Prepararsi quando c'è ancora tempo per decidere. Le banche davanti alla soglia quantistica

Preparing while there is still time to decide. Banks at the quantum threshold

Marco Elio Rottigni, Direttore Generale dell'ABI

Keywords
Sicurezza, cybersecurity, innovazione tecnologica, Intelligenza artificiale, quantum computing, banche

Jel codes
M15, O33, K24, G21, G28

La sicurezza bancaria si basa sulla fiducia e sulla protezione della persona. Oggi deve affrontare sfide fondamentali come cybersecurity, frodi, privacy, sovranità delle infrastrutture finanziarie, Intelligenza artificiale. Il quantum computing potrebbe compromettere gli attuali sistemi crittografici, perciò le banche devono prepararsi in anticipo, adottando nuove soluzioni di sicurezza. Intelligenza artificiale e tecnologie quantistiche offrono grandi opportunità, ma richiedono regole, controlli e responsabilità umane. È necessario proteggere le interdipendenze, rafforzare la resilienza e sviluppare capacità europee. La collaborazione tra banche, istituzioni e imprese è fondamentale, perché la sicurezza è un bene collettivo. L'obiettivo è governare l'innovazione mantenendo al centro la dignità umana, la riservatezza e la fiducia, trasformando l'incertezza in un futuro affidabile.

Banking security is based on trust and the protection of the person. Today it faces fundamental challenges such as cybersecurity, fraud, privacy, sovereignty of financial infrastructures, Artificial intelligence. Quantum computing could compromise current cryptographic systems, so banks must prepare in advance, adopting new security solutions. Artificial intelligence and Quantum technologies offer great opportunities, but they require rules, controls and human accountability. It is necessary to protect interdependencies, strengthen resilience and develop European capacities. Collaboration between banks, institutions and companies is crucial, because security is a collective good. The goal is to govern innovation while keeping human dignity, confidentiality and trust at the center, transforming uncertainty into a trustworthy future.

Introduzione

Negli ultimi mesi è emerso con grande evidenza che l'industria finanziaria si confronta con cinque dimensioni:
1. cybersecurity, frodi e data privacy;
2. sovranità dell'infrastruttura finanziaria;
3. Intelligenza artificiale e nuove tecnologie;
4. sicurezza fisica e resilienza infrastrutturale;
5. cultura della sicurezza, awareness e responsabilità condivisa.
Sono dimensioni tutte essenziali per guardare la sicurezza nella sua complessità e coglierne le molteplici implicazioni. È infatti sempre più chiaro a banche, istituzioni, consumatori e operatori quanto queste cinque dimensioni siano ormai interdipendenti.
E dietro ciascuna di esse c'è una parola più profonda, senza la quale il settore bancario non esiste: fiducia.

1. Dove nasce la fiducia

La fiducia dà valore a un pagamento che arriva, a un risparmio custodito, a un'identità digitale riconosciuta, a un dato protetto; ed è ciò che consente a una relazione economica di durare nel tempo. Le banche rendono possibile tutto questo ogni giorno attraverso infrastrutture, regole e garanzie spesso invisibili e lavorano perché ciò che oggi diamo per acquisito continui a essere affidabile anche domani. Perché la fiducia vive nel tempo.
In realtà, dietro la fiducia si nasconde qualcosa di ancora più radicale: la dignità della persona. Perché quando parliamo di sicurezza sembra che stiamo parlando di sistemi, di reti, di algoritmi, di perimetri. In verità stiamo sempre parlando di qualcuno. Dietro ogni credenziale c'è un nome; dietro ogni conto, una storia; dietro ogni dato, una vita che quel

Il testo riprende l'intervento di chiusura dell'autore a WeSec, Il Salone della Sicurezza, Milano, 23 settembre 2026.

dato non esaurisce. La sicurezza informatica è, in ultima analisi, una forma tecnica di rispetto.
E, proprio per questo, la sicurezza non può limitarsi all'oggi, ma deve proteggere anche ciò che dovrà restare affidabile domani: un'identità, un'informazione, un investimento, una promessa. Questo è esattamente il senso di WeSec: capire quali cambiamenti stanno già modificando il terreno su cui poggia la fiducia.
È da qui che nasce anche il tema del quantum per il mondo bancario: il quantum ci costringe a guardare dove quella fiducia sarà messa alla prova: nel tempo dell'innovazione, nella sicurezza delle infrastrutture, nella responsabilità delle scelte.

