El fomento de la privacidad en internet requiere una responsabilidad digital compartida entre todos los actores sociales involucrados, entre los que los niños y adolescentes deben jugar un papel activo esencial, debiendo ser considerados como ciudadanos digitales en un mundo hiperconectado.

[ILUSTRACIÓN: CLU/ ISTOCK]

Cuando hablamos de ciudadanía, solemos pensar en derechos y deberes, aunque pocas veces nos paramos a analizar su significado e implicaciones. El concepto se remonta en Occidente a los tiempos de la Antigua Grecia, en el marco de la participación directa en las decisiones que afectaban a la colectividad.

Entre las dimensiones sobre qué es un ciudadano, se encuentran la política, la social, la cultural o la subjetiva, entre otras, que definen el conjunto de derechos, deberes, percepciones, responsabilidades y comportamientos sobre un conjunto de personas. Así pues, la ciudadanía digital no es solo un conjunto de habilidades técnicas, sino una forma de participación activa, crítica y responsable en la vida pública digital.

El contexto: ciudadanos de un mundo hiperconectado

¿Por qué es importante comenzar con esta aclaración? Porque el concepto "menor de edad" diluye las características y homogeneiza a todos aquellos niños y adolescentes que aún no han cumplido una determinada edad, sin matices. En el ámbito digital, además, en ocasiones, se vincula a una connotación infantilizadora que se orienta hacia la mera protección del niño o adolescente, sin una participación activa del mismo.

Basta con recalcar que, entre las concepciones sociales para potenciar su privacidad, destaca la insistencia en el reforzamiento de protocolos de seguridad para acceder a plataformas online o a contenido considerado perjudicial para su desarrollo. Por ejemplo, podemos encontrar la propuesta de implementar sistemas de verificación de edad para impedir el acceso a plataformas pornográficas –recordemos que en España la edad de acceso a este contenido llega a situarse en los 8 años–.

Y es que el mayor riesgo en lo digital es la propia persona. No podemos olvidar que, detrás de un ciberataque hay un autor, y detrás de cada pantalla atacada hay una víctima. En cuestiones digitales, se dice que el principal factor de riesgo no es la herramienta –la tecnología– en sí, sino el factor humano. De hecho, hasta el 95% de los fallos de ciberseguridad tienen su origen en errores humanos. Por tanto, debemos tener una perspectiva social sobre la utilización de la tecnología: las herramientas digitales son medios, por y para personas.

Tampoco podemos –ni debemos– caer en el alarmismo generalizado que establece una relación causal entre la utilización de pantallas y redes sociales y consecuentes problemas en las personas, especialmente niños, adolescentes y jóvenes. Así lo muestra un estudio de Nature Human Behaviour, que señala que el riesgo del uso de la tecnología en jóvenes es, en todo caso, bajo y muy variado. En caso de materialización, los autores explican que no se relaciona de manera directa con el simple uso de la tecnología, entendido como las horas de pantalla, sino con variables moduladoras como el género, la edad o la supervisión parental.

Considerar a jóvenes como ciudadanos digitales implica su derecho a participación y expresión

Por tanto, abordar la privacidad y las posibles amenazas que conlleva la utilización de internet requiere una visión que integre a todo el conjunto de la sociedad, con especial atención a todos aquellos grupos más vulnerables. Considerar a los niños y jóvenes como ciudadanos digitales implica su derecho a participación y expresión, no como meros receptores de medidas coercitivas o de protección pasiva.

El dilema: la huella digital que siempre nos sigue

El desarrollo exponencial de internet y las redes sociales durante las últimas décadas ha supuesto una interconexión global sin precedentes, con numerosas ventajas e inconvenientes. Entre las ventajas, podemos destacar la democratización del conocimiento, las facilidades de comunicación o entretenimiento o los avances en múltiples campos de conocimiento científico.

