Computación Cuántica: Desafíos para la ciberseguridad en la Justicia y su posible utilización en la comisión de ilícitos. ¿Las firmas digitales estarán seguras?

Lucas Moyano[1]

Los avances tecnológicos prometen beneficios trascendentales para la sociedad, con el potencial de revolucionar campos tan diversos como la medicina —al acelerar el descubrimiento de fármacos que salvan vidas—, la ciencia de materiales —mediante la creación de compuestos con propiedades hasta ahora inimaginables—, las finanzas —optimizando estrategias de inversión— y la inteligencia artificial —potenciando su capacidad de aprendizaje automático—. Sin embargo, estos mismos progresos representan una amenaza latente para la ciberseguridad. Como toda herramienta inherentemente amoral, su impacto, benéfico o perjudicial, dependerá enteramente de la intención con la que se utilice.

Actualmente, la protección de nuestros datos e información digital descansa sobre una capa invisible: la criptografía. Este escudo digital resguarda nuestros mensajes, transacciones bancarias, historiales médicos e infraestructuras críticas. No obstante, la llegada de la computación cuántica amenaza con vulnerar y quebrar los sistemas de cifrado actuales.

La computación cuántica constituye un paradigma informático novedoso que explota los principios de la mecánica cuántica para abordar problemas cuya complejidad resulta intratable para las computadoras clásicas. A diferencia de estas últimas, que operan con bits de valores binarios (0 o 1), las computadoras cuánticas emplean qubits (bits cuánticos), capaces de representar ambos valores simultáneamente gracias al principio de superposición. Esta característica multiplica exponencialmente su capacidad de procesamiento.

Ante este panorama, surge una pregunta fundamental: ¿qué impacto podría tener este avance tecnológico en el ámbito de la Justicia?

Entre los efectos positivos, la integración de la computación cuántica con la inteligencia artificial (IA) presenta el potencial de transformar radicalmente la administración de los procesos legales. Podría optimizar la gestión de casos, robustecer la seguridad de la información y agilizar el acceso a la justicia, permitiendo analizar vastos conjuntos de datos, predecir posibles desenlaces judiciales y automatizar trámites legales, lo que reduciría considerablemente los tiempos de resolución de conflictos.

No obstante, uno de los impactos más inmediatos y significativos de la computación cuántica se encuentra en el ámbito de la ciberseguridad, principalmente por su

[1] Fiscal. Especialista en Cibercrimen y Evidencia Digital. Autor del Libro: Ciberdelitos Como Investigar en Entornos Digitales. Editorial Hammurabi

capacidad para superar la criptografía actual, base de la seguridad de la información digital utilizada en el sistema judicial.

En este punto, debemos recordar que la justicia argentina confía en la criptografía e implementa su uso para garantizar la seguridad y autenticidad de la información digital. Esto se logra a través de métodos como el cifrado —que resguarda los datos frente a accesos no autorizados— y las firmas digitales, que añaden una huella única a documentos y correos electrónicos, brindando seguridad en el intercambio de información. Dichas firmas garantizan tres aspectos fundamentales: la autenticidad (identificación fehaciente del firmante), la integridad (verificación de que el contenido no ha sido modificado luego de la firma) y la validez jurídica (equivalente a la firma manuscrita) del documento firmado digitalmente.

Esta seguridad, sin embargo, se ve amenazada por la computación cuántica. El algoritmo de Shor, desarrollado por el matemático Peter Shor, permitiría a las computadoras cuánticas —con la potencia necesaria— factorizar números grandes y resolver problemas de logaritmos discretos en tiempos razonables. En la práctica, esto significa que una computadora cuántica suficientemente avanzada podría obtener la clave privada a partir de la clave pública, permitiendo a un atacante falsificar firmas digitales que aparentarían ser legítimas.

Las consecuencias de esta capacidad son alarmantes. La falsificación de firmas digitales se convierte en una posibilidad real, permitiendo a ciberdelincuentes generar firmas apócrifas, falsificar documentos, contratos y transacciones. Esto facilitaría la suplantación de identidades digitales y pondría en duda la autenticidad de la evidencia digital. Además, la vulnerabilidad de los sistemas criptográficos actuales expondría la confidencialidad de los expedientes judiciales, dejando al descubierto datos sensibles y abriendo la posibilidad de manipulación de evidencia digital, con el consecuente riesgo para su autenticidad e integridad.

En un contexto donde la justicia argentina se esfuerza por modernizarse y adoptar los avances tecnológicos, estas nuevas amenazas nos obligan a mirar hacia el futuro con urgencia. Anticipar y fortalecer la ciberseguridad de los expedientes judiciales se vuelve una tarea prioritaria e ineludible ante la inminente llegada de la era cuántica.

Pero los desafíos no terminan ahí. Imaginemos un escenario aún más inquietante: la computación cuántica unida a la inteligencia artificial con fines delictivos. Sin dudas, la computación cuántica podría acelerar significativamente el desarrollo y las capacidades de la inteligencia artificial (IA) y, según el uso que se haga de ella, potenciar conductas criminales al habilitar acciones como las siguientes:

- Desarrollo de deepfakes más convincentes: creación de videos y audios falsos extremadamente realistas, utilizados con fines de fraude, difamación o manipulación.
- Ataques de phishing y de ingeniería social más sofisticados: IA capaz de analizar el comportamiento humano para generar ataques personalizados altamente efectivos.

- Sistemas de vigilancia y reconocimiento facial avanzados: seguimiento e identificación de personas sin su consentimiento, con posibles aplicaciones en el acoso o la persecución.
- Automatización de ciberataques: creación de malware y virus más inteligentes, adaptativos y difíciles de detectar.
- Fraude financiero avanzado: desarrollo de algoritmos capaces de identificar patrones y explotar vulnerabilidades en sistemas financieros con mayor precisión.

Conclusión

Es importante señalar que la computación cuántica aún se encuentra en una etapa relativamente temprana de desarrollo. La construcción de computadoras cuánticas lo suficientemente potentes y estables como para representar una amenaza concreta a los sistemas criptográficos actuales todavía enfrenta importantes desafíos técnicos.

Sin embargo, esta realidad no debe inducirnos a la inacción. Por el contrario, debería impulsarnos a prepararnos para un futuro que se acerca con rapidez. En mi opinión, resulta esencial adoptar medidas proactivas. Entre ellas, propongo las siguientes:

- Capacitación específica sobre los riesgos y oportunidades que implica la computación cuántica.
- Desarrollo e implementación de nuevos algoritmos de cifrado resistentes a ataques cuánticos.
- Adopción de medidas de seguridad más robustas y adaptativas, capaces de detectar y neutralizar ataques avanzados.

Todo lo anterior debe ir acompañado de un desarrollo normativo que aborde los desafíos emergentes de la computación cuántica. Este marco legal deberá centrarse en la protección de la seguridad de la información frente a la latente amenaza que implica la ruptura de la criptografía actual. Asimismo, deberá fomentar la innovación y el desarrollo responsable de tecnologías cuánticas, considerando aspectos fundamentales como la privacidad, las implicancias éticas y la necesidad de penalizar su uso con fines ilícitos.

La llegada de la era cuántica no es una posibilidad lejana, sino un desafío inminente que interpela directamente a nuestras instituciones. Es momento de anticiparse, actuar con responsabilidad y construir desde hoy una Justicia capaz de afrontar los riesgos del mañana.