENDER, NO SOLO DETECTAR

Una fuente confiable puede contener un argumento débil y una fuente interesada puede aportar un dato correcto. La alfabetización digital necesita ir más allá de clasificar sitios. El lector debe distinguir afirmación, evidencia y razonamiento. Esta estructura permite evaluar contenidos

incluso cuando la procedencia es conocida.

La estadística básica forma parte de esta capacidad. Porcentajes sin denominador, promedios sin distribución o gráficos con ejes truncados pueden producir interpretaciones engañosas. El usuario digital encuentra cifras diariamente y necesita preguntar población, periodo y fuente. La alfabetización de datos converge con educación científica.

Las recomendaciones personalizadas introducen otro sesgo: el usuario puede confundir frecuencia con consenso. Ver muchas publicaciones similares puede indicar que el sistema aprendió sus intereses, no que la mayoría de la sociedad piense igual. La diversidad informativa necesita búsqueda activa fuera de la corriente personalizada.

Los comentarios y reacciones pueden servir como señales sociales y alterar interpretación. Una publicación con miles de “me gusta” parece más legítima. Sin embargo, la popularidad mide interacción, no veracidad. Bots, campañas coordinadas o simples dinámicas virales pueden inflar visibilidad. La educación debe enseñar a separar métricas de calidad epistemológica.

La comprensión también requiere leer contexto temporal. Una noticia verdadera de hace cinco años puede circular como si fuera actual. El cambio de fecha puede alterar completamente su significado. Verificar fecha y lugar es una práctica básica que evita parte importante de la desinformación visual.

El objetivo final no es convertir a cada estudiante en fact-checker profesional. Es desarrollar una rutina razonable de confianza: detenerse, identificar fuente, rastrear evidencia, comparar cobertura y declarar incertidumbre. Esta rutina puede aplicarse a ciencia, consumo, salud, política o educación.

Cuando el usuario aprende a decir “esta afirmación parece plausible, pero todavía no tengo suficiente evidencia”, alcanza una forma de autonomía digital más valiosa que la seguridad rápida. La incertidumbre bien justificada es mejor que la certeza sin trazabilidad.

La verificación en red se vuelve más compleja cuando las fuentes se citan entre sí. Diez páginas pueden repetir la misma afirmación y crear apariencia de consenso aunque todas dependan de una fuente inicial. La educación necesita enseñar a identificar cadenas de citación. Contar enlaces no equivale a contar evidencias independientes.

La temporalidad de la información importa especialmente en ámbitos dinámicos. Una guía de seguridad de hace cinco años puede recomendar prácticas superadas; una estadística puede describir otra fase del fenómeno. La fecha no determina calidad, pero debe formar parte de la evaluación. El estudiante aprende a preguntar si necesita conocimiento histórico o estado actual.

Las fuentes oficiales tampoco son infalibles. Pueden cometer errores, actualizar datos o representar una perspectiva institucional. Su ventaja radica en autoridad y trazabilidad para ciertos tipos de afirmación. La alfabetización madura evita dos extremos: aceptar todo documento oficial sin examen o equiparlo con cualquier publicación anónima. Las fuentes poseen funciones y grados de autoridad.

La experiencia de Wikipedia puede utilizarse de manera pedagógica. La enciclopedia colaborativa no debería presentarse simplemente como fuente prohibida o definitiva. Sus referencias y páginas de discusión permiten observar cómo se construye y disputa conocimiento. El estudiante puede usarla como punto de partida, seguir fuentes y comparar estabilidad de artículos.

La búsqueda académica introduce otras competencias: palabras clave, operadores, filtros, DOI y lectura de resúmenes. No todos los estudiantes necesitan dominar bases especializadas, pero reconocer diferencia entre una búsqueda general y una base académica amplía repertorio. El tipo de pregunta determina dónde conviene buscar.

La evaluación de información termina siendo una práctica de triangulación. Una afirmación gana fuerza cuando diferentes fuentes competentes, con métodos distintos, convergen. Esta lógica conecta alfabetización digital con alfabetización científica y reduce dependencia de una sola autoridad.

6.3. PLATAFORMAS, ATENCIÓN Y PODER ALGORÍTMICO

Lo que vemos también depende de cómo está diseñado el entorno

Las plataformas conectan personas y oportunidades, pero organizan visibilidad mediante reglas, métricas y sistemas de recomendación. Comprender esa mediación es parte de la autonomía digital.

LA PLATAFORMA NO ES SOLO UN CANAL

Una plataforma digital define formatos, límites, incentivos y mecanismos de interacción. Permite ciertas acciones con un clic y vuelve otras difíciles. Gillespie (2018) muestra que las plataformas gobiernan espacios públicos mediante reglas de moderación y clasificación, aunque se presenten como intermediarios neutrales. La arquitectura participa en la conversación.

Las métricas visibles —seguidores, reproducciones, reacciones— cambian la forma en que usuarios perciben éxito. Una publicación puede diseñarse para maximizar interacción y no para comunicar con precisión. La economía de la atención convierte tiempo y comportamiento en recursos valiosos. Citton (2017) propone pensar la atención como un problema político y cultural; la educación digital puede traducir esa idea a hábitos cotidianos.

La recomendación algorítmica agrega personalización. El sistema observa señales y prioriza contenidos que considera relevantes. Esta capacidad puede ayudar a descubrir información y reducir sobrecarga. También puede estrechar la experiencia si el usuario interpreta el feed como representación espontánea del mundo. La educación necesita enseñar que cada feed es una construcción.

El término “algoritmo” suele utilizarse como explicación total. Decir “el algoritmo me mostró esto” oculta objetivos, datos y diseño. Un análisis más preciso pregunta qué conducta está optimizando la plataforma, qué señales utiliza y qué control tiene el usuario. La alfabetización algorítmica no exige programar; exige comprender relaciones entre datos, objetivo y salida.

Cotter (2019) mostró cómo creadores en Instagram desarrollan teorías y estrategias para ganar visibilidad frente a un algoritmo opaco. Esta relación produce una forma de poder: los usuarios adaptan conductas a reglas que conocen parcialmente. La educación digital puede utilizar el caso para explicar que la opacidad no elimina efectos; los participantes intentan inferir el sistema.

La moderación es otra capa. Eliminar acoso, amenazas o contenido ilegal puede proteger usuarios; decisiones excesivas o inconsistentes pueden afectar expresión legítima. Gillespie (2018) muestra que la moderación es trabajo central y difícil. La educación no necesita resolver cada controversia, pero sí distinguir reglas privadas, legislación y criterios comunitarios.

La plataforma termina siendo una institución híbrida: empresa, infraestructura, espacio social y sistema de datos. Tratarla únicamente como herramienta pedagógica deja fuera buena parte de su influencia.

LA ECONOMÍA DE LA ATENCIÓN: CUANDO LA INTERRUPCIÓN ESTÁ DISEÑADA

Las notificaciones parecen detalles de interfaz y, sin embargo, organizan el tiempo. Un punto rojo, una vibración o un conteo de mensajes crea urgencia. La plataforma compite por recuperar al usuario y convertir interrupciones en hábito. La educación digital debe enseñar que la distracción no es exclusivamente falta de disciplina individual; el entorno puede estar diseñado para solicitar atención.

Alter (2017) y Eyal (2014), desde perspectivas diferentes, describen cómo productos digitales utilizan bucles de hábito. Estas obras no sustituyen evidencia experimental, pero popularizaron una discusión sobre diseño persuasivo. Fogg (2003) había planteado desde la interacción humano-computador que la tecnología puede diseñarse para cambiar conductas. La cuestión educativa es reconocer cuándo una función ayuda y cuándo secuestra la prioridad.

La multitarea digital suele sentirse productiva porque muchas ventanas permanecen activas. Sin embargo, cambiar repetidamente de tarea tiene costos cognitivos. Ophir et al. (2009) encontraron diferencias en control cognitivo entre usuarios intensivos y moderados de multitarea mediática, aunque la literatura posterior ha discutido magnitud y causalidad. La enseñanza prudente no necesita afirmar que toda multitarea daña el cerebro; puede mostrar que la atención es limitada y que tareas complejas se benefician de menos interrupciones.

El bienestar digital debe evitar moralizar el tiempo de pantalla. Una hora de videollamada con familiares no equivale a una hora de consumo pasivo ni a una tarea académica. Orben y Przybylski (2019) mostraron que relaciones entre uso digital y bienestar adolescente son pequeñas y complejas. La cantidad de tiempo es un indicador pobre sin contexto.

Una educación útil puede trabajar con patrones: qué actividad, en qué momento, con qué efecto y bajo qué control. El estudiante registra interrupciones, identifica aplicaciones que fragmentan atención y prueba configuraciones. El objetivo no es alcanzar una cifra universal, sino gobernar el uso según metas.

El diseño de notificaciones puede convertirse en un caso de ingeniería inversa. ¿Qué conducta intenta producir?, ¿qué información ofrece?, ¿qué pasaría si se desactiva? Estas preguntas convierten una interfaz cotidiana en objeto de análisis. La autonomía comienza cuando el usuario descubre que muchas configuraciones predeterminadas pueden modificarse.

El bienestar digital se aleja así de discursos de abstinencia y se acerca a autorregulación informada. La tecnología puede ser intensiva y saludable en un contexto, e intensiva y destructiva en otro. La educación necesita criterio, no una prohibición uniforme.

El bienestar digital necesita distinguir uso activo y pasivo con cuidado. Algunas investigaciones han encontrado diferencias, pero las categorías son demasiado amplias para explicar todos los resultados. Comentar puede ser conexión significativa o conflicto; mirar puede ser relajación o comparación dañina. La educación debe trabajar con función y efecto personal, no con etiquetas rígidas.

La multitarea puede analizarse experimentalmente en clase. El estudiante realiza una tarea con notificaciones activas y otra con interrupciones reducidas, luego compara tiempo y errores. El ejercicio no pretende demostrar una ley universal con una muestra pequeña; permite observar la propia experiencia y discutir límites del diseño.

La regulación de atención también puede ser colectiva. Un grupo acuerda que durante una sesión los teléfonos permanezcan fuera de la mesa o en modo silencioso. Después evalúa si la regla mejoró concentración. La norma deja de ser moral y se convierte en hipótesis institucional.

El derecho a la desconexión añade una dimensión laboral y educativa. Si una cultura espera respuestas nocturnas, el problema no se resuelve únicamente con autocontrol. Las organizaciones necesitan definir urgencias y horarios. La autonomía individual depende de expectativas colectivas.

Las plataformas pueden ofrecer herramientas de bienestar —recordatorios, paneles de tiempo, límites— y al mismo tiempo depender de interacción. Esta tensión muestra que las soluciones internas tienen límites. El usuario puede utilizarlas y conservar criterio sobre el modelo del servicio.

La atención también está relacionada con accesibilidad cognitiva. Interfaces cargadas, ventanas emergentes y cambios constantes aumentan esfuerzo. El diseño inclusivo puede reducir distracción y beneficiar a muchos usuarios, no solo a quienes tienen diagnósticos específicos.