2. Quando la storia accelera: tre passaggi, una sola lezione

La storia non avanza sempre alla stessa velocità. Per lunghi periodi procede quasi in silenzio; poi alcune innovazioni cambiano il ritmo del tempo. Tre passaggi riassumono secoli:

1. intorno al 1450, Gutenberg cambia chi può sapere. Il torchio tipografico non ha reso tutti sapienti da un giorno all'altro: ha cambiato la struttura dell'accesso alla conoscenza, facendola uscire dal perimetro dei pochi. Prima lezione: ogni tecnologia ridistribuisce potere, e la vera posta in gioco non è la macchina, è chi ne resta fuori;
2. dal 1903 al 1969, in soli 66 anni, si passa da dodici secondi di volo alla Luna. L'arco di una sola vita umana. In quell'arco storico, maturano e si diffondono su vasta scala elettrificazione e produzione industriale di massa. Seconda lezione: l'intervallo tra una svolta e la successiva si accorcia, e con esso si accorcia il tempo per decidere;
3. dalla rivoluzione digitale all'Intelligenza artificiale che, nata come campo di ricerca nel 1956, ha conosciuto negli ultimi quindici anni un'accelerazione che l'ha portata a entrare nella quotidianità di imprese, istituzioni e persone. Terza lezione: oggi le accelerazioni non si mettono in fila, si sovrappongono, si sommano e si amplificano.

Tre passaggi, una lezione comune: ogni rivoluzione ha preparato il terreno e moltiplicato le possibilità della successiva, fino a comprimere le distanze tra una svolta e l'altra. E quando le accelerazioni si sovrappongono, chi custodisce la fiducia degli altri non può permettersi di decidere all'ultimo momento.

3. Davanti alla soglia quantistica

Ora siamo davanti a un'altra soglia. Non ne vediamo ancora tutta la profondità, ma ne avvertiamo già la forza. Per il settore bancario, che custodisce la fiducia nel tempo, questa compressione ha una conseguenza precisa: deve prepararsi prima che gli effetti diventino visibili. Dati cifrati oggi possono essere raccolti e conservati nell'attesa che, domani, nuove capacità consentano di leggerli. Un computer quantistico in grado di compromettere una parte degli attuali sistemi crittografici a chiave pubblica non è ancora disponibile: il rischio, però, ha già cominciato a modificare le decisioni del presente. È il futuro che proietta la propria ombra all'indietro.
La sfida quantistica non appartiene più soltanto al linguaggio del futuro. Il cosiddetto Q-Day non ha ancora una data certa. Proprio per questo non può essere trattato come un appuntamento da attendere: per i tempi della sicurezza e delle grandi infrastrutture finanziarie, la questione è già presente.
Non perché sappiamo quando accadrà, ma perché prepararci richiede anni: censire algoritmi, certificati, applicazioni, dispositivi e dipendenze dai fornitori; definire priorità; aggiornare sistemi complessi senza interrompere i servizi. Il tempo da considerare, dunque, non è solo quello che ci separa dal possibile arrivo della minaccia, ma anche quello necessario a rendere sicure e resilienti le infrastrutture che oggi sostengono la fiducia.
Se la preparazione richiede anni, attendere una data certa significherebbe iniziare troppo tardi. Per questo il Q-Day, dal punto di vista delle decisioni, produce effetti già oggi: orienta scelte, investimenti, standard e responsabilità. Non è ancora un evento compiuto, ma già una trasformazione da governare.
Ed è per questo che ricerca e programmi industriali, da un lato, standard crittografici post-quantum e piani di migrazione, dall'altro, sono già entrati nella fase dell'esecuzione. Il quantum computing non è semplicemente un computer

più veloce, ma un modo diverso di affrontare i problemi.
Nella fisica dei materiali sono emerse, su temi circoscritti, prime indicazioni di un possibile vantaggio quantistico, ancora oggetto di confronto scientifico. Non significa che il quantum sia superiore in tutto. Significa che, in alcuni domini, un modo diverso di calcolare può spostare il confine della conoscenza.
Intanto, i primi standard internazionali di crittografia post-quantum sono disponibili e l'Unione europea ha definito un piano coordinato di transizione. Gli standard del Nist sono dell'agosto 2024; il piano europeo, del giugno 2025, chiede di avviare la transizione entro la fine del 2026, di migrare i casi d'uso ad alto rischio entro il 2030 e il resto entro il 2035. Per organizzazioni e infrastrutture critiche non si tratta più di osservare, ma di pianificare e attuare migrazioni che richiederanno anni. Questa è già esecuzione. Ed è già responsabilità.
L'accelerazione è cominciata, anche se la destinazione non è ancora definita. E dalle due giornate di WeSec emerge una responsabilità comune: non subire la traiettoria, ma contribuire a orientarla.
Ed è qui che il quantum diventa decisivo. Non cambia soltanto il modo in cui calcoliamo: in alcuni ambiti, può ampliare enormemente le nostre capacità e trasformare il rapporto con la conoscenza, il potere, la sicurezza e il tempo. Potrà aiutarci a simulare molecole e materiali e ad affrontare problemi oggi fuori dalla portata del calcolo classico. Ma potrà anche mettere in discussione la crittografia a chiave pubblica sulla quale si regge una parte essenziale della vita digitale.

