DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

Outsourcing: Terze Parti fornitrici e governo del rischio

Marzo 2024

Domenico Roselli, Ispettorato Vigilanza, Banca d'Italia

Domenico Roselli, Ispettorato Vigilanza, Banca d'Italia *

* *Le opinioni espresse nel seguente lavoro non impegnano l'Istituto di appartenenza dell'autore.*

Indice: 1. L'esperienza USA; 1.1 BSCA; 1.2 Regolamentazione FED; 1.2.1 I rischi; 1.2.2 Gestione del rischio; 1.2.3 Ruolo dell'Alta Dirigenza; 1.2.4 Ruolo degli incentivi; 1.2.5 Supervisione e monitoraggio; 2 L'esperienza UE; 2.1 DORA; 2.1.1 Sistema interno di gestione dei rischi; 2.2 RTS e ITS; 2.3 Toolkit; 3. L'esperienza UK; 3.1 Discussion Paper ; 3.2 Consultation Paper

Il presente contributo lavoro illustra, in chiave comparata – USA, UE e UK – la regolazione dei rischi rivenienti dall'outsourcing a Terze Parti di prodotti e servizi bancari: oggetto di peculiare attenzione, in questo periodo, da parte delle Autorità di Vigilanza, domestiche e internazionali.

Il ricorso, da parte delle banche, a fornitori esterni di servizi e di prodotti, segnatamente basati sulla tecnologia, si sta espandendo ed evolvendo rapidamente (per numero, tipologia e concentrazione), accrescendo l'importanza del ruolo svolto dalle cd Terze Parti, nel settore finanziario.

Il fenomeno dell'esternalizzazione e i rischi che ne scaturiscono sono pertanto, da tempo, oggetto di discussione e analisi nelle principali sedi internazionali.

1. L'esperienza USA

1.1 BSCA

Negli Stati Uniti, l'utilizzo di *Thrird Parts*, per la fornitura di servizi e di prodotti, alle *financial institutions*, svolge, da tempo, un ruolo importante nel settore finanziario, tant'è che l'*interagency program* di supervisione dei fornitori di servizi tecnologici è in atto da diversi anni.

In proposito, il *Bank Service Company Act* (BSCA) conferisce poteri al *Federal Reserve Board of Governor* (FED)[1], alla *Federal Deposit Insurance Corporation* (FDIC) e all' *Office of the Comptroller of the Currency* (OCC), per regolamentare ed esaminare determinati servizi eseguiti da terzi, per conto di *savings asso-*

1 Il *Federal System* è oggi costituito da un'agenzia governativa centrale, il citato *Board of Governors* - con sede nella capitale e composto da 7 Governatori - e da dodici *Federal Reserve Bank* regionali.
Il *Board* e le *Reserve Bank* condividono la responsabilità nel campo della Vigilanza.

ciation, service companies and subsidiaries.

I servizi identificati nel suddetto provvedimento includono attività quali elaborazione di assegni e pagamenti; servizi di *back-office*; contabilità e servizi di elaborazione dati.

In relazione alle suddette attività, le agenzie:

A) possono regolamentarle ed esaminarle con la medesima invasività ("*the same extent*")[2] utilizzata nei riguardi dell'istituto finanziario, qualora sia questi a prestare il servizio.

Al riguardo, il 12 U.S. C*ode* 1464(d)(7), par. UN del BSCA, dispone infatti che: "*A service company or subsidiary that is owned in whole or in part by a savings association shall be subject to examination and regulation by the appropriate Federal banking agency to the same extent as that savings association*".

B) conducono *examinations* nei confronti dei fornitori di servizi che presentano rischi significativi per gli istituti finanziari clienti e per il settore finanziario.

Al riguardo, il *Code* 1867 della suddetta norma prevede che: "*The appropriate Federal banking agency of the principal shareholder or principal member of such a bank service company may authorize any other Federal banking agency that supervises any other shareholder or member of the bank service company to make such an examination*".

La richiamata disposizione prosegue, statuendo che: "*...whenever a depository institution that is regularly examined by an appropriate Federal banking agency, or any subsidiary or affiliate of such a depository institution that is subject to examination by that agency, causes to be performed for itself, by contract or otherwise, any services authorized under this chapter, whether on or off its premises:*

(1) *such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the depository institution itself on its own premises, and*

2 Crf. *Supervision and Regulation Report* della FED, maggio 2022, pag. 17, box 3.

(2) *the depository institution shall notify each such agency of the existence of the service relationship within thirty days after the making of such service contract or the performance of the service, whichever occurs first*".