La educación digital del bienestar se resume en observación y ajuste. No prescribe una cantidad universal; ayuda a descubrir cuándo el entorno está interfiriendo con aquello que la persona valora.

RECOMENDACIÓN, PERSONALIZACIÓN Y BURBUJAS INFORMATIVAS

La personalización resuelve un problema real: internet contiene más información de la que cualquier persona puede procesar. Sistemas de recomendación filtran y ordenan. El problema aparece cuando la lógica de selección es invisible o cuando el usuario atribuye a la realidad aquello que pertenece a su perfil. Comprender personalización significa reconocer que dos personas pueden recibir representaciones muy diferentes del mismo entorno.

Pariser (2011) popularizó la expresión “filter bubble”, aunque la investigación posterior ha mostrado una realidad más matizada. Las personas no viven necesariamente aisladas de todo desacuerdo, y la exposición depende de plataforma y comportamiento. La educación digital debe evitar convertir una metáfora en ley universal. Puede afirmar con mayor seguridad que la selección personalizada influye en la mezcla de contenidos y que diversificar fuentes requiere acción.

Bakshy et al. (2015) estudiaron exposición a noticias ideológicamente diversas en Facebook y encontraron que tanto el algoritmo como las elecciones de los usuarios afectan la diversidad de contenidos. Este tipo de evidencia ayuda a escapar de explicaciones monocausales. El sistema importa y la conducta del usuario también.

La recomendación también puede crear ventajas. Plataformas de música, aprendizaje o video permiten descubrir contenidos que el usuario nunca habría buscado. La educación digital no debe tratar toda personalización como manipulación. Necesita evaluar objetivo, transparencia, control y consecuencias. La misma técnica puede apoyar descubrimiento o reforzar consumo repetitivo.

El control del usuario puede incluir seguir fuentes diversas, limpiar historial, ajustar preferencias o cambiar de servicio. Sin embargo, parte de la lógica permanece fuera de su alcance. La autonomía es parcial. Reconocer límites protege frente a la fantasía de control total y justifica

regulación y diseño responsable.

La alfabetización algorítmica puede evaluarse mediante explicaciones causales sencillas: si interactúo repetidamente con cierto contenido, ¿qué señales recibe el sistema y qué resultado podría esperar? El estudiante no necesita conocer código para comprender bucles de retroalimentación.

Las plataformas amplían participación y acceso, mientras organizan atención y visibilidad. Comprender ambas funciones permite examinar sus incentivos y sus efectos sin reducirlas a una herramienta neutral ni atribuirles control absoluto sobre los usuarios.

La economía de la atención se vuelve más comprensible cuando se analiza el modelo de negocio. Muchas plataformas ofrecen acceso sin pago directo y obtienen ingresos mediante publicidad, suscripciones, comisiones o venta de servicios. Cuando la publicidad depende de interacción, retener atención adquiere valor económico. Esta relación no prueba que toda función esté diseñada para “adictar”, pero explica por qué el tiempo del usuario importa.

Los indicadores de engagement pueden orientar diseño. Reproducciones, tiempo de permanencia y frecuencia de retorno se convierten en métricas. Una función que incrementa una métrica puede ser considerada exitosa aunque tenga efectos ambiguos sobre bienestar. La educación digital necesita enseñar que un indicador empresarial y un objetivo del usuario pueden no coincidir.

El scroll infinito ofrece un caso simple. Eliminar el punto natural de cierre reduce oportunidades para decidir si continuar. La función puede mejorar comodidad y aumentar consumo. Analizarla permite discutir diseño sin demonizarlo. El usuario puede compensar mediante límites, temporizadores o elecciones de formato.

Las rachas, recompensas y conteos también transforman conducta. En una aplicación educativa pueden sostener práctica; en otros contextos pueden generar presión para mantener actividad. La misma mecánica produce efectos distintos según propósito y usuario. La alfabetización de diseño necesita evitar juicios absolutos.

La personalización comercial también puede servir al usuario. Un servicio de música que aprende gustos reduce esfuerzo de búsqueda. La pregunta de autonomía es si la persona comprende que la selección es parcial y puede explorar fuera de ella. Control y transparencia importan más que la existencia misma de recomendación.

La atención posee una dimensión colectiva. Cuando millones de usuarios dedican tiempo a contenidos seleccionados por unas pocas plataformas, estas empresas adquieren capacidad para influir en agendas culturales. Napoli (2019) analiza esta dimensión de interés público. La educación digital puede incorporar la idea sin convertir cada recomendación en manipulación deliberada.

Comprender economía de atención permite al usuario pasar de “me distraje” a “¿qué diseño y qué hábito produjeron esta interrupción?”. Esta reformulación abre opciones de intervención más específicas.

Las plataformas también configuran normas sociales mediante aquello que hacen visible. Un contador público de seguidores convierte popularidad en señal; una opción de “visto” modifica expectativas de respuesta; una racha convierte continuidad en objetivo. Estas funciones no determinan conducta, pero crean presiones. La alfabetización digital puede tratar la interfaz como texto cultural que comunica qué comportamientos valora.

La opción predeterminada tiene especial poder porque muchas personas no cambian configuraciones. Privacidad, reproducción automática y notificaciones pueden depender de defaults. La educación conductual muestra que aquello que viene activado suele mantenerse. Enseñar a revisar configuraciones iniciales es una práctica simple de autonomía.

La opacidad algorítmica también produce mitologías. Usuarios intentan descifrar por qué una publicación obtuvo alcance o por qué una cuenta fue recomendada. Algunas teorías contienen observaciones útiles y otras se convierten en supersticiones digitales. Cotter (2019) muestra cómo creadores negocian esta incertidumbre. La educación puede enseñar a distinguir evidencia de rumores sobre “el algoritmo”.

La personalización puede reforzar hábitos porque aprende de aquello que hacemos incluso cuando no representa una preferencia estable. Ver varios videos sobre un tema por curiosidad puede modificar recomendaciones durante días. El usuario necesita comprender que sus acciones entrenan parcialmente su entorno. Esta conciencia permite intervenir mediante historial, suscripciones o búsquedas deliberadas.

Las métricas pueden crear comparación social. Un trabajo creativo valorado por su calidad puede sentirse irrelevante si recibe poca interacción. La educación necesita separar objetivos: aprender, comunicar a una audiencia específica o maximizar alcance son metas distintas. No

todas deberían evaluarse con la misma métrica.

La plataforma también define aquello que puede medirse. Aspectos fáciles de cuantificar ganan visibilidad frente a relaciones o aprendizajes difíciles de contar. Esta limitación es importante en educación: una plataforma puede registrar clics y tiempo y no comprender calidad de reflexión. Los datos de actividad no son sinónimo de aprendizaje.

La gobernanza de plataformas incluye una cuestión de poder de salida. Un usuario puede estar en desacuerdo con reglas y continuar porque allí se encuentran sus contactos, audiencia o materiales. Los efectos de red hacen costoso abandonar. La libertad de elección formal puede coexistir con dependencia práctica. La educación digital necesita enseñar a reconocer esta situación y a conservar copias, contactos y alternativas cuando sea posible.

La portabilidad de datos intenta reducir parte de ese costo. Poder descargar contenidos, contactos o históricos aumenta control, aunque los formatos y compatibilidad pueden limitar utilidad. La idea pedagógica es importante: los datos producidos por una persona no deberían quedar completamente atrapados en una interfaz. Exportar y respaldar son prácticas de autonomía.

Las comunidades en línea también desarrollan normas informales. Una plataforma puede permitir una conducta y un grupo considerarla inapropiada. El usuario aprende simultáneamente reglas técnicas, términos de servicio y expectativas comunitarias. La competencia social digital consiste en navegar estas capas sin asumir que son equivalentes.

La moderación automatizada introduce errores de escala. Sistemas pueden detectar patrones rápidamente y equivocarse en ironía, contexto o idioma. La revisión humana puede corregir y también ser inconsistente. La educación digital necesita mostrar que gobernar grandes comunidades implica compensaciones entre velocidad, costo y contexto. No existe moderación perfecta.

La transparencia de las reglas importa porque usuarios adaptan su conducta. Una norma vaga puede producir autocensura o aplicación arbitraria. Publicar criterios y ofrecer explicaciones no elimina desacuerdo, pero mejora previsibilidad. Esta lógica conecta con el debido proceso estudiado en el capítulo jurídico.

Las plataformas educativas participan de la misma problemática. Un sistema puede bloquear una entrega, marcar actividad sospechosa o clasificar desempeño. La institución necesita saber qué decisiones toma automáticamente y cómo puede revisarlas. La tecnología de aula no está fuera de la gobernanza; es una extensión de ella.

Comprender plataformas, por tanto, requiere mirar más allá de contenido y usuario. Existe una tercera capa: las reglas y sistemas que organizan la interacción. La educación digital madura hace visible esta arquitectura para que las personas puedan usarla sin confundirla con una ley natural.

La alfabetización algorítmica necesita además enseñar que un sistema puede ser útil sin ser completamente comprensible para el usuario. Una persona no conoce el funcionamiento interno de un motor de búsqueda y puede utilizarlo con eficacia. El problema aparece cuando atribuye al sistema una neutralidad o una autoridad que no tiene. La competencia consiste en saber qué tipo de salida produce, qué datos pueden influir y qué decisiones relevantes no conviene delegar sin revisión.

Esta distinción entre uso y delegación es especialmente importante. Una recomendación musical puede aceptarse con bajo costo de error; una recomendación médica, financiera o académica exige otro estándar. La misma tecnología de personalización cambia de significado según consecuencia. La educación digital puede enseñar a clasificar decisiones por impacto y ajustar el nivel de verificación.

La opacidad tampoco es idéntica en todos los casos. A veces el sistema es técnicamente complejo; otras veces la empresa decide no revelar detalles; en otras, la personalización es sencilla pero invisible. Nombrar el tipo de opacidad ayuda a formular preguntas más precisas. “No entiendo el algoritmo” puede convertirse en “no sé qué objetivo optimiza” o “no sé qué datos usa”. Esa precisión es una forma de alfabetización.

La capacidad de experimentar controladamente puede aumentar comprensión. Cambiar deliberadamente una preferencia, limpiar historial o seguir fuentes nuevas permite observar cómo responde el sistema, aunque nunca revele toda su lógica. El usuario aprende mediante intervención y comparación. Esta práctica es más educativa que aceptar explicaciones míticas sobre lo que “el algoritmo quiere”.

La portabilidad complementa esta alfabetización porque reduce dependencia. Guardar contactos, exportar documentos y utilizar formatos estándar permite cambiar de servicio sin empezar de cero. Una plataforma que dificulta la salida puede ofrecer muchas funciones y reducir

autonomía. La educación digital debe incluir la pregunta por la reversibilidad de una elección tecnológica.

Esta reversibilidad es un criterio útil también para instituciones. Adoptar una herramienta de manera piloto, conservar copias y acordar condiciones de salida permite aprender sin comprometer todo el sistema. La gobernanza tecnológica madura evita convertir una innovación inicial en dependencia irreversible por simple inercia.

