ITA**SEC19**
Terza Conferenza Italiana sulla CyberSecurity

Sicurezza, privacy, normative: come farli coesistere in ambito Fintech?

Intervento del Capo del Dipartimento Mercati
e sistemi di pagamento della Banca d'Italia

Paolo Marullo Reedtz

Pisa, 14 febbraio 2019

Sicurezza, privacy, normative: evoluzione tecnologica e problematiche regolamentari

Il tema proposto per questo Panel - *Sicurezza, privacy, normative: come farli coesistere in ambito Fintech?* - è per sua natura assai complesso chiamando in causa evoluzioni economiche, tecnologiche e regolamentari che si dipanano in un ambiente tipicamente *cross-sector* e che spaziano dalla dimensione nazionale a quelle europea e globale.

Fra i comparti nei quali l'impatto dell'evoluzione digitale si è manifestato prima è certamente quello dei pagamenti al dettaglio, sostenuto in Europa da un decennale impegno normativo volto a promuovere la diffusione dei pagamenti elettronici.

L'utilizzo di tecnologie che consentono di ampliare la raccolta di dati e di estrarne il massimo contenuto informativo si va ora diffondendo con grande rapidità anche in altri settori, dal credito alla gestione e consulenza finanziaria, alle assicurazioni, alla gestione dei rischi.

Di fronte all'incedere dell'innovazione, regolamentatori e autorità di vigilanza devono valutare compiutamente gli effetti che gli sviluppi tecnologici esercitano sulla struttura dei mercati e sui modelli di *business*. Ciò è necessario per poter governare i rischi per la stabilità dei singoli operatori e del sistema finanziario, per prevenire arbitraggi normativi che alterino le condizioni di parità concorrenziale, per evitare, al tempo stesso, di porre ostacoli ingiustificati all'innovazione tecnologica e finanziaria.

I destinatari dell'azione regolamentare sono innanzitutto i singoli operatori bancari e finanziari e i prestatori di servizi di pagamento. Ad esempio, le condizioni di sicurezza informatica in cui ciascuno di essi opera hanno riflessi: *i)* sulla clientela, per i rischi di frode e di violazione della riservatezza dei dati; *ii)* sugli altri operatori del settore, per le possibili conseguenze di eventuali "incidenti" in termini di fiducia e di contagio; *iii)* sull'affidabilità dei sistemi ai quali essi partecipano, primi fra tutti quelli di pagamento.

Rilevano altresì le infrastrutture del mercato finanziario, quali i sistemi di pagamento e i soggetti che gestiscono sedi di negoziazione e di post trading. La sicurezza di questi soggetti è essenziale per la stabilità sistemica e dunque interessa

le banche centrali, nelle loro funzioni di sorveglianza sul sistema dei pagamenti e di supervisione delle infrastrutture di mercato, quest'ultima svolta insieme alle altre Autorità preposte alla regolamentazione dei mercati finanziari (in Italia la Consob).

Sempre più pregante è pure il ruolo dei fornitori di servizi tecnici (*technical service providers*, TSP), la cui sicurezza si riflette sui singoli committenti e impatta sui sistemi ai quali essi forniscono servizi di rete e infrastrutturali.

Su ciascuno di questi snodi cruciali si apre una sfida per i regolamentatori e per le autorità finanziarie, chiamati a individuare le modalità d'azione che meglio consentono di perseguire i loro fini istituzionali, tenendo conto delle complessità del contesto e dei nuovi modelli di offerta, della centralità assunta dalle esigenze di protezione delle informazioni e della evoluzione dei rischi connessi con il *cyber space*.

Per alcuni aspetti si tratta di adattare o ampliare gli strumenti di vigilanza già esistenti, ad esempio quelli relativi alla gestione dei rischi, fra i quali il rischio operativo, o alla *compliance*; in altri casi occorre individuare strumenti nuovi, come nel campo dei presidii rispetto al *cyber risk*. In altri casi ancora sorge l'esigenza di valutare l'impatto di normative nuove con un campo di applicazione anche più ampio del tradizionale perimetro del sistema finanziario, come nel caso della *General Data Protection Regulation* (GDPR).

Il mio intervento si focalizzerà, in particolare, sugli aspetti relativi ai rischi operativi e cibernetici, in ragione della loro relativa novità, della crescente intensità, del potenziale altamente dirompente per singoli operatori, per la clientela e per i sistemi. Riguarderà le due direttrici dell'azione di regolamentazione e supervisione: quella sui singoli operatori del settore finanziario e quella relativa alla stabilità, affidabilità ed efficienza del sistema e delle infrastrutture del mercato finanziario.

