UNIVERSIDAD Rafael Belloso Chacín

Revista Electrónica de Estudios Telemáticos
TÉLÉMATIQUE

Editorial

En la era digital actual, la frontera entre el código y la mente se ha vuelto casi imperceptible, transformando la seguridad digital en un campo de batalla donde la Inteligencia Artificial (IA) y las ciencias cognitivas convergen para disputar el control de la verdad. Esta rápida evolución tecnológica no solo redefine nuestra interacción con la tecnología, sino que plantea desafíos urgentes que obligan a establecer nuevas normas éticas para proteger, más allá de la integridad de los datos, la propia autonomía de la voluntad humana.

Si bien la IA ha revolucionado áreas críticas como la seguridad digital mediante la respuesta automatizada y la optimización de procesos en diferentes áreas del saber, su implementación conlleva el riesgo de la opacidad algorítmica. Esta capacidad de decisión autónoma, aunque eficiente, plantea serias preocupaciones éticas; si los sistemas se entrenan con datos sesgados, pueden transformar una mejora en la calidad de vida, en una herramienta que perpetúe desigualdades y vulnere derechos fundamentales.

Por otra parte, las ciencias cognitivas, encargadas de estudiar la mente y los procesos de pensamiento, demuestran que el eslabón más crítico de la seguridad digital no es el servidor, sino el cerebro humano. Al comprender procesos como la atención, la memoria y la toma de decisiones bajo estrés, los atacantes perfeccionan técnicas de ingeniería social y phishing que explotan nuestras vulnerabilidades evolutivas. Si bien la neurociencia y la psicología aportan información valiosa para integrar la IA en sistemas más intuitivos y eficaces, este poder también plantea serios dilemas morales sobre hasta qué punto la tecnología debe intervenir, o incluso manipular, la percepción y el comportamiento humano.

En tal sentido, para una protección de la información más eficiente, se debe exigir algoritmos auditables que resguarden al usuario sin sacrificar su libertad y privacidad, frente a sistemas de vigilancia masiva. Este desafío se intensifica con la autonomía de la IA, que abre un debate crítico sobre la responsabilidad ante posibles errores, haciendo indispensable el desarrollo de marcos éticos que definan quién debe rendir cuentas para garantizar que la tecnología se utilice siempre en beneficio del bien común.

Uno de los mayores desafíos en la seguridad digital es la atribución de responsabilidad, ya que las decisiones autónomas de la IA y la predicción cognitiva desdibujan las líneas de autoría y fragmentan la noción tradicional de acción y consecuencia, ante fallos que discriminan usuarios o exponen datos. Para mitigar esta problemática, se debe implementar un modelo de Responsabilidad Compartida, que vincule moralmente a desarrolladores y psicólogos. Este enfoque garantiza que la ciberseguridad funcione como un bien común, priorizando la dignidad y la privacidad humana por encima de la infraestructura técnica.

En definitiva, enfrentar la convergencia entre la inteligencia artificial y la vulnerabilidad cognitiva exige abandonar la visión puramente técnica de la ciberseguridad. El verdadero desafío de nuestra era radica en construir un ecosistema digital regulado, transparente y moralmente responsable, donde programadores y expertos del comportamiento colaboren activamente. Solo mediante este marco de corresponsabilidad será posible transformar las herramientas de control potencial en escudos de protección social. El éxito de esta transición tecnológica no se medirá por la autonomía de sus sistemas, sino por su capacidad inquebrantable de supeditarlos a la dignidad, la privacidad y el bienestar común.

Dra. María Eugenia Fossi Medina
Decana de Ingeniería
URBE

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No. 01– Año 2026