Este análisis de mediación y delegación permite relacionar los capítulos 6 y 11. Los sistemas generativos añaden problemas de producción de contenido a preguntas ya presentes: qué datos intervienen, qué objetivo persigue el sistema, qué salida produce, qué riesgo implica y qué posibilidad de revisión conserva el usuario.

6.4. IDENTIDAD, PRIVACIDAD Y SEGURIDAD DIGITAL

Los datos no desaparecen cuando dejamos de mirar la pantalla

La vida digital produce rastros. Protegerse implica hábitos personales, pero también comprender responsabilidades institucionales y consecuencias de almacenar información a gran escala.

IDENTIDAD DIGITAL: UNA PERSONA, MUCHOS RASTROS

La identidad digital no es una copia exacta de la identidad física. Está compuesta por cuentas, publicaciones, historiales, datos transaccionales y perfiles inferidos. boyd (2014) muestra cómo adolescentes negocian públicos y privacidad dentro de redes donde el contexto puede colapsar: un mensaje pensado para amigos llega a familiares, docentes o desconocidos. La audiencia real supera a la imaginada.

Esta persistencia cambia la relación con el error. Una broma, comentario o fotografía puede reaparecer años después y fuera de contexto. La educación digital necesita enseñar que publicar produce memoria distribuida. Borrar una publicación reduce visibilidad, pero no garantiza desaparición de copias, capturas o archivos.

La identidad también puede ser construida por otros. Etiquetas, fotografías, menciones y bases de datos agregan información que la persona no creó. La autonomía digital incluye gestionar aquello que se publica sobre uno y respetar la identidad ajena. Pedir consentimiento antes de compartir una imagen de otra persona es una práctica sencilla con fundamento ético y jurídico.

La reputación en línea puede producir efectos reales en empleo, relaciones y seguridad. Sin embargo, la educación debe evitar asustar a estudiantes con la idea de una “huella digital” permanente que determina toda su vida. El objetivo es desarrollar criterio y capacidad de reparación. Las personas cambian y los contextos importan.

La identidad requiere autenticación. Contraseñas, gestores y factores adicionales no son meros detalles técnicos; protegen acceso a información y capacidad de actuar en nombre propio. La cuenta comprometida puede utilizarse para fraude, acoso o pérdida de archivos. La seguridad forma parte de la autonomía.

El anonimato también tiene funciones legítimas. Puede proteger denunciantes, jóvenes vulnerables o participación en comunidades sensibles. Una educación digital madura evita identificar anonimato con conducta irresponsable. Analiza beneficios y riesgos según contexto.

La identidad digital es, en suma, relacional y técnica. Se construye mediante lo que publicamos, lo que otros registran y lo que sistemas infieren. La alfabetización consiste en comprender estas capas y saber intervenir en ellas.

La privacidad contextual de Nissenbaum (2010) ofrece una alternativa a pensar que la privacidad consiste únicamente en ocultar información. Un dato puede ser apropiado en un contexto y problemático cuando se transfiere a otro. Compartir una dirección con un servicio de entrega tiene sentido; utilizarla para una finalidad inesperada plantea otra cuestión. La educación digital puede enseñar a preguntar no solo “¿es secreto?”, sino “¿es apropiado este flujo?”.

Los permisos de aplicaciones permiten practicar esta lógica. Cámara, ubicación o contactos pueden ser necesarios para una función y excesivos para otra. Revisar permisos enseña minimización desde la perspectiva del usuario. La persona no necesita comprender toda la infraestructura para identificar una incoherencia básica entre función y dato.

El perfilado agrega inferencias que el usuario nunca declaró. A partir de comportamiento,

un sistema puede estimar intereses o riesgo. Couldry y Mejias (2019) analizan críticamente la extracción de datos como parte de modelos económicos. La educación puede utilizar esta discusión para mostrar que el rastro digital incluye lo que hacemos y lo que se infiere.

La privacidad también se negocia socialmente. Publicar una fotografía grupal afecta a otros. Una persona puede sentirse cómoda con una imagen y otra no. La educación necesita prácticas de consentimiento cotidiano: preguntar antes de etiquetar, compartir o incluir información identificable en trabajos públicos.

La seguridad de identidad debe contemplar recuperación. Una contraseña robusta sirve poco si el correo de recuperación está comprometido. Configurar métodos alternativos y conservar códigos de respaldo son prácticas que aumentan resiliencia. La alfabetización digital puede enseñar el ciclo completo de acceso, no solo creación de contraseña.

La suplantación se vuelve más compleja con contenido sintético. Una voz o imagen pueden imitar a una persona. La respuesta general es verificar solicitudes inusuales por un canal independiente. La técnica cambia; el principio de autenticación fuera de banda permanece.

La privacidad madura se entiende como gestión de flujos, no como desaparición. Participar digitalmente produce datos. La autonomía consiste en reducir exposición innecesaria, comprender contextos y exigir responsabilidades a quienes almacenan información.

EQUIFAX: CUANDO PROTEGER DATOS EXCEDE LA CAPACIDAD DEL USUARIO

En septiembre de 2017, Equifax anunció un incidente que expuso información personal de aproximadamente 147 millones de personas. La FTC alegó posteriormente que la compañía no había tomado medidas razonables para proteger su red y alcanzó, junto con otras autoridades, un acuerdo de al menos 575 millones de dólares y potencialmente hasta 700 millones. Los datos comprometidos incluían nombres, fechas de nacimiento, números de identificación y direcciones, información capaz de facilitar robo de identidad y fraude (Federal Trade Commission, 2019a).

El caso es pedagógicamente valioso porque desmonta una explicación individualista de la seguridad. Una persona afectada podía haber utilizado contraseñas excelentes y no controlar cómo Equifax almacenaba sus datos. La seguridad digital es una relación entre comportamiento del usuario y prácticas institucionales. Culpas exclusivamente al individuo por una filtración de terceros confunde niveles de responsabilidad.

La FTC señaló fallas relacionadas con vulnerabilidades y protección de información. La lección transferible es que actualizar, segmentar, monitorear y gobernar datos son responsabilidades organizacionales. En una escuela, empresa o gobierno, la ciberseguridad necesita inventario de sistemas, responsables y planes de respuesta. No puede depender solo de una charla anual.

El caso también muestra que los datos poseen una vida posterior al incidente. Cambiar una contraseña no modifica un número de identificación expuesto. La respuesta incluye monitoreo, alertas y medidas frente a fraude. La educación digital necesita enseñar qué hacer después de una brecha: verificar comunicación oficial, cambiar credenciales cuando corresponda, vigilar cuentas y desconfiar de estafas que aprovechan el propio incidente.

La asimetría informativa es central. Las personas rara vez saben qué empresas poseen copias de sus datos, qué sistemas los procesan o cuánto tiempo permanecen almacenados. Esta opacidad justifica principios de minimización y transparencia. Recoger menos información reduce superficie de daño.

Equifax también permite hablar de responsabilidad sin convertir el caso en argumento contra toda base de datos. Los sistemas de información pueden ofrecer beneficios importantes. El problema es gobernarlos según sensibilidad, necesidad y riesgo. La educación digital necesita evitar tanto la despreocupación como el rechazo absoluto.

La privacidad deja de ser así una preferencia individual y se vuelve una cuestión de diseño institucional. El usuario necesita hábitos; la organización necesita controles; la regulación establece obligaciones. La autonomía se distribuye.

Equifax muestra también el problema de la concentración. Una organización que reúne grandes volúmenes de datos se convierte en objetivo valioso. El beneficio de centralizar puede ser eficiencia; el costo es aumentar impacto potencial de una brecha. La gobernanza necesita evaluar esta relación y aplicar controles proporcionales a sensibilidad y volumen.

La notificación posterior a una brecha es parte de la respuesta. Las personas necesitan saber qué ocurrió, qué información pudo verse afectada y qué acciones pueden tomar. Una comunicación ambigua puede agravar daño porque crea espacio para estafas. Los atacantes suelen aprovechar incidentes conocidos para enviar mensajes falsos. La educación digital debe

enseñar a buscar el portal oficial en lugar de seguir enlaces inesperados.

El monitoreo de identidad plantea otra lección. Algunas consecuencias de una brecha aparecen meses o años después. La seguridad no termina cuando el incidente desaparece de las noticias. Esta temporalidad contrasta con la lógica rápida de internet y obliga a pensar en seguimiento.

La minimización de datos funciona como prevención. Una organización no puede perder aquello que nunca recogió. Este principio cuestiona la tendencia a almacenar “por si acaso”. La educación institucional puede pedir justificar cada categoría de información: qué función cumple y cuánto tiempo es necesaria.

El cifrado reduce exposición bajo ciertas condiciones, pero no resuelve todos los riesgos. Los datos deben descifrarse para algunos usos y las claves también necesitan protección. La pedagogía no debe presentar tecnologías como soluciones mágicas. La seguridad funciona en capas.

La responsabilidad del proveedor y la del usuario se encuentran en los puntos de configuración. Una institución puede ofrecer autenticación multifactor y el usuario no activarla; puede imponerla para reducir el riesgo. Decidir qué controles son opcionales o obligatorios es una cuestión de gobernanza.

El caso Equifax enseña finalmente que la privacidad tiene consecuencias materiales. La exposición de identificadores puede facilitar fraude y obligar a las personas a invertir tiempo en protección. Los datos no son abstractos; pueden producir costos en la vida real.

WANNACRY: SEGURIDAD COMO CONTINUIDAD Y RESPONSABILIDAD COLECTIVA

El 12 de mayo de 2017, WannaCry se propagó globalmente mediante ransomware y afectó servicios del NHS en Inglaterra. El National Audit Office documentó que al menos 81 de 236 trusts fueron afectados, además de cientos de organizaciones de atención primaria. El ataque interrumpió servicios, obligó a desviar pacientes y mostró dependencia de sistemas digitales en funciones críticas.

El hallazgo más educativo del informe es que las organizaciones afectadas compartían vulnerabilidades conocidas y podían haber reducido riesgo mediante actualizaciones y gestión de firewalls. El Department of Health había recibido advertencias previas sobre sistemas antiguos y ciberseguridad. La lección no es que “alguien no hizo clic correctamente”, sino que la seguridad depende de mantenimiento institucional.

Los sistemas heredados crean un dilema. Una organización puede depender de software antiguo porque equipos especializados no funcionan con versiones nuevas, porque migrar cuesta o porque la operación no puede detenerse. Actualizar parece una tarea técnica y puede convertirse en decisión presupuestal y de continuidad. La educación digital organizacional debe enseñar a gestionar deuda tecnológica.

Las copias de seguridad constituyen otra capa. Ransomware explota la dependencia de datos disponibles. Una copia desconectada y probada puede reducir impacto. Sin embargo, respaldar sin comprobar restauración crea una falsa sensación de seguridad. La ciberseguridad necesita procesos verificables.

La respuesta a incidentes incluye comunicación. ¿Qué servicios se detienen?, ¿quién informa?, ¿qué sistemas se aíslan?, ¿cómo se prioriza recuperación? Las organizaciones necesitan planes antes de la crisis. Esta preparación convierte seguridad en gestión de continuidad y no en asunto exclusivo del departamento de tecnología.