Sebbene le mie argomentazioni saranno largamente riferite al mondo dei pagamenti, il loro campo di applicazione potrà essere letto anche in un ambito più ampio, data la già menzionata pervasività degli sviluppi tecnologici.

Sicurezza degli operatori e stabilità sistemica

In questa fase di trasformazione dei mercati, dei servizi e dei processi di produzione il sistema finanziario si va caratterizzando per la crescente complessità, segnata da nuove interdipendenze con soggetti non più solo di natura finanziaria e

da rischi di concentrazione in capo a fornitori di tecnologia che offrono servizi di importanza critica a una platea molto ampia di utenti.

Sempre di più le vulnerabilità del sistema finanziario risultano ben superiori alla somma di quelle dei suoi singoli componenti.

In un simile scenario risulta ormai chiaro che l'azione sul fronte micro-prudenziale non può che rappresentare solo una parte della più articolata strategia che regolamentatori e autorità finanziarie devono adottare per un'efficace azione di prevenzione e gestione dei rischi sistemici. Ed è ormai evidente anche quanto insufficiente sarebbe una regolamentazione che non comprendesse i TSP nel suo perimetro.

I rischi *cyber* non conoscono, per loro natura, barriere settoriali o confini geografici: nessun operatore può ritenersene esente, magari per non aver mai sperimentato incidenti o attacchi dall'esterno; per lo stesso motivo nessuna controparte può essere considerata intrinsecamente sicura. Proprio perché la probabilità di divenire bersaglio di attacchi non può considerarsi a priori bassa, è necessario che, presso ogni singola entità, alla capacità di prevenire incidenti si accompagni una capacità di risposta pronta ed efficace. Non deve inoltre mancare la disponibilità a fornire informazioni sulle minacce percepite o subite anche agli altri operatori del mercato, in modo da arginare il diffondersi della crisi e ottenere collaborazione sulle più appropriate modalità di intervento.

Il contenimento e la gestione dei rischi informatici richiedono elevata consapevolezza delle possibili conseguenze e strutture di contrasto ben organizzate a livello di singola giurisdizione ma non possono essere affidate unicamente a normative di carattere nazionale.

Per questo è nelle sedi di cooperazione internazionale che si è concentrata la formulazione di regole e linee-guida volte a rafforzare i presidii ai rischi operativi di intermediari, fornitori di servizi tecnologici e infrastrutture del settore dei pagamenti e del mercato finanziario da applicare in un'ottica *worldwide*[1].

La Guidance on cyber resilience for financial market infrastructures, pubblicata dal CPMI-IOSCO a giugno 2016, ha posto per prima l'accento sul concetto di resilienza cibernetica come capacità di un'entità finanziaria di anticipare, resistere, contenere e ripristinare la propria operatività a seguito di un attacco *cyber*.

---

[1] Questo lavorio può giovarsi, dallo scorso novembre, di un comune quadro lessicale in materia di *cyber security* in ambito finanziario, messo a punto dal Financial Stability Board su richiesta dei Ministri delle Finanze e dei Governatori delle banche centrali dei paesi del G20.

Essa non enuncia principi aggiuntivi ma integra i *Core Principles* per le infrastrutture del mercato finanziario emanati congiuntamente dal CPMI e dall'IOSCO nel 2012, esplicitandoli in termini di capacità e controlli che le infrastrutture finanziarie devono sviluppare per rafforzare la propria *cyber resilience*.

Il set di principi internazionali si è poi arricchito grazie ai lavori sviluppati in ambito G7. Nel 2016 sono stati pubblicati i Principi di alto livello rivolti a tutti gli operatori del settore finanziario dei paesi del G7; ad essi si può far riferimento, su base volontaria, nel definire le strategie aziendali e i processi operativi di rafforzamento della *cyber resilience* e nel valutarne l'efficacia in relazione all'evolversi delle minacce esterne[2]. Hanno fatto seguito Principi metodologici per la valutazione dei livelli di sicurezza cibernetica indirizzati sia agli operatori sia alle autorità[3]; Principi per lo svolgimento di test avanzati di intrusione (i cosiddetti test di tipo *red-teaming*) [4] per verificare e migliorare nel continuo le capacità di protezione, rilevamento e risposta agli incidenti *cyber*; Principi per la gestione del rischio di terze parti[5] che gli operatori finanziari e gli stessi fornitori di servizi tecnologici e di rete possono utilizzare per valutare la propria *cyber resilience* e che le autorità possono considerare nel definire gli assetti normativi e i requisiti di vigilanza.