En cambio, el acceso a redes sociales, especialmente para niños y adolescentes, ha ampliado el concepto de seguridad hacia nuevos horizontes que, hasta hace pocas décadas, no se contemplaban. Un ejemplo es el impacto de la huella digital, entendida como el rastro de información que dejamos en internet de manera voluntaria o involuntaria con cada foto, ubicación, búsqueda o comentario.

Un reciente estudio español ha revelado que el 62 % de adolescentes encuestados asegura entender el tipo de información que comparte en las plataformas y un 46 % ha mostrado preocupación por su huella digital; sin embargo, más de la mitad afirma no conocer cómo proteger su información personal en las redes.

El contenido que volcamos en internet, en general, no sale nunca de internet

El contenido que volcamos en internet, en general, no sale nunca de internet. Y esta exposición prolongada puede dar pie a problemas graves. En edades tempranas, el ciberacoso, es decir, el hostigamiento facilitado por el uso de nuevas tecnologías con el objetivo de atemorizar, humillar o ejercer algún tipo de daño a otras personas, es una de las principales amenazas derivadas de la utilización de redes sociales. Son múltiples los casos que podríamos destacar, pero el ejemplo de Kayla Laws, una joven estadounidense que se vio sometida a un proceso de "pornovenganza", muestra su impacto a diferentes niveles: individualmente, por los mensajes e insultos recibidos durante meses y que llegaron a traspasar el ámbito digital; socialmente, por el debate existente en torno a la privacidad y el intercambio de fotografías y vídeos de contenido sexual; y tecnológicamente, por el impacto que supuso la huella digital, que escapó del control de la víctima y fue utilizada en su contra.

Además, la persistencia de la huella digital deriva en numerosas implicaciones para cualquier persona, tanto en el presente como en el futuro: la reputación online influye cada vez más en procesos de selección de empleo, becas o admisión en universidades.

El reto: crear responsabilidad digital compartida

Agrupando estas ideas –tecnología producida por y para humanos, con errores humanos y que debe contar con una participación activa de todos los humanos–, resulta evidente que la línea a seguir no se orienta hacia la prohibición en el acceso a internet o las redes sociales, sino hacia la educación en su uso. La educación digital no puede limitarse a evitar daños. Debe aspirar a empoderar a una generación que puede ser nativa, pero no por ello necesariamente competente en la materia.

La mera prohibición impide o, al menos, dificulta el correcto desarrollo de competencias digitales, que además son clave para el futuro. La alfabetización digital, más allá de la seguridad en las contraseñas o el

conocimiento sobre la utilización de software, debe incluir la correcta gestión de la identidad digital y la prevención de amenazas, como el ciberacoso, el grooming o la recopilación de información personal para utilizarla con fines de ingeniería social.

En este sentido, el framework de competencias digitales propuesto por el Joint Research Centre y la Comisión Europea (DigComp) orienta estos esfuerzos en una de las prioridades del continente: la transición hacia la era digital. Así, proponen que los ciudadanos deben contar con una serie de competencias que se enmarcan en cinco dimensiones: seguridad, alfabetización de información, creación de contenido digital, solución de problemas y, por último, comunicación y colaboración (Joint Research Centre, 2022). Es en esta última dimensión sobre la que recae la principal responsabilidad sobre la educación digital, ya que educar en ciudadanía digital supone enseñar a convivir en un espacio donde lo tecnológico y lo social son inseparables.

La construcción de esta responsabilidad digital involucra la participación de múltiples actores y sectores: desde el familiar y educativo, para dotar de herramientas y conocimiento crítico sobre las redes sociales, hasta las organizaciones privadas, para integrar la privacidad en el diseño de plataformas seguras, siguiendo el marco privacy by design, es decir, diseñado para priorizar por defecto la privacidad del usuario.

Hacer de internet un espacio de oportunidad, no un lugar de vulnerabilidad permanente

En definitiva, necesitamos hacer de internet un espacio de oportunidad, participación y crecimiento, no un lugar de vulnerabilidad permanente. Si queremos una sociedad justa, segura y democrática, debemos formar ciudadanos críticos para navegar en esta compleja era tecnológica.