WannaCry también ofrece una lección para usuarios: actualizar dispositivos, desconfiar de archivos, utilizar autenticación y mantener copias son prácticas razonables. Pero el capítulo insiste en distribuir responsabilidad. Un estudiante no debe cargar con la seguridad de una plataforma educativa que la institución seleccionó; la institución debe proteger su infraestructura.

La educación digital más madura enseña una cultura de seguridad: prevención, detección, respuesta y aprendizaje. El objetivo no es vivir con miedo a cada enlace, sino construir sistemas donde un error no produzca daño desproporcionado.

Tabla 14. Dimensiones de autonomía y seguridad digital

Riesgo digital	Responsabilidad del usuario	Responsabilidad institucional
Acceso indebido	Contraseñas únicas y autenticación adicional	Gestión de accesos, monitoreo y recuperación.
Pérdida de datos	Copias personales de archivos críticos	Backups, redundancia y pruebas de restauración.
Filtración de información	Compartir solo lo necesario	Minimización, cifrado y control de proveedores.
Phishing	Verificar remitente y canal	Filtros, formación y procesos de reporte.
Sistemas vulnerables	Actualizar dispositivos propios	Inventario, parches y gestión de sistemas heredados.

Nota. Síntesis de los criterios desarrollados en este capítulo.

WannaCry ofrece además una lección sobre dependencia de software. Un sistema operativo sin soporte deja de recibir correcciones y aumenta exposición. Las organizaciones pueden mantenerlo por compatibilidad con equipos costosos o aplicaciones antiguas. Esta deuda tecnológica se acumula silenciosamente. La educación digital institucional necesita enseñar que posponer una migración es una decisión con riesgo.

La gestión de parches parece una tarea rutinaria y, precisamente por ello, suele posponerse. Actualizar puede interrumpir sistemas y generar incompatibilidades; no actualizar conserva vulnerabilidades. La gobernanza necesita ventanas de mantenimiento, pruebas y responsables. La seguridad rara vez depende de una herramienta espectacular; suele depender de disciplina operativa.

La segmentación de redes limita propagación. Aunque el estudiante general no necesita configurar una red empresarial, puede comprender el principio: un problema en una parte no debería dar acceso automático a todo. Esta idea se aplica a cuentas, permisos y almacenamiento. Separar reduce el daño de una credencial comprometida.

Las copias de seguridad requieren una regla de oro: una copia que nunca se ha restaurado es una promesa, no una garantía. Las instituciones deben probar recuperación. En el aula, el estudiante puede aprender una versión simple: conservar al menos una copia independiente de trabajos importantes y verificar que puede abrirse.

La cultura de reporte es esencial. Si un usuario teme ser castigado por haber hecho clic, puede ocultar el incidente y aumentar daño. Las organizaciones necesitan canales donde reportar rápidamente sea valorado. La seguridad madura trata el error humano como riesgo a gestionar, no como vergüenza a esconder.

El simulacro de incidente puede enseñar roles. Un grupo recibe un escenario: archivos cifrados, plataforma caída y familias esperando información. Debe decidir qué aislar, a quién informar, qué priorizar y cómo continuar la clase. La ciberseguridad se convierte en problema de organización.

WannaCry permite relacionar prevención, limitación del daño, recuperación y aprendizaje. La seguridad requiere procesos que reduzcan la probabilidad de fallo y permitan responder cuando este ocurre; una lista de prohibiciones dirigida al usuario no sustituye esa capacidad institucional.

La seguridad digital también necesita cultura de actualizaciones personales. Muchas personas posponen parches porque interrumpen tareas o temen cambios. La educación puede explicar que las actualizaciones suelen corregir vulnerabilidades, aunque también sea razonable esperar cuando una actualización crítica ha mostrado fallas. La decisión necesita información, no automatismo ciego.

Los gestores de contraseñas permiten resolver un conflicto: se recomienda usar credenciales únicas, pero recordar decenas de claves es inviable. Enseñar el principio y las herramientas disponibles evita consejos imposibles. La seguridad efectiva adapta recomendaciones a capacidades humanas.

La autenticación multifactor añade otra capa, pero no todos los métodos ofrecen la misma resistencia. La educación general no necesita jerarquías técnicas exhaustivas; puede enseñar que un segundo factor reduce riesgo y que códigos nunca deberían compartirse ante solicitudes inesperadas. La ingeniería social intenta precisamente convertir al usuario en canal de acceso.

El phishing funciona porque imita señales de autoridad y crea urgencia. Una actividad pedagógica puede comparar mensajes y pedir identificar remitente real, enlace y solicitud. El objetivo no es memorizar diseños sospechosos —que cambian—, sino verificar canal por una vía independiente.

La seguridad física del dispositivo también importa. Una pantalla sin bloqueo o un equipo compartido puede exponer información aun sin ataque remoto. La alfabetización digital reúne

seguridad técnica y hábitos cotidianos. El riesgo surge en la interacción entre ambos.

Las instituciones necesitan una cultura donde reportar errores sea rápido. Si un estudiante entrega credenciales en un sitio falso, avisar de inmediato puede permitir bloquear cuenta. Castigar automáticamente el error puede fomentar silencio. La seguridad aprende mejor de incidentes cuando existe confianza para informar.

La privacidad institucional también debe considerar el principio de menor privilegio. No todas las personas dentro de una organización necesitan acceso a todos los datos. Limitar permisos reduce exposición accidental o maliciosa. Esta idea puede enseñarse con analogías: una escuela no entrega llaves de todas las oficinas a cada miembro. Los sistemas digitales requieren una lógica semejante.

La gestión de proveedores agrega otra cadena de riesgo. Una escuela puede proteger bien su red y utilizar un servicio externo con controles deficientes. La seguridad necesita revisar contratos, prácticas y flujos de datos. Equifax muestra el daño que puede producir una organización central; los ecosistemas actuales incluyen muchas organizaciones conectadas.

Los incidentes también exigen aprendizaje posterior. Restaurar el servicio es apenas una fase. La institución necesita investigar causa, corregir controles y comunicar cambios. Sin esta etapa, la organización puede repetir el mismo patrón. La cultura de seguridad convierte cada incidente en una fuente de conocimiento.

El factor humano suele describirse como “el eslabón más débil”, una metáfora que puede ser contraproducente. Las personas también detectan anomalías, reportan mensajes y adaptan respuestas. Diseñar sistemas que dependan de comportamiento perfecto es frágil. La seguridad efectiva combina controles técnicos con usuarios capaces de reconocer y comunicar riesgos.

La formación en phishing debería evitar simulaciones humillantes. Una prueba que expone públicamente a quien cayó puede reducir confianza y hacer que futuros errores se oculten. El objetivo es aprender qué señales funcionaron y mejorar el sistema. La seguridad necesita una cultura de reporte sin vergüenza.

La continuidad académica merece un plan propio. Si una plataforma de evaluación cae durante una entrega, ¿existe otra vía? Si se pierde acceso a una cuenta, ¿puede el estudiante demostrar su trabajo? Estas situaciones muestran que la resiliencia digital también es justicia educativa: nadie debería perder una oportunidad por una falla sistémica sin alternativa.

La ciberseguridad se integra así con gobernanza, equidad y confianza. No es una competencia aislada. Un sistema seguro protege datos, pero también protege continuidad y legitimidad institucional.

6.5. CREAR, PARTICIPAR Y CONVIVIR EN ENTORNOS DIGITALES

Autoría, colaboración, bienestar y responsabilidad pública

La educación digital no termina en consumir información. También forma personas capaces de crear, colaborar y participar sin perder autoría, cuidado ni conciencia de audiencia.

CREAR DIGITALMENTE: DE PRODUCIR RÁPIDO A PRODUCIR CON TRAZABILIDAD

La facilidad de creación digital ha reducido barreras. Un estudiante puede grabar, editar, publicar y distribuir con herramientas gratuitas. Esta democratización es valiosa, pero introduce una responsabilidad sobre procedencia. Copiar, remezclar y citar necesitan reglas. Jenkins et al. (2009) describen culturas participativas donde creación y circulación forman parte del aprendizaje. La alfabetización debe incorporar ética de reutilización.

Las licencias abiertas ofrecen una vía. Creative Commons permite a autores especificar condiciones de uso mediante combinaciones reconocibles. La educación digital puede enseñar a distinguir dominio público, licencias abiertas y material protegido. El objetivo no es formar abogados de propiedad intelectual, sino evitar que “está en internet” se interprete como “puedo usarlo de cualquier manera”.

La atribución también fortalece trazabilidad. Citar una imagen, un dato o una idea permite que otros regresen a la fuente. Esta práctica conecta ética y epistemología. Cuando se pierde origen, aumenta riesgo de descontextualización y desinformación.

La colaboración digital añade gestión de versiones, permisos y autoría compartida. Un documento puede ser editado por muchas personas; saber quién cambió qué ayuda a resolver errores. El historial de versiones se convierte en memoria colectiva. La competencia incluye

acordar roles y normas de edición.

La inteligencia artificial generativa intensifica el problema de procedencia porque puede producir material sin mostrar sus fuentes. Quien utiliza una herramienta conserva responsabilidad sobre exactitud, atribución y decisiones autorales. El capítulo 11 profundiza en alfabetización en IA; aquí este criterio se integra a la creación digital responsable.

La creación también debe ser accesible. Subtítulos, textos alternativos, contraste y estructura permiten que más personas utilicen el contenido. Diseñar para diversidad transforma la competencia digital en responsabilidad social.

Crear con autonomía significa, por tanto, producir algo que puede explicarse: qué fuentes se usaron, qué herramientas intervinieron, qué derechos se respetaron y qué decisiones tomó el autor. La velocidad deja de ser el único indicador de habilidad.

La creación digital también transforma la relación con archivo y versión. Un contenido puede editarse después de publicado, pero las versiones previas quizá hayan circulado. Corregir de manera transparente —indicando qué cambió— fortalece confianza. La cultura digital tiende a premiar rapidez; la autoría responsable necesita conservar memoria de correcciones.

Las licencias abiertas pueden utilizarse como aprendizaje de agencia autorial. Elegir una licencia obliga a decidir qué usos se permiten. El estudiante deja de ser solo consumidor sujeto a derechos ajenos y se reconoce como creador con capacidad de establecer condiciones. Esta experiencia cambia la comprensión de propiedad intelectual.

La remezcla posee un valor cultural y educativo importante. Jenkins (2006) muestra cómo la convergencia y participación alteran la producción cultural. La educación no debería tratar toda reutilización como plagio ni toda copia como creatividad. Debe distinguir transformación, atribución y permisos.

Los datos también pueden ser creación. Una hoja construida por estudiantes, un mapa o un conjunto de observaciones necesita documentación. Indicar cómo se recolectaron, qué significan las columnas y qué limitaciones existen permite reutilización. La alfabetización digital incluye cultura de datos abiertos con responsabilidad.