Il lavoro nelle sedi internazionali tende, di fatto, a promuovere una maggiore armonizzazione tra le giurisdizioni nella definizione del perimetro del *cyber risk* e, quindi, della *cyber resilience* attesa per i soggetti vigilati. Il Comitato di Basilea per la vigilanza bancaria ha pubblicato nel dicembre scorso un report *sulle best practices* osservate nelle varie giurisdizioni e sta predisponendo nuove linee-guida che guardano alla *cyber resilience* come a una importante componente del più ampio concetto di *operational resilience*.

Sempre a dicembre la European Banking Authority ha diffuso, per la consultazione, le *Guidelines on ICT and security risk management*, con l'obiettivo di disciplinare in un unico documento la gestione dei rischi IT derivanti da eventi sia interni sia esterni (es. malfunzionamenti operativi, ma anche *data breach* e attacchi *cyber*) riguardanti banche, imprese di investimento e prestatori di servizi di pagamento. L'obiettivo è di definire un set minimo di regole applicabili presso

---

2 "*G-7 Fundamental Elements of Cybersecurity for the Financial Sector" (2016).*
3 "*G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector" (2017).*
4 "*G-7 Fundamental Elements for Threat-Led Penetration Testing" (2018).*
5 "*G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector" (2018).*

tutte le categorie di operatori secondo un principio di proporzionalità in relazione alle dimensioni e alle caratteristiche delle singole realtà.

L'affidabilità dei singoli operatori costituisce, oltre che un obiettivo a sé stante, una precondizione per la resilienza del circuito dei pagamenti interbancari, per il quale essi fungono da punti di accesso (*endpoints*) ma di cui possono costituire un punto di debolezza in grado, nei casi estremi, di compromettere la fiducia nell'integrità dell'intero sistema fino a incepparne il funzionamento.

È in questa ottica che, nello scorso maggio, il Comitato sui Pagamenti e le Infrastrutture di Mercato (CPMI) della Banca dei Regolamenti Internazionali ha messo a punto un approccio organico per la riduzione del rischio di frode presso gli *endpoints* del sistema dei pagamenti all'ingrosso[6]. La strategia si fonda su sette elementi di alto livello che definiscono un insieme di misure da applicare per rafforzare le capacità di prevenzione, rilevamento, risposta e comunicazione riguardo alle frodi[7]. Le misure proposte integrano i *Core Principles* e la successiva *Cyber Guidance del CPMI-IOSCO*; riguardano la protezione degli asset informativi (hardware, software, dati), la gestione degli accessi fisici e logici, l'organizzazione e i processi secondo un approccio olistico alla sicurezza. L'adesione degli operatori di mercato alla strategia così definita viene incoraggiata e monitorata da parte delle banche centrali nazionali, attente anche a individuare eventuali ostacoli al recepimento delle indicazioni e spazi di miglioramento legati a possibili forme di collaborazione.

Come si è avuto modo di rilevare, crescente attenzione viene riservata al ruolo dei fornitori di servizi tecnici in ragione del carattere essenziale della loro attività ai fini del buon funzionamento delle infrastrutture di mercato (es. SIA per il sistema europeo di pagamento al dettaglio STEP2) e dell'ampia platea degli operatori finanziari serviti (es. SWIFT che fornisce servizi di messaggistica finanziaria ad una comunità di circa 11000 soggetti in tutto il mondo). L'azione delle autorità di regolamentazione e supervisione su questi soggetti si muove lungo due direttrici: *i)* una azione indiretta, che si traduce nel chiedere agli operatori finanziari il rispetto di requisiti sul governo dei rischi generati da "terze parti" e sull'esternalizzazione di servizi a fornitori esterni[8]; *ii)* una azione diretta, svolta prevalentemente sulla base

---

6 *CPMI Paper, Reducing the risk of wholesale payments fraud related to endpoint security, May 2018.*

7 La strategia è rivolta a tutti gli stakeholder pubblici e privati del settore finanziario che interesse nel ridurre il rischio di frodi nei pagamenti all'ingrosso, compresi gli operatori dei sistemi di pagamento, i fornitori di servizi di rete e di messaggistica, i loro partecipanti e i rispettivi regolamentatori, supervisori e sorveglianti.