4. Il potere dentro la tecnologia

Ogni grande innovazione distribuisce opportunità e crea nuove asimmetrie. La stampa ha ampliato l'accesso al sapere; l'industria ha concentrato capitale e capacità produttiva; il digitale ha diffuso strumenti potentissimi e concentrato dati e infrastrutture in pochi nodi globali. Il quantum richiederà talenti rari, investimenti ingenti e infrastrutture specializzate. La questione del potere è già dentro la tecnologia.
E dove c'è potere asimmetrico, c'è sempre una questione di dignità. Perché la disuguaglianza che si profila non riguarda soltanto l'accesso a una macchina: riguarda la possibilità di comprendere e contestare decisioni che ci riguardano. Se la capacità di calcolare si concentra, si concentra anche la capacità di sapere, di prevedere e di influenzare.
Non è scritto quale modello saprà guidare meglio questa transizione. I sistemi più accentrati possono apparire più rapidi nel concentrare dati, investimenti e decisioni; quelli fondati su apertura, pluralità e controllo democratico dispongono però di una risorsa decisiva, che ci riporta al punto di partenza: la fiducia. Ma la fiducia non può restare un principio dichiarato, deve tradursi in capacità, collaborazione e velocità di esecuzione.

5. Intelligenza, calcolo, responsabilità

L'Intelligenza artificiale ha potenziato le nostre capacità. Il quantum computing promette di esplorare possibilità oggi irraggiungibili.
L'Intelligenza artificiale e il quantum computing, però, non sono due versioni, una più potente dell'altra, della stessa tecnologia. L'Intelligenza artificiale che conosciamo oggi opera su sistemi classici: apprende dai dati, riconosce schemi, genera contenuti e previsioni, supporta le decisioni. Il quantum non è una nuova forma di intelligenza: è un modo radicalmente diverso di calcolare, fondato sulle leggi della fisica quantistica, che potrebbe offrire un vantaggio su problemi specifici, dalla simulazione di materiali e molecole all'ottimizzazione, con implicazioni profonde anche per la crittografia. L'una amplia ciò che possiamo ricavare dai dati; l'altro può spostare, in alcuni ambiti, il confine di ciò che riusciamo a calcolare in tempi utili.
La domanda, allora, non è quale dei due sostituirà l'altro, ma quale rapporto si creerà tra loro. Procederanno lungo traiettorie parallele? Oppure finiranno per rafforzarsi reciprocamente? È possibile che il futuro sia ibrido: calcolo classico, Intelligenza artificiale e quantum chiamati non a sostituirsi, ma a cooperare. Quale parte dei problemi affi-

deremo a ciascuno? E chi governerà il punto in cui le loro capacità si incontrano?

Governare questa trasformazione significa, innanzitutto, governare i dati che la rendono possibile. E governance non significa moltiplicare burocrazia e adempimenti fini a sé stessi: significa assicurare una gestione ordinata e responsabile dei dati. Sapere quali utilizziamo, da dove provengono, chi può accedervi, per quali finalità e con quali garanzie. Significa rendere i processi tracciabili, le responsabilità riconoscibili e le decisioni verificabili.

Per una banca questo è essenziale, perché un dato non è mai soltanto una risorsa tecnologica: può rappresentare l'identità, il risparmio, il lavoro e i progetti di una persona. La governance, quindi, come ciò che consente all'innovazione di diventare affidabile, sostenibile e duratura.

Non possiamo prevedere con certezza quale forma prenderà questa convergenza. Ma possiamo, e dobbiamo, governarne l'evoluzione perché, nel settore bancario, non comprometta la fiducia delle persone.

Con l'Intelligenza artificiale stiamo imparando che delegare capacità non significa delegare responsabilità. Il quantum aggiunge una domanda ancora più radicale: chi potrà accedere a una risorsa così scarsa e potente? Come valideremo e verificheremo risultati prodotti da calcoli che non possiamo replicare efficientemente con sistemi classici? Come eviteremo che i benefici si concentrino e i rischi ricadano sulla collettività?