La colaboración distribuida exige acuerdos. ¿Quién puede editar?, ¿quién aprueba la versión final?, ¿cómo se resuelve un conflicto de cambios? Los sistemas ofrecen herramientas, pero el grupo necesita gobernanza. La competencia digital colectiva se parece a una pequeña institución.

La accesibilidad debería incorporarse desde el diseño y no al final. Añadir subtítulos después de producir un video puede ser más costoso que planificarlos. Un documento con estilos de encabezado correctos facilita navegación. La inclusión digital también es una competencia de creación.

Producir con trazabilidad significa poder responder tres preguntas: de dónde viene el material, qué transformaciones se hicieron y quién asume responsabilidad. Esta estructura será particularmente importante al incorporar herramientas generativas.

CIUDADANÍA DIGITAL: PARTICIPAR SIN CONFUNDIR VISIBILIDAD CON INCIDENCIA

Choi (2016) propone comprender ciudadanía digital mediante ética, alfabetización mediática, participación y compromiso crítico. Jones y Mitchell (2016) enfatizan respeto y compromiso cívico. Estos marcos muestran que ser ciudadano digital no significa únicamente comportarse bien en línea. Incluye participar, expresarse y comprender consecuencias.

Las redes permiten organizar campañas, documentar problemas y conectar comunidades. También pueden producir una ilusión de incidencia. Una publicación con miles de interacciones puede generar conversación y no modificar una decisión institucional. La educación digital necesita distinguir expresión, movilización e incidencia. Cada una tiene valor, pero responde a objetivos diferentes.

La participación responsable requiere conocer audiencia. Un comentario en un grupo cerrado puede salir de contexto; una denuncia pública puede afectar reputación; una imagen puede identificar a personas vulnerables. La velocidad de publicación exige una pausa ética: ¿tengo permiso?, ¿qué daño podría producir?, ¿qué evidencia respalda la afirmación?

El acoso digital muestra por qué la convivencia necesita límites. Kowalski et al. (2014) sintetizaron investigación sobre cyberbullying y encontraron asociaciones con múltiples factores y consecuencias. La educación debe enseñar a documentar, bloquear, reportar y buscar apoyo. No basta con pedir a la víctima que “ignore” ni con tratar toda discusión intensa como acoso.

La moderación de comunidades puede ser una experiencia pedagógica. Los estudiantes

diseñan reglas para un foro y deben distinguir desacuerdo, insulto, amenaza, desinformación y spam. Cada categoría puede requerir respuesta distinta. Esta tarea muestra que gobernar una comunidad es más complejo que prohibir palabras ofensivas.

La ciudadanía digital también implica derechos. Privacidad, libertad de expresión y protección frente a acoso pueden entrar en tensión. La educación necesita casos donde principios se cruzan y decisiones deben justificarse. No existe una regla universal que resuelva todos los conflictos de moderación.

Participar digitalmente con madurez significa comprender que la publicación crea consecuencias para otros y para uno mismo. La autonomía se vuelve relacional: mi libertad de publicar convive con derechos, normas y audiencias.

La ciudadanía digital puede expresarse también mediante cuidado de la información común. Corregir un dato, no amplificar un rumor y citar una fuente son pequeñas acciones que mejoran el entorno. Esta perspectiva evita reducir ciudadanía a grandes campañas. La calidad del espacio digital depende de millones de prácticas ordinarias.

La identidad de grupo puede intensificar conflictos. En comunidades en línea, una crítica a una idea puede percibirse como ataque a la pertenencia. Las reglas de moderación pueden pedir responder al contenido y evitar generalizaciones sobre personas o colectivos. Esta disciplina ayuda a mantener conversaciones difíciles.

El bloqueo y la denuncia son herramientas de autoprotección, no necesariamente señales de falta de diálogo. Una persona no está obligada a exponerse a hostigamiento para demostrar apertura. La educación debe distinguir desacuerdo de conducta abusiva y enseñar rutas de apoyo.

La evidencia de cyberbullying muestra asociaciones con malestar y múltiples factores, pero las experiencias varían. Kowalski et al. (2014) advierten sobre diversidad de definiciones y métodos. La escuela necesita criterios claros para reconocer repetición, intención, desequilibrio y alcance, evitando trivializar o inflar cada conflicto.

La participación pública requiere también protección de datos de terceros. Una campaña escolar puede querer documentar un problema mediante fotografías y terminar exponiendo a personas. El consentimiento y la anonimización forman parte de la ciudadanía digital, incluso cuando la causa es legítima.

La incidencia necesita teoría de cambio. Publicar puede generar visibilidad; para modificar una política se necesita identificar quién decide, qué evidencia cuenta y qué mecanismo existe. Esta conexión con educación ciudadana evita confundir métricas de plataforma con impacto institucional.

La ciudadanía digital madura combina voz y responsabilidad. Participar no significa callar para evitar riesgos, ni publicar sin considerar consecuencias. Significa comprender el entorno y elegir formas de expresión proporcionales al objetivo.

BIENESTAR DIGITAL: MÁS ALLÁ DEL TIEMPO DE PANTALLA

El debate público sobre bienestar digital suele reducirse a horas. Esta métrica es fácil de medir y pobre para explicar. Orben y Przybylski (2019) encontraron asociaciones pequeñas entre uso de tecnología digital y bienestar adolescente, y advierten sobre problemas de medición. Odgers y Jensen (2020) revisan temores sobre adolescencia digital y concluyen que los efectos son heterogéneos. La educación debe resistir mensajes simplistas.

El contexto importa. El mismo dispositivo puede sostener amistad, juego, estudio o hostigamiento. La calidad del uso, el momento y la posibilidad de desconectar son más informativos que el tiempo total. Un estudiante puede pasar muchas horas en una herramienta de creación sin experimentar el mismo efecto que en una secuencia compulsiva de desplazamiento.

El sueño ofrece un criterio más concreto. El uso nocturno puede desplazar horas de descanso y las notificaciones pueden fragmentarlo. La educación puede trabajar con rutinas: dejar dispositivos fuera de la cama, programar modos de descanso o desactivar avisos. Estas decisiones son más accionables que una prohibición general.

La comparación social es otra dimensión. Plataformas basadas en imágenes muestran selecciones curadas de la vida ajena. La educación socioemocional puede dialogar aquí con la digital: reconocer que una publicación es representación y que métricas de aprobación pueden afectar autopercepción. El objetivo no es patologizar redes, sino crear distancia crítica.

La desconexión también puede ser un privilegio. Algunos trabajos y hogares exigen disponibilidad continua. La educación digital necesita reconocer condiciones sociales y no convertir el autocontrol en única explicación. Una organización puede establecer expectativas

razonables de respuesta y proteger tiempos de descanso.

El bienestar digital se evalúa mejor mediante preguntas funcionales: ¿interfiere con sueño?, ¿desplaza responsabilidades?, ¿produce ansiedad?, ¿permite conexión significativa?, ¿puedo detenerme cuando lo decido? Estas preguntas convierten una cifra genérica en análisis personal.

La meta no es menos tecnología por definición. Es una relación donde el usuario pueda decidir cuándo entrar, para qué permanecer y cuándo salir. Esa capacidad de gobernar atención constituye una forma central de autonomía digital.

El bienestar digital también puede analizarse desde autonomía. Si una persona planea cinco minutos y permanece una hora sin haber decidido, existe una brecha entre intención y comportamiento. Esa brecha puede explorarse sin diagnosticar adicción. La educación trabaja con objetivos, señales y configuraciones.

La gestión de notificaciones es un punto de entrada simple. Clasificar avisos en urgentes, importantes y prescindibles permite diseñar reglas. Muchas aplicaciones activan notificaciones por defecto; desactivarlas transforma el teléfono de emisor constante a herramienta consultada de forma más deliberada.

Los espacios físicos importan. Colocar el teléfono fuera del alcance durante una tarea reduce el costo de decidir repetidamente si mirarlo. La educación conductual muestra que modificar el entorno puede ser más eficaz que depender de voluntad constante. Esta idea conecta con la economía conductual del capítulo financiero.

Las plataformas de video corto presentan un flujo continuo que reduce puntos de salida. Una estrategia puede ser entrar con propósito específico o utilizar temporizadores. La educación no necesita condenar el formato; necesita observar cómo estructura el tiempo y si coincide con la intención del usuario.

El bienestar también depende de relaciones. Una comunidad digital puede ofrecer apoyo difícil de encontrar localmente. Reducir el análisis a “menos pantalla” podría eliminar un recurso importante. La calidad de conexión social necesita formar parte de la evaluación.

Las familias y escuelas deben evitar vigilancia excesiva como única respuesta. Monitorear cada acción puede deteriorar confianza y enseñar poco sobre autorregulación. Las reglas necesitan evolucionar con edad y competencia. El objetivo es que el control externo pueda disminuir a medida que aumenta capacidad interna.

La autonomía digital se reconoce cuando la persona puede explicar qué uso le aporta valor, qué señales indican interferencia y qué cambios puede realizar. Esa reflexión es más estable que cumplir un límite impuesto sin comprenderlo.

La convivencia digital necesita enseñar también reparación. Si una persona comparte información falsa o publica algo que perjudica a otra, borrar puede no ser suficiente. Reconocer error, corregir públicamente y evitar repetir puede reconstruir confianza. La cultura de internet tiende a registrar fallas; la educación puede normalizar procesos de rectificación.

La permanencia del contenido modifica las disculpas. Una corrección puede circular menos que la publicación original. Por ello, quien corrige debería hacerlo en el mismo canal y con visibilidad proporcional cuando sea posible. Esta práctica combina ética y comprensión de difusión.

El derecho al olvido, la eliminación y la memoria pública son debates complejos que varían jurídicamente. En educación general conviene evitar fórmulas. Puede trabajarse el conflicto: una persona quiere que un contenido antiguo desaparezca y otra defiende interés público. La alfabetización digital reconoce que privacidad y memoria pueden entrar en tensión.

La moderación comunitaria necesita transparencia. Si una cuenta es sancionada, conocer la regla y la posibilidad de revisión aumenta legitimidad. Esta lógica coincide con el debido proceso del capítulo jurídico. Los entornos digitales son también espacios normativos.

La colaboración en línea puede beneficiar a personas que encuentran difícil participar oralmente en clase. Foros asincrónicos ofrecen más tiempo para elaborar. Sin embargo, también pueden excluir a quienes tienen mala conectividad o habilidades de escritura limitadas. Cada formato redistribuye ventajas.

La ciudadanía digital se beneficia de repertorios múltiples: publicar, deliberar, documentar, solicitar información, crear recursos y organizar comunidades. Reducir participación a redes sociales invisibiliza otras formas de acción digital con menor visibilidad y mayor incidencia.

El bienestar digital puede trabajarse mediante diseño de rutinas colectivas. Una clase puede acordar momentos de consulta de mensajes, periodos de trabajo sin interrupción y criterios para emergencias. Después se revisa si la norma funcionó. Esta práctica convierte la autorregulación en diseño institucional y evita cargar todo sobre voluntad individual.