I riferiti accertamenti si focalizzano su: gestione della tecnologia; integrità dei dati; riservatezza delle informazioni; disponibilità dei servizi; conformità.

Le risultanze delle suddette verifiche vengono condivise con fornitori di servizi e istituti finanziari clienti, anche al fine di aiutare questi ultimi nel monitoraggio costante del rischio riveniente dall'utilizzo di Terze Parti.

1.2 La regolamentazione FED

L'attività regolamentare della FED che è derivata dalla suddetta fonte primaria, ha rappresentato la dettagliata declinazione dei richiamati poteri che, in chiave comparata, costituisce tuttora un importante paradigma per la normazione successiva degli altri Paesi.

In proposito, l'Autorità di Vigilanza ha pubblicato, nel dicembre 2013, una *Guidance on Managing Outsourcing Risk*[3], con l'obiettivo di assistere le *financial institutions* nella comprensione e gestione dei rischi associati all'esternalizzazione di un'attività bancaria a un fornitore di servizi.

In relazione ai suddetti rischi, il *Board* ha altresì emesso una specifica *Supervisory letter* in materia.

3 Nell'atto (Lettera SR 13/19), che contiene l'emissione della citata Guida, sono indicati i seguenti documenti correlati:
- Lettera RS 13-1/Lettera CA 13-1: Policy supplementare sulla Funzione di revisione interna e sulla sua esternalizzazione;
- Lettera di RS 11-7: *Guidance on Model Risk Management*;
- Lettera RS 06-4: *Interagency Advisory* sull'uso non sicuro e "*unsound*" delle limitazioni alle disposizioni sulla responsabilità, nelle lettere di incarico di revisione contabile esterna;
- Lettera RS 03-5: *Interagency Guide*, sulla funzione di audit interno e sulla sua esternalizzazione.
Inoltre, la Guida fa riferimento alla normativa emanata dalla citata FFIEC, tra cui:
• il *booklet* sulla sicurezza delle informazioni, del settembre 2016;
• il *booklet* dei servizi tecnologici in outsourcing, sopra citato.
Infine, si specifica che le valutazioni dei fornitori di servizi dovrebbero includere il rapporto *Service Organization Control 2* dell'*American Institute of Certified Public Accountants* ("SOC 2").

vedi l'articolo online

La Guida è rivolta a qualsiasi "istituto finanziario" vigilato dalla *Federal Reserve*, indipendentemente dalle dimensioni dell'intermediario. In particolare, si applica a tutte le banche, alle *bank and savings* e alle *loan holding companies* (comprese le filiali non bancarie) e, altresì, a qualsiasi U.*S. operation*, compiuta da una *foreign banking organisation*.

Il suddetto documento si basa e integra l'*Outsourcing Technology Services Booklet* del *Federal Financial Institutions Examination Council* ("FFIEC"), del giugno 2004.

In materia, anche la *Federal Reserve Bank of New York* - con *Circolare del 13 aprile 2000, n. 11242* (*Outsourcing of Information & Transaction Processing*) - ha stigmatizzato la possibilità di incorrere in rischi aggiuntivi, qualora il controllo operativo sulle attività esternalizzate si rivelasse insufficiente.

Al riguardo, la suddetta *branch* regionale ha istituito, in passato, un team di lavoro dedicato, che ha interloquito con una sezione trasversale degli intermediari finanziari del Secondo Distretto, nonché fornitori di servizi, consulenti di gestione e di processo, avvocati e accademici (cfr. *Circolare del 14 ottobre 1999, n. 11193)*, al fine di raccogliere, sul campo, elementi utili per l'attività di supervisione.

I risultati della suddetta analisi sono riassunti in un documento, *Outsourcing Financial Services Activity: Industry Practices to Mitigate Risks*, che esamina la varietà di approcci che i partecipanti al mercato hanno sviluppato per mitigare il rischio di *outsourcing,* individuando quali di essi costituiscono "pratiche corrette".

1.2.1 I rischi

I potenziali rischi derivanti dall'utilizzo di fornitori di servizi, per svolgere funzioni operative, sono illustrati nella sezione II della Guida.

Alcuni di essi sono, in generale, inerenti all'attività esternalizzata stessa; mentre altri, più specifici, vengono introdotti proprio con il coinvolgimento di un fornitore di servizi.