Non dobbiamo, tuttavia, confondere l'accelerazione con una corsa inevitabile verso il tracollo. La tecnologia non ha una direzione morale propria: non è, in sé, né salvezza né minaccia. Il suo impatto dipenderà da noi, dalle regole, dalle Istituzioni e dai valori con cui sapremo orientarla. Ma, accanto alla necessaria prudenza, dovremmo conservare anche la capacità di stupirci. C'è una bellezza profondamente umana nel lasciarsi sorprendere da possibilità che, fino a ieri, sembravano impensabili. Il futuro, quindi, non va guardato soltanto con timore: va compreso e governato, ma anche accolto con curiosità e fiducia, mantenendo sempre la persona al centro.

Per questo, l'etica deve diventare parte dell'architettura: fini dichiarati, accessi governati, decisioni tracciabili, validazione etica degli algoritmi, risultati sottoposti a verifica, responsabilità umane riconoscibili. Quanto più cresce la potenza del calcolo, tanto più deve essere alta la qualità delle decisioni che la orientano.

Vorrei essere esplicito su un punto. A WeSec abbiamo parlato molto di perimetri: perimetri di rete, perimetri fisici, perimetri di fornitura. Ma esiste un perimetro che viene prima di tutti gli altri, e che nessuna tecnologia può ridisegnare: il perimetro della persona.

La dignità umana non è una preferenza culturale europea: è il primo articolo della Carta dei diritti fondamentali dell'Unione, che la definisce inviolabile. E non è un caso che il regolamento europeo sull'Intelligenza artificiale abbia scelto, per questa tecnologia, la parola antropocentrica: la tecnologia come strumento per le persone, e non come misura delle persone.

6. La leadership che anticipa

La leadership non misura il futuro con un calendario: lo prende sul serio abbastanza presto da trasformarlo in un percorso.

Dalle evidenze e dal confronto emersi a WeSec si ricavano, a mio avviso, tre traiettorie di leadership, decisive per governare il futuro senza subirlo:

- non basta proteggere il perimetro, dobbiamo proteggere le interdipendenze. Le vulnerabilità attraversano fornitori, cloud, reti di pagamento, identità digitali e territori. Nessuna organizzazione può essere davvero sicura se non lo è anche l'ecosistema in cui opera;
- non basta alzare muri, dobbiamo costruire sistemi che imparano ed evolvono. In un contesto che cambia rapidamente, la sicurezza deve funzionare come un sistema resiliente e adattivo, capace di riconoscere minacce nuove, adattare le difese e imparare dagli eventi. Proteggere, oggi, significa anche conservare la libertà di cambiare domani;
- non basta avere regole europee, dobbiamo costruire anche capacità europee. Le dipendenze nel cloud, nei semiconduttori, nell'Intelligenza artificiale e nelle filiere quantistiche non possono essere eliminate, ma possono essere

governate: mappando le esposizioni, privilegiando standard aperti, sviluppando soluzioni europee nei punti più critici e cooperando da una posizione più solida. È così che si impedisce alla dipendenza di diventare vulnerabilità.

È una sfida decisiva per l'Europa ed è anche la direzione indicata dalla Quantum Europe Strategy adottata dalla Commissione europea nel luglio 2025: il patrimonio di regole, diritti e affidabilità deve camminare insieme a capacità industriale, competenze, investimenti e velocità di esecuzione.

7. La sicurezza come bene comune

In questo passaggio, le banche hanno una responsabilità particolare. Non perché debbano risolvere da sole la sfida tecnologica, ma perché sono un crocevia della vita economica: dati, pagamenti, identità, risparmio e credito. Quando la fiducia in una banca tiene, milioni di persone possono agire e progettare. Quando si incrina, l'incertezza corre più veloce del denaro.

Concorrenza e cooperazione devono quindi incontrarsi. Le banche continueranno a innovare e competere. Ma sugli standard, sulle minacce, sulle dipendenze critiche e sul dialogo con Autorità e fornitori, la sicurezza è un bene precompetitivo e collettivo.

Qui il ruolo dell'ABI diventa concreto: creare linguaggi comuni, trasformare segnali dispersi in un'agenda condivisa, portare il confronto dove serve e preparare per tempo ciò che nessun operatore può affrontare da solo. In una transizione così lunga, chi pensa di potercela fare senza gli altri rischia di diventare l'anello più debole.