8 Si possono richiamare a tale proposito i Principi del G7 pubblicati a ottobre 2018 sulla gestione dei rischi cyber rivenienti dalle terze parti e l'allegato F ai principi del CPMI che prescrive requisiti di continuità di servizio e gestione dei rischi operativi ai cosiddetti *critical service providers* delle infrastrutture finanziarie.

di accordi di cooperazione tra autorità competenti data l'operatività tipicamente *cross-border* dei soggetti in questione[9].

Le autorità guardano inoltre con favore alle iniziative di autoregolamentazione assunte da grandi fornitori di servizi tecnologici e di rete sulla scorta dell'esperienza di alcuni incidenti di sicurezza informatica. Gli utenti dei loro servizi sono sollecitati a svolgere controlli sistematici aventi per oggetto: l'adeguatezza dei presidii interni (politiche, processi e personale), eventualmente predisponendo piani di rafforzamento; la capacità di individuare frodi nelle relazioni commerciali prima che esse possano sprigionare i loro effetti dannosi; la prontezza e l'efficacia della capacità di risposta agli attacchi e di comunicazione agli altri operatori al fine di circoscrivere gli effetti sistemici.

Le salvaguardie a fronte dei rischi informatici e cibernetici, poste in primo luogo in funzione della solidità degli operatori finanziari, vanno a beneficio anche della clientela: ne proteggono il patrimonio di dati, ne rafforzano la fiducia nei confronti dei nuovi servizi disponibili sul mercato. Da esse non possono prescindere politiche volte a favorire l'innovazione e la competizione.

Ne è un esempio, nell'Unione europea, la *Payment Service Directive 2* - PSD2, la nuova direttiva sui servizi di pagamento, recepita negli stati membri nel corso del 2018, che gli operatori proprio in questi mesi sono chiamati ad attuare.

Con essa il legislatore europeo ha, per la prima volta, riconosciuto e disciplinato modelli di servizio di tipo "Fintech" basati sull'accesso di terze parti ai conti della clientela (fenomeno battezzato come *open banking*). Ai prestatori di servizi di pagamento viene infatti imposto di predisporre canali dedicati per il dialogo con i fornitori dei nuovi servizi di disposizione degli ordini di pagamento (*Payment Initiation Service Providers*, PISP) e di informazione sui conti (*Account Information Service Providers*, AISP). La possibilità di accedere a basi informative finora di esclusivo utilizzo da parte delle singole banche abbatte di colpo le barriere all'ingresso nei mercati di numerosi prodotti creditizi e finanziari, trasferendo le opportunità di cross-selling a una gamma molto più ampia di operatori; sposta la competizione sul terreno delle capacità di archiviazione e di utilizzo delle informazioni; costringe gli intermediari

---

[9] Ad esempio, questo è il caso della supervisione cooperativa su SWIFT svolta dalle Banche Centrali del G10 o della supervisione su SIA svolta dalla Banca d'Italia sulla base dei poteri attribuitigli dal legislatore (art. 146 del TUB) che di recente è stata ampliata con informative periodiche in ambito Eurosistema.

tradizionali a rivedere i loro modelli di *business* ricercando, se del caso, sinergie con le imprese del Fintech.

Questo nuovo sviluppo, che apre la disponibilità degli archivi aziendali a un novero potenzialmente ampio di operatori, può suscitare preoccupazioni per i rischi di sicurezza connessi con l'utilizzo delle credenziali di accesso ai conti bancari. Per gestire i nuovi rischi la direttiva ha definito un ampio set di requisiti di sicurezza, applicabili a tutti gli attori del nuovo ecosistema e articolato su quattro pilastri: l'autenticazione forte della clientela, la gestione del rischio IT a livello aziendale, il reporting obbligatorio degli incidenti, la comunicazione sicura tra gli operatori sfruttando tecnologie tipiche del mondo internet come le *Application Programming Interfaces* (API). Le autorità competenti per l'attuazione della PSD2 hanno adesso il compito, non facile, di monitorare la corretta implementazione delle misure entro la scadenza fissata dalla direttiva (settembre 2019) e successivamente di verificarne l'efficacia.

La Strategia *Cyber* dell'Eurosistema

Secondo quanto finora argomentato, efficaci politiche di rafforzamento della *cyber resilience* devono far leva su tre ambiti di applicazione, logicamente separati ma fortemente interconnessi: la resilienza a livello di singolo operatore, quella a livello di sistema, la collaborazione fra operatori e di questi con le autorità.