In particolare, l'istituto finanziario dovrebbe considerare le seguenti categorie di rischi, prima di stipulare e nel corso di un accordo di *outsourcing*:

- **conformità**, che sorgono quando il fornitore di servizi non osserva le leggi e i regolamenti statunitensi applicabili;

- **concentrazione**, che si profilano allorché i servizi o i prodotti esternalizzati sono forniti da un numero ristretto di fornitori di servizi ovvero sono concentrati in aree geografiche delimitate;

- **reputazionali**, scaturenti dai riflessi negativi dell'attività del fornitore di servizi sul pubblico, che induce la formazione di un'opinione negativa su un istituto finanziario;

- **legali,** che si determinano quando un fornitore di servizi espone l'intermediario a spese e a possibili azioni legali;

- **operativi**, rivenienti dall'esposizione dell'istituto finanziario, da parte del fornitore di servizi, a perdite dovute a processi ovvero sistemi interni inadeguati o *failed* ovvero, infine, a eventi esterni ed errori umani;

- **Paese**, che sorgono quando un istituto finanziario assume un fornitore di servizi con sede all'estero, esponendo l'istituto a possibili condizioni ed eventi economici, sociali e politici, del Paese in cui ha sede il fornitore.

1.2.2 Gestione del rischio

La Sezione IV.G della Guida espone le modalità con le quali gli intermediari possono governare il rischio associato ai servizi di *outsourcing*, esercitando la supervisione sui fornitori terzi.

Al riguardo, infatti, il suddetto programma di amministrazione dei rischi rivenienti dall'attività del fornitore di servizi dovrebbe prevedere, appunto, un **livello adeguato di sorveglianza e controlli**, commisurato alla rischiosità, previsto dagli accordi di esternalizzazione.

La complessità della suddetta gestione dipende, ovviamente, da una serie di fattori: numero e tipologia delle attività in *outsourcing*; criticità della funzione esternalizzata; reputazione del fornitore.

Particolare attenzione, va da sé, dovrebbe essere prestata alle attività che potrebbero avere un impat-

vedi l'articolo online

to sostanziale sul *core-business* dell'ente e a quelle che comportano rischi di conformità significativi.

Sebbene le attività da svolgere per attuare un efficiente programma di gestione del rischio dovrebbero essere plasmate caso per caso, occorre di solito considerare:

A) Valutazione

La *Guidance* rileva che, prima di decidere se esternalizzare o meno un'attività d'impresa, è fondamentale effettuare una valutazione del rischio dell'attività stessa.

In particolare, le *financial institutions* dovrebbero analizzare le implicazioni connesse allo svolgimento di un'attività *in-house*, rispetto a farla svolgere da un fornitore di servizi; vagliando, altresì, se l'esternalizzazione di una determinata funzione è coerente con la direzione strategica e la strategia aziendale complessiva dell'organizzazione.

L'adeguata valutazione del rischio, peraltro, dovrebbe sostanziarsi in un processo continuo e, pertanto, aggiornato, revisionato a intervalli appropriati (Sezione IV.A).

B) *Due diligence* e selezione dei fornitori di servizi

La Guida ritiene che gli intermediari dovrebbero valutare la profondità e l'accuratezza della *due diligence* dei possibili fornitori di servizi, in modo coerente con portata, complessità e importanza dell'accordo dell'*outsourcing* pianificato, tenendo altresì adeguatamente conto della reputazione del fornitore di servizi e della sua *familiarity* con l'istituto finanziario.

Più specificamente, la Sezione IV.B della Guida considera tre aree essenziali, nell'elezione di un potenziale fornitore di servizi:

- **background aziendale, reputazione e strategia**: segnatamente, status del fornitore nel settore; storia e reputazione aziendale; licenza e qualifica ed eventuali questioni legali o normative pendenti;

- **prestazioni e condizioni finanziarie**: quali, tra l'altro, il rendiconto finanziario più recente; la crescita della quota di mercato del servizio da parte del fornitore; la copertura assicurativa di questi e l'adeguatezza della revisione da parte del fornitore di servizi delle condizioni finanziarie di eventuali subappaltatori;

- **controlli interni**, con particolare riferimento a: controlli di accesso; formazione dei dipendenti; sicurezza dei dati e informatica; protezione dei dati per le informazioni sensibili; conservazione dei dati; supporto clienti e servizi; rispetto delle leggi e dei regolamenti.

1.2.3 Ruolo dell'Alta Dirigenza

La Sezione III della Guida raccomanda che l'Alta Dirigenza stabilisca *policy* che governino l'utilizzo del fornitore di servizi e forniscano una gestione efficace delle relazioni e delle attività di Terze Parti.

Le suddette linee di condotta dovrebbero stabilire un programma di gestione del rischio del fornitore di servizi che affronti la valutazione del rischio e la suddetta *due diligence* (v. *supra*), gli *standards for contract provisions and considerations*, il monitoraggio continuo dei fornitori di servizi e la continuità aziendale, la pianificazione di emergenza.