Per questo abbiamo creato WeSec 2026, l'appuntamento trasversale sulla sicurezza che si è svolto a Milano il 22 e 23 settembre (v. box). Un luogo stabile di consapevolezza, confronto e responsabilità condivisa, aperto gratuitamente a tutti. È l'espressione del lavoro di due Comitati tecnico-strategici di ABI – «Sicurezza Digitale» e «Internazionalizzazione e Trend Geopolitici» – che presidiano due macro-trend sempre più intrecciati tra loro: la sicurezza, nelle sue dimensioni fisica e digitale, e l'evoluzione degli scenari geopolitici. Dei risultati concreti che ne escono – e per i quali ringrazio tutti coloro che ci hanno lavorato – uno è ABI Atlas, il Centro di competenza permanente sulla geopolitica del settore bancario, concepito per trasformare l'analisi degli scenari globali in capacità decisionale e operativa.

Mi piace leggere nel logo di WeSec2026 il diaframma di un obiettivo fotografico: un'apertura che regola la luce e consente allo sguardo di mettere a fuoco, linee diverse che con-

Box

La prima edizione di WeSec: un approccio strategico alla sicurezza

2.000 presenze nell'arco delle due giornate, 110 aziende partner coinvolte e presenti nell'area espositiva. Ma a dare il senso del valore della prima edizione di WeSec, Il Salone della Sicurezza, il nuovo evento promosso dall'ABI e svoltosi al MiCo di Milano il 22 e 23 settembre, sono soprattutto i numeri della ricchezza informativa che ha caratterizzato le due giornate: 31 sessioni (tra cui la plenaria di apertura e quella di chiusura trasmesse in diretta da Class Cnbc), 185 relatori, 5 aree tematiche verticali.

Una ricchezza di voci, idee, visioni, case history che hanno restituito l'ampiezza e la complessità dell'ecosistema della sicurezza. Per la prima volta affrontato secondo una visione strategica, nelle sue relazioni con i temi-chiave che guidano le sfide e i rischi del mondo contemporaneo: dalla geopolitica all'Intelligenza artificiale, dalle infrastrutture critiche alla resilienza operativa, fino a temi di frontiera come il quantum computing e gli scenari inediti che si aprono con le nuove potenze di calcolo. Un'occasione per mettere a confronto e in dialogo ambiti e competenze diverse, settore privato e istituzioni pubbliche italiane ed europee, università e mondo della ricerca.

Con la prima edizione di WeSec – appuntamento realizzato da ABIServizi-ABIEventi in collaborazione con CertFin, ABI Lab, Ossif e FEduF, con il partner istituzionale PagoPA e con il knowledge partner Deloitte – l'ABI ha posto un tema nodale per lo sviluppo economico, sociale e anche culturale del Paese. Consolidando la centralità del settore finanziario per la crescita e promuovendo, con l'apertura gratuita del Salone a tutti i cittadini, il dialogo con le giovani generazioni e i cittadini.

vergono verso un centro comune. È una metafora precisa di ciò che abbiamo fatto in quelle due giornate: leggere meglio i rischi, condividere la conoscenza, trasformare punti di vista diversi in una direzione comune.
Con un impegno preciso: trasformare la cultura della sicurezza in una responsabilità condivisa. La sicurezza non è un ostacolo all'innovazione: è la condizione che permette all'innovazione di durare e alla fiducia delle persone di reggere nel tempo.

8. Una domanda per il futuro

In un mondo nel quale sapremo calcolare ciò che oggi appare impossibile, sapremo anche governare quella potenza perché non resti privilegio di pochi? Sapremo proteggere ciò che rimane essenziale: la continuità dei servizi, la riservatezza, la libertà economica, la fiducia?

E soprattutto: sapremo far sì che, mentre le macchine diventano più potenti, le persone non diventino più piccole? Perché la vera misura di questa transizione non sarà quanti qubit avremo, né quanti modelli, né quanta velocità. Sarà una domanda molto più semplice: al termine di tutto questo, la persona conterà di più o di meno?
La risposta non verrà da una tecnologia soltanto.Verrà dalla qualità delle Istituzioni, dalla competenza delle imprese, dal coraggio delle scelte e dalla capacità di cooperare. Questo è il messaggio che portiamo fuori da questa edizione: prepararsi quando c'è ancora tempo per decidere, non quando resta soltanto il tempo di reagire.
Trasformare l'incertezza in fiducia è il mestiere delle banche da sempre. Cambia il rischio, cambia la tecnologia. Non cambia il compito.
Il futuro non ci chiede di essere indovinato. Ci chiede di essere reso affidabile.