Las familias enfrentan un desafío semejante. Las reglas de dispositivos suelen formularse

como horarios fijos y pueden entrar en conflicto con tareas, amistades o diferencias de edad. Una aproximación educativa puede organizar la conversación alrededor de sueño, seguridad, responsabilidades y autonomía progresiva. Las reglas se justifican por función y pueden revisarse.

La comparación social necesita alfabetización visual. Una fotografía digital es selección de momento, encuadre y edición. El estudiante puede analizar cómo una serie de decisiones construye una representación sin asumir falsedad. Comprender producción reduce la tendencia a comparar la vida completa propia con una selección ajena.

El bienestar también incluye capacidad para buscar comunidades de apoyo. Jóvenes con intereses minoritarios pueden encontrar pertenencia en línea. Esta posibilidad es uno de los grandes beneficios de la conectividad y recuerda que la protección no debe convertirse en aislamiento. La educación necesita enseñar criterios para reconocer comunidades saludables y señales de riesgo.

El conflicto entre autonomía y protección cambia con la edad. Un control parental adecuado para un niño pequeño puede ser invasivo para un adolescente mayor. La competencia digital se construye cuando los controles externos disminuyen a medida que aumenta juicio. La meta no es vigilancia permanente, sino autonomía progresiva.

La escuela puede evaluar bienestar sin recopilar datos íntimos mediante escenarios y decisiones ficticias. Pedir a estudiantes que revelen horas, hábitos o conflictos personales puede crear exposición innecesaria. La educación digital debe aplicar a su propia metodología los principios de privacidad que enseña.

La relación saludable con tecnología no se mide por ausencia de problemas. Incluye capacidad de reconocer un patrón que no funciona, cambiar configuración, pedir apoyo y revisar. El bienestar se vuelve una competencia de ajuste continuo.

6.6. ENSEÑAR LO DIGITAL SIN CONVERTIRLO EN UNA LISTA DE APLICACIONES

Problemas auténticos, transferencia y gobernanza educativa

La tecnología cambia más rápido que cualquier currículo. La respuesta no es perseguir cada novedad, sino enseñar principios que permitan comprender la siguiente herramienta.

EL PROBLEMA ANTES QUE LA APLICACIÓN

Una secuencia digital profunda comienza con una tarea. “Necesitamos verificar una afirmación”, “debemos proteger una base de datos escolar”, “queremos crear un recurso accesible” o “necesitamos reducir interrupciones en un proyecto”. La herramienta aparece después. Este orden evita que el currículo dependa de marcas y convierte la tecnología en medio.

TPACK de Mishra y Koehler (2006) propuso integrar conocimiento tecnológico, pedagógico y disciplinar. El marco ha sido ampliamente utilizado y debatido, pero conserva una intuición valiosa: saber usar una herramienta no indica cómo enseñarla ni para qué contenido. La competencia docente necesita comprender la interacción.

Redecker (2017), mediante DigCompEdu, organiza competencias docentes en compromiso profesional, recursos digitales, enseñanza, evaluación, empoderamiento del alumnado y desarrollo de competencia digital. El marco evita tratar al docente como operador de software. Su trabajo incluye selección, diseño, evaluación y acompañamiento.

El GEM Report 2023 advierte que evidencia robusta sobre impacto de tecnología educativa sigue siendo limitada en muchos ámbitos y que productos cambian con rapidez. Esto exige prudencia frente a promesas comerciales. Una escuela debería preguntar qué problema resuelve la herramienta, qué evidencia existe, qué datos recoge, cuánto cuesta mantenerla y qué alternativa menos compleja existe.

La prueba piloto es una estrategia sensata. Antes de adoptar una plataforma para toda la institución, puede probarse en un grupo, definir indicadores y recoger experiencia. Si no mejora el problema, detener la expansión no es fracaso; es buena gobernanza. La educación digital también se aplica a quienes toman decisiones de compra.

La evaluación de estudiantes debe medir transferencia. Una tarea puede cambiar de herramienta y conservar el criterio. Si el estudiante solo funciona dentro de una interfaz específica, la competencia es frágil. Cambiar de plataforma permite observar qué principios comprendió.

El aprendizaje digital durable se construye cuando una persona puede explicar por qué eligió una herramienta y qué riesgos consideró. Esa explicación vale más que la velocidad con la

que navega por menús.

La selección de tecnología docente necesita considerar también carga cognitiva. Una herramienta con muchas funciones puede exigir aprendizaje que compite con el contenido. A veces una plataforma sencilla produce mejores resultados porque reduce atención a la interfaz. El principio es adecuación, no sofisticación.

La formación docente debe incluir oportunidades para experimentar como estudiante. Recibir una tarea ambigua en una plataforma, gestionar una contraseña o navegar una interfaz poco accesible ayuda a comprender fricciones. La competencia pedagógica digital no surge únicamente de tutoriales técnicos.

La evaluación automatizada necesita cautela. Puede ofrecer retroalimentación rápida y liberar tiempo, pero los criterios deben corresponder con objetivos y existir mecanismos para revisar errores. La herramienta es especialmente útil en tareas estructuradas y más limitada en producciones complejas donde el juicio contextual importa.

La privacidad educativa debe incorporarse a la selección de recursos. Una aplicación gratuita puede financiarse mediante datos o publicidad. La institución necesita comprender términos y minimizar cuentas innecesarias. El beneficio pedagógico debe compararse con exposición.

La sostenibilidad ambiental de la tecnología también merece lugar. Dispositivos, centros de datos y ciclos de reemplazo tienen impactos materiales. El GEM Report 2023 incluye sostenibilidad entre criterios para evaluar tecnología educativa. La educación digital no debería tratar la nube como infraestructura sin huella.

El soporte técnico es parte de la implementación. Una herramienta que funciona en una demostración puede fracasar cuando treinta usuarios intentan conectarse. Probar capacidad, compatibilidad y procedimientos de ayuda evita que la pedagogía dependa de condiciones ideales.

La innovación educativa digital necesita una pregunta de salida: si dejamos de usar esta herramienta, ¿qué habremos aprendido que permanece? Si la respuesta es “nada fuera de la aplicación”, el valor formativo puede ser limitado.

SEIS PROBLEMAS PARA UNA ALFABETIZACIÓN TRANSFERIBLE

El primer problema es verificación. Se entrega una publicación viral y el estudiante debe investigar fuente, evidencia, fecha y cobertura independiente. La evaluación se centra en la ruta de verificación, no solo en el veredicto. Los trabajos de McGrew y Breakstone ofrecen sustento para esta estrategia.

El segundo problema es privacidad. Una aplicación ficticia solicita permisos de ubicación, contactos, cámara y micrófono. El estudiante decide cuáles son coherentes con su función y explica riesgos. La actividad conecta datos, consentimiento y minimización sin necesitar un caso real.

El tercer problema es seguridad. Se presenta un incidente de ransomware inspirado en WannaCry y se pide construir un plan de prevención y recuperación: actualizaciones, copias, segmentación, comunicación y responsables. El caso enseña que la seguridad es organizacional.

El cuarto problema es recomendación. Dos usuarios ficticios reciben feeds diferentes. Los estudiantes analizan señales posibles y diseñan acciones para diversificar información. La tarea enseña personalización sin atribuir intenciones que no pueden probarse.

El quinto problema es creación accesible. El grupo produce un recurso con subtítulos, texto alternativo, licencias y fuentes. La calidad se evalúa por uso responsable y no solo por estética. Esta actividad integra autoría, accesibilidad y comunicación.

El sexto problema es atención. Los estudiantes registran durante varios días cuándo las notificaciones interrumpen una tarea, modifican configuraciones y comparan resultados. La experiencia funciona como pequeño experimento personal, sin convertir el bienestar en competencia moral.

Los seis problemas comparten estructura: identificar objetivo, comprender sistema, actuar, observar y revisar. Esa secuencia puede sobrevivir a la desaparición de cualquier plataforma específica.

Los problemas auténticos necesitan una línea de base. Antes de afirmar que una estrategia de atención funcionó, el grupo debe observar cómo era el patrón previo. Antes de decir que una campaña redujo phishing, conviene medir capacidad inicial para detectar mensajes. La evaluación convierte actividad digital en aprendizaje investigable.

El caso de verificación puede incorporar ambigüedad: una afirmación parcialmente

correcta, una fuente confiable que simplifica o un dato verdadero usado fuera de contexto. Los problemas más educativos no son siempre falsedades evidentes. La vida digital exige matices.

La auditoría de permisos puede compararse entre dos aplicaciones que cumplen la misma función. El estudiante pregunta cuál solicita menos información y qué características justifican diferencias. Esta comparación hace visible que el diseño tecnológico contiene decisiones sobre datos.

El ejercicio de ransomware puede incluir decisiones difíciles: apagar sistemas y suspender servicios, o intentar continuar con riesgo de propagación. La actividad enseña que seguridad tiene costos y que la preparación reduce la necesidad de improvisar bajo presión.

La recomendación algorítmica puede trabajarse sin acceder a datos personales reales mediante perfiles ficticios. Esto protege privacidad y permite explorar cómo señales distintas producen feeds distintos. La simulación enseña mecanismos sin convertir al estudiante en objeto de observación.

La creación accesible necesita usuarios de prueba. Un recurso puede cumplir una lista técnica y continuar siendo confuso. Pedir a compañeros que lo utilicen revela barreras. La accesibilidad se convierte en experiencia de diseño iterativo.

El experimento de atención debe evitar convertir datos personales en competencia pública. Cada estudiante puede analizar sus propios resultados sin publicar tiempos. La educación digital responsable protege intimidad incluso cuando estudia hábitos.

GOBERNANZA ESCOLAR: DATOS, COMPRAS, SEGURIDAD Y DERECHO A DESCONECTARSE

La educación digital no puede recaer únicamente en el aula. Las instituciones deciden plataformas, permisos, tiempos y políticas. La OECD (2023a) insiste en gobernanza del ecosistema digital. Una escuela que enseña privacidad y contrata servicios sin revisar tratamiento de datos transmite mensajes contradictorios.

La gobernanza digital educativa comienza con una pregunta de inventario: qué sistemas utiliza la institución, qué datos contienen y quién es responsable. Muchas organizaciones acumulan herramientas durante años sin una visión completa. Una aplicación adoptada por un grupo se convierte en dependencia institucional y puede continuar almacenando información después de que deja de utilizarse. El inventario es la base para seguridad, privacidad y continuidad.

La interoperabilidad introduce ventajas y riesgos. Conectar sistemas evita duplicar datos y puede facilitar seguimiento de aprendizaje. Al mismo tiempo, cada integración crea nuevas rutas de acceso. La gobernanza debe aplicar principio de necesidad: compartir aquello que cumple una función y evitar circulación simplemente porque es técnicamente posible.

La dependencia de proveedor aparece cuando contenidos, evaluaciones o historiales solo pueden extraerse en formatos cerrados. Migrar puede ser costoso y producir pérdida de información. La escuela necesita considerar portabilidad antes de adoptar. Esta decisión no es meramente técnica; afecta autonomía institucional y sostenibilidad financiera.