Non è dunque un caso che proprio su questi tre pilastri si fonda la strategia adottata nel 2017 dalla BCE e dalle Banche centrali dell'Eurosistema con l'obiettivo di rafforzare le capacità di resistere alle minacce *cyber* da parte dei sistemi di pagamento e delle infrastrutture di post-trading che rientrano nel quadro giuridico delle banche centrali dell'Eurosistema (*Oversight Strategy on Cyber resilience for FMIs*)[10].

Muovendo da prime valutazioni circa lo stato di preparazione dei singoli operatori desunte dai risultati di un *survey* condotta presso sistemi di pagamento, depositari centrali e controparti centrali, sono stati messi a punto strumenti diretti all'individuazione e alla rimozione di debolezze nei processi interni di controllo del rischio *cyber*.

Lo scorso dicembre sono state pubblicate dalla BCE le *Cyber Resilience Oversight Expectations (CROE)*, definite coerentemente con la *Guidance* del

[10] La strategia è prioritariamente rivolta ai sistemi di pagamento all'ingrosso che svolgono un ruolo centrale e critico nel sistema finanziario europeo. Per i soggetti che non rientrano nel mandato di sorveglianza dell'Eurosistema, ciascuna Banca centrale nazionale rimane responsabile dell'applicazione della strategia all'interno della propria giurisdizione, previo accordo con le altre *National Competent Authorities*.

CPMI-IOSCO in tema di resilienza cibernetica per le infrastrutture di mercato. Si tratta di un *tool* di supervisione utile a: supportare le infrastrutture finanziarie con indicazioni dettagliate su come rendere operativa la G*uidance* e su come condurre il processo di autovalutazione; rappresentare uno strumento che le autorità possono utilizzare per vagliare le capacità di *cyber resilience* rispetto ad un livello atteso di maturità degli operatori vigilati definito a priori (*levels of expectations*); realizzare una base comune di confronto per una proficua e continua interazione tra le autorità e i soggetti regolati.

È stato inoltre definito un *framework* (*European Threat Intelligence Based Ethical Red Teaming - TIBER-EU)* per l'esecuzione di *penetration test* che possano rivelare eventuali punti deboli nei processi di controllo dei rischi *cyber* presso le singole entità e indicare, sia al management sia alle autorità di vigilanza, gli aspetti sui quali intervenire. Nell'ambito dell'Eurosistema sono già state avviate le iniziative necessarie allo svolgimento di un test sul sistema di regolamento lordo paneuropeo Target2. *TIBER-EU* costituisce uno schema utilizzabile, in linea di principio, anche presso altri operatori sistemici, in primo luogo le grandi banche; a tale scopo, in vari paesi sono in corso contatti con altre autorità di settore per valutare gli opportuni adattamenti. Il comune riferimento a un unico *framework* di simulazione è un obiettivo di grande rilievo, in quanto consentirebbe un mutuo riconoscimento dei risultati delle simulazioni da parte degli organismi di supervisione e allevierebbe gli oneri regolamentari per operatori con attività *cross-border*.

Il secondo pilastro della strategia dell'Eurosistema, quello focalizzato sulla resilienza del sistema, richiede in primo luogo una definizione precisa delle interdipendenze fra le diverse componenti dell'ecosistema. Per questo si attribuisce grande importanza agli aspetti metodologici e alla concreta predisposizione di uno schema di rilevazione dei nessi operativi fra banche, TSPs e FMIs come presupposto per la valutazione degli effetti sistemici di crisi presso singole componenti e per la messa in atto di adeguati interventi.

Il terzo pilastro si fonda sullo sviluppo della collaborazione fra le varie categorie di infrastrutture del mercato finanziario e di queste con le autorità europee e nazionali. A tale scopo all'inizio dello scorso anno è stato costituito, presso la BCE, un forum di dialogo fra infrastrutture di mercato, fornitori di servizi critici, organismi europei e banche centrali che svolgono funzioni di lead overseer fra cui la Banca d'Italia, lo *Euro Cyber Resilience Board for pan-European Financial Infrastructures* (*ECRB*). Compito del Comitato è individuare questioni di valenza strategica e di promuovere indirizzi strategici e posizioni comuni volte a rafforzare la resilienza cibernetica del sistema finanziario europeo. Nelle prime riunioni del

Board si è deciso di focalizzare l'attenzione in primo luogo: sulle prassi aziendali meglio idonee a promuovere una piena consapevolezza dei rischi *cyber* fra il personale; sull'esigenza di un *framework* per lo scambio di informazioni sulle minacce *cyber* fra gli operatori; sulla predisposizione di un modello di gestione delle crisi in cui siano definiti *trigger*, operatori coinvolti, strutture e protocolli di cooperazione, canali di comunicazione.

