La tecnología hecha por y para humanos necesita precisamente la humanidad, el valor de las ciencias sociales y las artes propias de las personas para poner al ser humano en el verdadero centro de su propia (r)evolución.

A menudo dividimos el mundo profesional según el conocimiento experto de dos categorías considerándolas erróneamente excluyentes: *ciencias y letras*; esta dicotomía nos llevaría irremediablemente a pensar que en la era digital en la que nos encontramos no se necesita gente de letras, nada más lejos de la realidad.

Entre otros muchos, Bill Aulet, director general de *The Martin Trust for MIT Enterpreneurship*, Mariano Belinki, CEO de *Santander Global Asset Management* o Scott Hartley, inversor de riesgo en Silicon Valley insisten en que las humanidades, las ciencias sociales y las artes liberales son ahora más relevantes que nunca precisamente por el desarrollo tecnológico exponencial.

Lo cierto es que dividir el entorno profesional en *ciencias y letras* es una clasificación ya en origen errónea, y la mejor muestra de ello es la necesidad de expertos considerados *fuzzys*[1] que, desde los profesionales de las TIC y particularmente la ciberseguridad, se está explicitando.

Si las tecnologías son efectivamente creadas por personas, llevarán implícitas las imperfecciones y sesgos propias de su condición

En realidad, si las tecnologías son creadas por y para las personas, resultaría lógico pensar que las SSH[2] deben ser parte clave tanto en su creación como en su uso. Tal y como recuerda la Comisión Europea[3], las SSH abarcan una amplia gama de disciplinas como la sociología, la economía, la psicología, la ciencia política, la historia y las ciencias culturales, el derecho y la ética, campos esenciales del conocimiento desde los que se apoyan tanto la elaboración de políticas basadas en evidencias como el diseño de las soluciones ante los problemas sociales y tecnológicos en la actualidad.

Es más, cabe decir que, si las tecnologías son efectivamente creadas por personas, llevarán implícitas las imperfecciones y sesgos propios de su condición. Una clara muestra de ello es el problema existente con los datos que nutren los algoritmos, por ejemplo, en los sistemas biométricos: los modelos dedicados a la detección, identificación y verificación en los sistemas de reconocimiento facial realizan clasificaciones erróneas en función del color de la piel, la edad y el sexo de los individuos (Cámara y Jordá, 2020). En este sentido, especial interés reviste el informe AI100 (2021) sobre 100 años de inteligencia artificial y cuyas conclusiones, una vez más, inciden en la ineludible obligación de incluir áreas de investigación vinculadas con las humanidades y muy especialmente con las ciencias sociales para ampliar las posibilidades futuras de esta tecnología, tanto para minimizar los impactos negativos en la sociedad como para potenciar los positivos.

La integración efectiva de la SSH es, por tanto, un determinante clave del impacto social en el desarrollo tecnológico, pues resulta fácilmente imaginable la infinidad de problemas sociales, jurídicos y éticos derivados

de la discriminación implícita en la aplicación de determinadas tecnologías disruptivas ante diversos retos sociales: desde la falta de higiene democrática de unas elecciones o la potenciación de los discursos de odio, hasta la discriminación racial y étnica en la prevención del delito o la discriminación de género en el entorno laboral. Resulta que no se trata de un ejercicio de prospectiva, todos estos efectos ya se han constatado[4].

Los músicos son profesionales con especial potencial de éxito como analistas de ciberseguridad

Sin restar importancia a los relevantes avances tecnológicos, eminentemente positivos[5], sin duda se producirán resultados más alentadores si integramos todas las disciplinas involucradas en cada nuevo paso. En este sentido, es relevante construir un proceso de co-diseño que reconozca y aborde las habilidades que cada nueva propuesta requiera, ya sea un proyecto de investigación, una herramienta digital o una solución tecnológica a una necesidad social. Buena señal de esta necesidad es la breve y dramática historia de Spot, el perro robot de la policía de NYPD que comenzó a patrullar en febrero de 2021 y que fue rápidamente sacrificado a las pocas semanas al considerarse terrorífico y espeluznante por la ciudadanía[6]. En este caso podemos ver que la seguridad depende de una serie de factores humanos y de cuestiones sociales y culturales, como la confiabilidad, y de forma específica estas disciplinas propias de las letras son necesarias para analizar las interacciones persona-máquina.

Del mismo modo, el uso de inteligencia artificial para la manipulación de imágenes abre un mundo nuevo en el entorno del marketing y la cinematografía[7], y específicamente en para su vertiente más oscura necesita de expertos en comunicación, periodismo, criminología o psicología para detectar malos usos. De hecho, en el entorno concreto de la ciberseguridad, *soft skills* como la creatividad, el pensamiento crítico o el trabajo en equipo son elementos centrales para garantizar una mayor protección. Así, David Tudehope, director general de *Macquarie Telecom Group*, señala a los músicos como profesionales con especial potencial de éxito como analistas de ciberseguridad o cazadores de amenazas dadas sus destacadas capacidades en la detección de rarezas en patrones de conducta[8].

En materia de ciberincidentes, IBM no se ha cansado de repetir en sus informes anuales desde 2009 que más del 90% de ellos se debe a errores humanos (*IBM X-Force Threat Intelligence Index*, 2009-2020). Estos datos ponen de manifiesto que la seguridad informática no se limita a la tecnología y los sistemas, también se trata de las personas que utilizan esos sistemas y de cómo sus comportamientos vulnerables pueden derivar en graves consecuencias; lo cual nos lleva irremediablemente a considerar la seguridad como parte necesaria de la cultura de empresa, donde los factores psicológicos, sociales y legales juegan un papel trascendental. Pues bien, si el mejor cortafuegos humano en ciberseguridad es la formación y la concienciación, entonces expertos en educación y en comunicación tendrían un valor extraordinario a la hora de diseñar e implementar ese tipo de dinámicas. Así, en los equipos de trabajo, cuanta mayor diversidad haya, más herramientas de protección tendrá la organización a su disposición.

No hay revolución sin cultura, y la revolución digital será humana o no será.

En conclusión, la tecnología, que siempre es un medio, tiene como origen y fin el ser humano; por ello, las disciplinas humanas y sociales son una parte más del engranaje de conocimientos sobre el desarrollo tecnológico que forma parte de evolución humana en la IV Revolución Industrial[9]. Por tanto, para situar verdaderamente al ser humano en el centro deberemos apoyarnos de las perspectivas que las SSH nos aportan. No hay revolución sin cultura, y la revolución digital será humana o no será.