La evidencia sobre efectividad tecnológica merece el mismo escrutinio que cualquier intervención educativa. UNESCO (2023a) señala que la evidencia robusta es limitada en muchos ámbitos y que los productos evolucionan más rápido que su evaluación. Esto genera un mercado donde testimonios y demostraciones pueden pesar más que estudios comparativos. La alfabetización institucional consiste en formular preguntas sobre evidencia antes de comprar.

La innovación también tiene costos de oportunidad. Capacitar docentes en una nueva plataforma consume tiempo que podría destinarse a otra necesidad. Cambiar herramientas frecuentemente puede producir fatiga y reducir profundidad pedagógica. La novedad tecnológica necesita justificar por qué su beneficio compensa transición.

Los datos de estudiantes introducen responsabilidades longitudinales. Una plataforma puede registrar patrones de uso durante años. La institución debería saber cuánto tiempo conserva esa información, cómo elimina cuentas y qué ocurre cuando un estudiante se retira. La gobernanza digital necesita pensar el final del ciclo, no solo el alta.

Un ecosistema saludable conserva redundancia mínima. Si un servicio crítico falla, existe un procedimiento alternativo. La redundancia puede parecer ineficiente en tiempos normales y resultar decisiva durante una interrupción. La experiencia de pandemia y ataques informáticos mostró que continuidad educativa depende tanto de planes como de dispositivos.

La compra de tecnología debería incluir evaluación pedagógica, técnica, de seguridad y accesibilidad. El precio inicial es una parte del costo. Existen licencias, capacitación, soporte, migración y dependencia de proveedor. La alfabetización institucional significa comprender

costo total y salida.

Las cuentas de estudiantes requieren gestión de ciclo de vida. Se crean, cambian permisos y deben cerrarse cuando la relación termina. Una cuenta abandonada puede conservar datos y convertirse en riesgo. La gobernanza digital necesita procesos, no solo contraseñas.

El derecho a la desconexión puede traducirse a normas educativas sobre horarios de mensajes y expectativas de respuesta. La disponibilidad permanente no mejora necesariamente aprendizaje. Definir franjas y urgencias reduce ansiedad y ayuda a diferenciar comunicación institucional de mensajería instantánea.

La respuesta a incidentes debe estar ensayada. ¿A quién reporta un estudiante un correo sospechoso?, ¿qué ocurre si se filtra información?, ¿quién comunica a familias? Un protocolo sencillo vale más que una política extensa desconocida. La seguridad necesita rutas.

La participación estudiantil puede mejorar gobernanza. Quienes usan plataformas diariamente detectan fricciones que administradores no ven. Consultar no significa delegar decisiones técnicas, pero aporta experiencia. La ciudadanía digital también se aprende participando en reglas del entorno.

Una institución digitalmente madura conserva alternativas. Puede exportar datos, continuar temporalmente sin una plataforma y cambiar de proveedor. La resiliencia protege autonomía colectiva del mismo modo que la alfabetización protege autonomía personal.

Tabla 15. Evidencias para evaluar la competencia digital

Problema educativo	Capacidad central	Producto de aprendizaje
Noticia viral	Lectura lateral y trazabilidad	Informe de verificación con fuentes.
App con permisos	Privacidad y minimización	Auditoría de datos y decisión justificada.
Ransomware escolar	Seguridad y continuidad	Plan de prevención, respuesta y recuperación.
Feed personalizado	Alfabetización algorítmica	Explicación de señales y estrategia de diversificación.
Recurso multimedia	Autoría y accesibilidad	Contenido con licencias, fuentes y diseño inclusivo.
Sobrecarga de notificaciones	Autogestión de atención	Experimento de configuración y reflexión.

Nota. Síntesis de los criterios desarrollados en este capítulo.

La revisión tecnológica institucional necesita criterios públicos de finalidad, accesibilidad, seguridad, privacidad, costo y portabilidad. El inventario de sistemas permite identificar dependencias; un procedimiento periódico permite revisar si continúan justificadas. La consulta a docentes y estudiantes aporta evidencia de uso, sin sustituir la evaluación técnica ni las responsabilidades de quienes deciden.

La carga de trabajo debe formar parte del análisis. Una plataforma puede reducir una tarea y aumentar registros o mensajes en otra. La evaluación necesita observar tiempo, comprensión de retroalimentación y barreras, además de actividad o número de cuentas. Las familias requieren información clara sobre finalidad, canales legítimos y soporte. La transformación digital no se demuestra únicamente por adopción.

La continuidad se prueba con ejercicios seguros: recuperar un archivo de prueba, ensayar una comunicación de interrupción o verificar una alternativa de entrega. La institución registra qué falló y quién debe corregirlo. Conservar memoria de decisiones, incidentes y cambios evita que cada renovación de personal reinicie el aprendizaje. Los criterios de salida y eliminación de cuentas deben acordarse desde la entrada.

El currículo puede distinguir principios duraderos de procedimientos que envejecen rápido. Verificación, privacidad, atención, seguridad, autoría y accesibilidad forman un núcleo transferible; rutas de menú y nombres de aplicaciones sirven como ejemplos temporales. Lenguaje, ciencias, sociales, tecnología, artes y orientación pueden trabajar esas capacidades desde problemas propios. La formación docente se fortalece mediante comunidades de práctica que comparten dudas y soluciones, sin exigir dominio completo de todas las herramientas.

Retirar una plataforma puede ser una decisión madura cuando la evidencia no justifica su continuidad. La evaluación debe preguntar qué capacidad desarrollaron las personas, qué dependencia se creó y qué riesgos o inequidades aparecieron. Los capítulos 6 y 11 comparten esa preocupación por el juicio: la generación automatizada de contenido agrega exigencias de procedencia, evaluación y responsabilidad, dentro de un ecosistema que ya contiene condiciones de acceso y gobierno. La aplicación siguiente muestra cómo traducir estos criterios en una decisión revisable.

APLICACIÓN ILUSTRATIVA: SELECCIONAR UNA HERRAMIENTA SIN PERDER AUTONOMÍA INSTITUCIONAL

Esta aplicación ilustrativa plantea una decisión de gobernanza escolar: seleccionar un medio para recibir trabajos y ofrecer retroalimentación. El escenario ficticio dispone de tres alternativas: una plataforma comercial con funciones automáticas, un servicio sencillo de archivos y comunicación ya utilizado, o una combinación de entregas presenciales y archivos con criterios comunes. Ninguna se presenta como ganadora. La tarea es justificar qué opción responde mejor a una necesidad definida y bajo qué condiciones podría probarse. No se simulan resultados de adopción ni se usan datos de estudiantes reales. La secuencia puede ocupar cinco sesiones y un ensayo controlado con materiales ficticios.

El docente proporciona una ficha de tarea —quién entrega, quién revisa, cuándo y qué evidencia de recepción se necesita—; descripciones equivalentes de las tres opciones; un aviso de privacidad ficticio; condiciones de exportación y cierre; un presupuesto de ejercicio; y cuatro perfiles de uso. Los perfiles describen restricciones funcionales sin etiquetar personas: conexión intermitente, dispositivo compartido, uso de lector de pantalla y disponibilidad limitada de tiempo. También se entrega un archivo de prueba con nombres inventados y contenidos no sensibles. Todas las características de los servicios se identifican como datos del escenario, sin atribuirlos a marcas reales.

En la primera sesión, el grupo convierte la necesidad en requisitos observables. Debe poder entregar un archivo, comprobar recepción, acceder a una devolución, corregir una versión y recuperar el trabajo. Añade restricciones de accesibilidad, soporte, carga docente y privacidad. Separar requisito de función atractiva evita elegir por novedad. Una herramienta con más botones puede no resolver mejor la tarea. El equipo define qué información permitiría comparar opciones y qué afirmaciones de sus descripciones son promesas que todavía requieren prueba. Este paso articula acceso del acápite 6.1 y verificación del 6.2.

La segunda sesión reconstruye el flujo de información. Para cada alternativa, una hoja de inventario registra dato solicitado, finalidad, persona o entidad que accede, lugar de almacenamiento según el material, duración y condición de eliminación. Si el aviso no proporciona una respuesta, la casilla no se completa por plausibilidad: se convierte en consulta al proveedor ficticio. El equipo cuestiona cuentas o permisos que no cumplen una función clara. No descarga herramientas desconocidas ni introduce credenciales reales. La privacidad del acápite 6.4 se practica como análisis de decisiones de diseño, además de hábito personal.

La tercera sesión prepara un ensayo de usabilidad con los perfiles. Cada participante realiza las mismas tareas con archivos de prueba y anota pasos, obstáculos, solicitud de ayuda y forma de recuperar una versión. Un equipo puede diseñar en papel las pantallas de una alternativa y explicar qué no puede evaluar con ese recurso. Cuando hay una prueba funcional, las observaciones se identifican como registros del ensayo y no como evidencia de eficacia educativa. Se comprueba si una persona puede obtener la información necesaria mediante el formato que utiliza; una lista de funciones accesibles no sustituye esa observación.

La cuarta sesión examina continuidad y salida. El grupo recibe un aviso ficticio de interrupción del servicio y decide cómo mantener entregas y devoluciones sin perder trazabilidad. Debe señalar quién comunica, qué canal alternativo se usa, cómo se reconoce una entrega y qué registros se conservan. Después intenta recuperar los archivos de prueba en un formato reutilizable o especifica el procedimiento que tendría que verificar. La alternativa se evalúa desde el ciclo completo: entrada, uso, corrección y salida. Esta exigencia convierte portabilidad y respaldo en parte de la selección, sin suponer que toda dependencia puede eliminarse.

La comparación final incluye beneficio para la tarea, barreras, datos, costo total, soporte y reversibilidad. El presupuesto del ejercicio debe distinguir adquisición, tiempo de formación, mantenimiento y migración; no se afirma que una opción sin pago directo carezca de costo. Cada equipo declara sus prioridades antes de valorar las alternativas y presenta una objeción a su propia recomendación. Una decisión puede favorecer un servicio sencillo si reduce cargas o una herramienta más compleja si aporta una capacidad necesaria y verificable. La calidad del argumento depende de correspondencia con la necesidad, no del grado de sofisticación tecnológica.

La quinta sesión redacta un plan de piloto institucional. El documento define alcance, participantes ficticios, tareas, responsables, criterios de revisión y condiciones para continuar, modificar o detener. La eventual adopción corresponde a la institución competente; el grupo no suscribe contratos ni crea cuentas reales por iniciativa del ejercicio. Los indicadores propuestos deben permitir observar recepción, comprensión de retroalimentación, barreras y carga de

trabajo. Se distingue actividad en la plataforma de aprendizaje: contar accesos no demuestra que una devolución haya sido comprendida o utilizada. Si una función de IA interviene, el plan añade revisión humana, procedencia y límites, en relación con el capítulo 11.

El producto es un informe de decisión con requisitos, inventario de datos, protocolo y registros del ensayo, comparación de alternativas, plan de continuidad y salida, y propuesta de piloto. La evaluación usa cuatro criterios con igual peso: adecuación a la tarea, trazabilidad de pruebas, consideración de diversidad y privacidad, y reversibilidad de la decisión. Cada criterio se clasifica como insuficiente, explicado o demostrado con límites explícitos. La regla es pedagógica y no una certificación técnica. Inventar pruebas, ocultar una restricción decisiva o utilizar datos reales no autorizados exige rehacer el informe. La devolución final identifica qué puede sostenerse con los materiales y qué consulta especializada o prueba adicional se requiere antes de adoptar.