Conclusioni

In queste brevi considerazioni si è voluto sottolineare come, nel contesto di un sistema finanziario di elevata complessità, i regolamentatori e le autorità di vigilanza siano chiamati a sviluppare un set di strumenti ben più articolato che in passato. In questo ambito il dialogo con l'industria e la collaborazione fra le autorità assumono un rilievo crescente ai fini del contenimento dei rischi sistemici.

A conclusione ci si può domandare quali iniziative siano state concretamente assunte in Italia sulla scia di questi orientamenti.

L'obiettivo della collaborazione delle autorità col mercato è stato perseguito con grande convinzione. Ne è risultata la costituzione a dicembre del 2016, su iniziativa della Banca d'Italia e dell'ABI, di una struttura specializzata nella *cybersecurity* del settore bancario e finanziario, il *Computer Emergency Response Team* (CERTFin), alla quale hanno di recente aderito l'IVASS e l'ANIA. Al nuovo organismo è affidato il compito di contribuire a prevenire e contrastare le minacce informatiche connesse con lo sviluppo delle nuove tecnologie e dell'economia digitale. A tale scopo il CERTFin funge da centro per l'esame e la condivisione delle informazioni sulle minacce informatiche e sugli incidenti nonché per l'analisi delle possibili contromisure; partecipa a simulazioni fra i principali attori del sistema finanziario; in caso di crisi effettiva svolge funzioni di analisi delle risposte appropriate. Il contributo del CERTFin alla sicurezza informatica del sistema finanziario è divenuto rapidamente assai sostanziale: dall'avvio della sua attività ha prodotto oltre 2.200 segnalazioni relative a oltre 1.800 fenomeni rilevati e analizzati.

L'attività del CERTFin si pone in linea con la Strategia Nazionale in tema di *cybersecurity*, essendo il settore finanziario fra quelli coperti dal decreto di recepimento della Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione ((*Network and Information Security Directive* - NIS).

Nel *framework* nazionale il Ministero dell'Economia e delle Finanze è l'autorità politica con la responsabilità di attuazione della Direttiva per il settore finanziario, responsabilità che svolge in collaborazione con la Banca d'Italia e la Consob. Sono stati individuati gli operatori di servizi essenziali del settore al fine di coordinare gli obblighi richiesti agli operatori NIS (requisiti di sicurezza e obblighi di notifica degli incidenti) con quelli già richiesti dall'articolato corpus normativo del settore finanziario.

Nella Banca d'Italia l'esigenza di cogliere la trasversalità delle tematiche *cyber* nel settore finanziario per assicurare una visione strategica d'insieme ha consigliato l'istituzione di meccanismi di coordinamento delle diverse funzioni interessate: tecnologiche; di vigilanza bancaria, finanziaria ed assicurativa; di oversight sulle infrastrutture del mercato finanziario; di ricerca economica.

Le iniziative dell'Istituto nel campo della vigilanza bancaria e della sorveglianza sul sistema dei pagamenti, si inquadrano in una specifica linea di azione del piano strategico dell'Istituto, volta alla promozione dell'innovazione digitale e della resilienza cibernetica del settore finanziario italiano.

Parallelamente si sviluppa una linea di azione relativa alla protezione degli asset critici della Banca, i cui presidii di difesa informatica sono oggetto di continuo adeguamento, sulla base delle linee guida e delle migliori prassi nazionali e internazionali. In quest'ambito rientra anche la creazione di un CERT interno (CERTBI) e il potenziamento della capacità di *cyber threat intelligence* nel quadro di un approccio pro-attivo alla gestione della sicurezza.

Un ulteriore contributo è fornito dalla raccolta di dati statistici sulla frequenza e la distribuzione degli attacchi cibernetici nei vari settori economici: si tratta di un ambito in cui mancano informazioni affidabili, che risultano tuttavia indispensabili per guidare i necessari interventi di *policy*. La Banca d'Italia ha condotto nel 2017, per la prima volta nel nostro paese, una rilevazione sull'impatto economico degli attacchi informatici al settore privato non finanziario, stimando i danni subiti e le spese sostenute dalle imprese per approntare le necessarie difese.

Grafica a cura della Divisione Editoria e stampa della Banca d'Italia