CONCLUSIÓN. GOBERNAR EL PROPIO USO EN UN ECOSISTEMA QUE TAMBIÉN NOS GOBIERNA

La educación digital busca transformar acceso y uso en capacidad de juicio. Conectividad, dispositivo, habilidades, soporte, accesibilidad y condiciones sociales se combinan. Un recurso disponible puede seguir siendo difícil de utilizar. La autonomía requiere que la persona pueda realizar tareas significativas, reconocer límites propios y obtener ayuda sin asumir cargas desproporcionadas.

La abundancia de información exige construir confianza. Buscar, verificar, rastrear y comparar necesitan enseñanza explícita; la familiaridad con internet no garantiza estas capacidades. Las plataformas añaden selección, incentivos y métricas que influyen en atención y visibilidad. Comprender cómo una representación se produce permite utilizarla sin confundir popularidad con evidencia ni un flujo personalizado con la realidad completa.

Privacidad, seguridad y convivencia reúnen responsabilidades personales e institucionales. Equifax y WannaCry muestran límites del control del usuario y la importancia de mantenimiento, gobernanza y continuidad. Crear y participar exige atribución, accesibilidad y cuidado de terceros. El bienestar depende de función, contexto y capacidad de regular el uso; una cifra universal de tiempo no describe todas las experiencias ni reemplaza apoyo cuando existe interferencia significativa.

La autonomía también incluye revisar una elección y poder salir. Conservar copias, documentar configuraciones, utilizar formatos interoperables cuando sea posible y verificar exportación disminuye el costo de cambiar. Las instituciones necesitan pensar en portabilidad, cierre de cuentas y alternativas desde la adopción. La atención requiere oportunidades de desconexión acordes con las tareas y las condiciones sociales. La reversibilidad convierte una decisión tecnológica en una opción que puede evaluarse y corregirse.

El capítulo 6 propone capacidades transferibles: verificar, proteger, comprender mediaciones, crear con trazabilidad y elegir según propósito. Los problemas del acápite 6.6 permiten practicar esas decisiones con criterios observables. El capítulo 11 retoma estas bases para examinar sistemas que generan contenido y participan en tareas cognitivas. La meta educativa es que personas e instituciones puedan explicar sus decisiones, reconocer dependencias y revisar efectos, en lugar de adoptar cada novedad como prueba automática de progreso.

REFERENCIAS

- Almatrafi, O., Johri, A., & Lee, H. (2024). A systematic review of AI literacy conceptualization, constructs, and implementation and assessment efforts (2019–2023). *Computers and Education Open*, 6, 100173. <https://doi.org/10.1016/j.caeo.2024.100173>
- Alter, A. (2017). *Irresistible: The rise of addictive technology and the business of keeping us hooked*. Penguin Press.
- Bakshy, E., Messing, S., & Adamic, L. A. (2015). Exposure to ideologically diverse news and opinion on Facebook. *Science*, 348(6239), 1130–1132. <https://doi.org/10.1126/science.aaa1160>
- boyd, d. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.
- boyd, d., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210–230. <https://doi.org/10.1111/j.1083-6101.2007.00393.x>
- Breakstone, J., Smith, M., Wineburg, S., Rapaport, A., Carle, J., Garland, M., & Saavedra, A. (2021). Students' civic online reasoning: A national portrait. *Educational Researcher*, 50(8), 505–515. <https://doi.org/10.3102/0013189X211017495>
- Buckingham, D. (2007). Digital media literacies: Rethinking media education in the age of the Internet. *Research in Comparative and International Education*, 2(1), 43–55.
- Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.
- Caulfield, M., & Wineburg, S. (2023). *Verified: How to think straight, get duped less, and make better decisions about what to believe online*. University of Chicago Press.
- Choi, M. (2016). A concept analysis of digital citizenship for democratic citizenship education in the internet age. *Theory & Research in Social Education*, 44(4), 565–607. <https://doi.org/10.1080/00933104.2016.1210549>
- Citton, Y. (2017). *The ecology of attention*. Polity.
- Cotter, K. (2019). Playing the visibility game: How digital influencers and algorithms negotiate influence on Instagram. *New Media & Society*, 21(4), 895–913. <https://doi.org/10.1177/1461444818815684>
- Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.
- Creative Commons. (s. f.). *About CC licenses*.
- Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. *Journal of Educational Multimedia and Hypermedia*, 13(1), 93–106.
- European Commission. (2022a). *Ethical guidelines on the use of artificial intelligence and data in teaching and learning for educators*. Publications Office of the European Union.
- European Commission. (2022b). *Guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training*. Publications Office of the European Union.
- Eyal, N. (2014). *Hooked: How to build habit-forming products*. Portfolio.
- Federal Trade Commission. (2019a). *Equifax to pay \$575 million as part of settlement with FTC, CFPB, and states related to 2017 data breach*.
- Fogg, B. J. (2003). *Persuasive technology: Using computers to change what we think and do*. Morgan Kaufmann.
- Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
- Hargittai, E. (2002). Second-level digital divide: Differences in people's online skills. *First Monday*, 7(4). <https://doi.org/10.5210/fm.v7i4.942>
- Helsper, E. J. (2021). *The digital disconnect: The social causes and consequences of digital inequalities*. SAGE.
- Hobbs, R. (2010). *Digital and media literacy: A plan of action*. Aspen Institute.
- International Telecommunication Union. (2023). *Facts and figures 2023*. ITU.
- Jenkins, H. (2006). *Convergence culture: Where old and new media collide*. New York University Press.
- Jenkins, H., Purushotma, R., Weigel, M., Clinton, K., & Robison, A. J. (2009). *Confronting the challenges of participatory culture: Media education for the 21st century*. MIT Press.
- Jones, L. M., & Mitchell, K. J. (2016). Defining and measuring youth digital citizenship. *New Media & Society*, 18(9), 2063–2079. <https://doi.org/10.1177/1461444815577797>
- Kahne, J., & Bowyer, B. (2017). Educating for democracy in a partisan age: Confronting the challenges of motivated reasoning and misinformation. *American Educational Research Journal*, 54(1), 3–34. <https://doi.org/10.3102/0002831216679817>
- Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073–1137. <https://doi.org/10.1037/a0035618>
- Livingstone, S. (2004). Media literacy and the challenge of new information and communication technologies. *The Communication Review*, 7(1), 3–14.
- Livingstone, S., & Helsper, E. J. (2007). Gradations in digital inclusion: Children, young people and the digital divide. *New Media & Society*, 9(4), 671–696. <https://doi.org/10.1177/1461444807080335>
- McGrew, S. (2020). Learning to evaluate: An intervention in civic online reasoning. *Computers & Education*, 145, 103711. <https://doi.org/10.1016/j.compedu.2019.103711>
- McGrew, S., Breakstone, J., Ortega, T., Smith, M., & Wineburg, S. (2018). Can students evaluate online sources? Learning from assessments of civic online reasoning. *Theory & Research in Social Education*, 46(2), 165–193. <https://doi.org/10.1080/00933104.2017.1416320>
- McGrew, S., Smith, M., Breakstone, J., Ortega, T., & Wineburg, S. (2019). Improving students' web savvy: An

- intervention study. *British Journal of Educational Psychology*, 89(3), 485–500. <https://doi.org/10.1111/bjep.12279>
- Metzger, M. J., Flanagin, A. J., & Medders, R. B. (2010). Social and heuristic approaches to credibility evaluation online. *Journal of Communication*, 60(3), 413–439. <https://doi.org/10.1111/j.1460-2466.2010.01488.x>
- Mishra, P., & Koehler, M. J. (2006). Technological pedagogical content knowledge: A framework for teacher knowledge. *Teachers College Record*, 108(6), 1017–1054.
- Napoli, P. M. (2019). *Social media and the public interest: Media regulation in the disinformation age*. Columbia University Press.
- National Audit Office. (2017). *Investigation: WannaCry cyber attack and the NHS*. UK
- Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education*, 59(3), 1065–1078. <https://doi.org/10.1016/j.compedu.2012.04.016>
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- Odgers, C. L., & Jensen, M. R. (2020). Annual research review: Adolescent mental health in the digital age: Facts, fears, and future directions. *Journal of Child Psychology and Psychiatry*, 61(3), 336–348. <https://doi.org/10.1111/jcpp.13190>
- OECD. (2021a). *Children & young people's mental health in the digital age*.
- OECD. (2023a). *OECD Digital Education Outlook 2023: Towards an effective digital education ecosystem*. OECD Publishing. <https://doi.org/10.1787/c74f03de-en>
- Ophir, E., Nass, C., & Wagner, A. D. (2009). Cognitive control in media multitaskers. *Proceedings of the National Academy of Sciences*, 106(37), 15583–15587. <https://doi.org/10.1073/pnas.0903620106>
- Orben, A., & Przybylski, A. K. (2019). The association between adolescent well-being and digital technology use. *Nature Human Behaviour*, 3, 173–182. <https://doi.org/10.1038/s41562-018-0506-1>
- Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin Press.
- Potter, W. J. (2010). The state of media literacy. *Journal of Broadcasting & Electronic Media*, 54(4), 675–696.
- Redecker, C. (2017). *European framework for the digital competence of educators: DigCompEdu*. Publications Office of the European Union.
- Ribble, M. (2015). *Digital citizenship in schools: Nine elements all students should know* (3rd ed.). ISTE.
- Scolari, C. A. (Ed.). (2018). *Teens, media and collaborative cultures: Exploiting teens' transmedia skills in the classroom*. Universitat Pompeu Fabra.
- Selwyn, N. (2016). *Education and technology: Key issues and debates* (2nd ed.). Bloomsbury.
- Selwyn, N. (2022). *Education and technology: Key issues and debates* (3rd ed.). Bloomsbury.
- UNESCO. (2023a). *Global Education Monitoring Report 2023: Technology in education: A tool on whose terms?*
- UNESCO. (2023b). *Guidance for generative AI in education and research*.
- UNESCO. (2024a). *AI competency framework for students*.
- van Deursen, A. J. A. M., Helsper, E. J., Eynon, R., & van Dijk, J. A. G. M. (2017). The compoundness and sequentiality of digital inequality. *International Journal of Communication*, 11, 452–473.
- van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2014). The digital divide shifts to differences in usage. *New Media & Society*, 16(3), 507–526.
- van Dijk, J. (2020). *The digital divide*. Polity.
- Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens*. Publications Office of the European Union. <https://doi.org/10.2760/115376>
- Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe.
- Warschauer, M. (2004). *Technology and social inclusion: Rethinking the digital divide*. MIT Press.
- Wineburg, S., McGrew, S., Breakstone, J., & Ortega, T. (2016). *Evaluating information: The cornerstone of civic online reasoning*. Stanford History Education Group.
- Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.