Al riguardo, i Vertici dovrebbero essere responsabili dell'adeguata attuazione di tali politiche: questo è uno snodo critico determinante per traguardare efficacemente le misure delineate che, altrimenti, rischiano di rimanere una mera dichiarazione di intenti.

Infine, il *Top management* dovrebbe fornire al Consiglio di amministrazione dell'ente informazioni sufficienti sui possibili e attuali accordi di esternalizzazione, in modo che il consesso amministrativo possa comprendere pienamente i rischi posti dalle suddette convenzioni.

1.2.4 Remunerazione degli incentivi

Gli enti finanziari dovrebbero, poi, valutare attentamente la concessione di qualsiasi incentivo che possa essere incorporato nei contratti con i fornitori di servizi, valutando, in particolare, se tali benefici possano indurre il fornitore di servizi ad assumersi rischi inutili: con danni alla reputazione, aumento del contenzioso o altri rischi per l'intermediario stesso (Sezione IV. D).

vedi l'articolo online

1.2.4 Supervisione e monitoraggio

Secondo la Sezione IV.E della Guida, il processo di supervisione, compreso il livello e la frequenza del reporting gestionale, dovrebbe essere focalizzato sul rischio. Gli enti dovrebbero, in proposito, stabilire i processi per misurare le prestazioni rispetto ai livelli di servizio richiesti contrattualmente e definire la frequenza delle revisioni delle prestazioni, rispetto al profilo di rischio del fornitore di servizi.

Ad esempio, i fornitori di servizi a rischio più elevato potrebbero opportunamente richiedere valutazioni e monitoraggi più frequenti.

2. L'esperienza UE

2.1 DORA

Il 16 gennaio 2023, è stato emanato il Regolamento UE sulla resilienza operativa digitale, (*Digital Operational Reslience Act*, noto con l'acronimo DORA), che entrerà in vigore il 17 gennaio 2025, che mira a favorire lo sviluppo dei servizi digitali, armonizzando e rafforzando i presidi di sicurezza tecnica e di *governance* degli intermediari vigilati, anche con riferimento, appunto, ai servizi informatici e tecnologici forniti da soggetti terzi.

Si legge, al riguardo, nel "Considerando" n. 29 del citato provvedimento che "*anche se il diritto dell'Unione in materia di servizi finanziari contiene talune norme generali in materia di esternalizzazione, il monitoraggio della dimensione contrattuale non è sempre saldamente radicato nel diritto dell'Unione. In assenza di norme dell'Unione che si applichino in maniera chiara e mirata alle disposizioni contrattuali stipulate con fornitori terzi di servizi ICT, la fonte esterna dei rischi informatici rimane una questione non adeguatamente affrontata*".

"*È pertanto necessario stabilire alcuni principi fondamentali che indirizzino la gestione, da parte delle entità finanziarie, dei rischi informatici derivanti da terzi, che sono di particolare importanza quando le entità finanziarie ricorrono a fornitori terzi di servizi ICT a supporto delle loro funzioni essenziali o importanti*".

I suddetti "*principi sono complementari alla normativa settoriale applicabile all'esternalizzazione*".

L'attuale normativa di settore, difatti, regola in maniera puntuale unicamente i rapporti di esternalizzazione, con particolare riferimento a quelli riguardanti le funzioni essenziali o importanti. La nuova disciplina, invece, trova applicazione in relazione a tutti i "*contractual arrangement*" instaurati tra operatori del settore finanziario e fornitori terzi, purché tali accordi riguardino l'uso di servizi di *Information and Communication Technologies*, e, quindi, non solo ai contratti di esternalizzazione[4].

Con specifico riferimento all'*outsourcing*, il Regolamento DORA unifica la regolamentazione in materia delle attività ICT per l'intero settore finanziario. Rispetto alla *Direttiva NIS2* - anch'essa adottata a fine 2022 - che regola i requisiti generali di sicurezza digitale, DORA rappresenta, inoltre, una normativa specifica.

I requisiti derivanti dalla regolamentazione dell'esternalizzazione per gli enti finanziari riguardano, sostanzialmente, due aree: la creazione di un sistema interno per la gestione del rischio di esternalizzazione e l'integrazione specifica dei requisiti normativi negli accordi contrattuali con fornitori di servizi terzi.

2.1.1 Sistema interno di gestione dei rischi

In relazione al primo profilo (che qui interessa, per l'economia del presente lavoro), "p*er un solido monitoraggio dei rischi informatici derivanti da terzi nel settore finanziario, è necessario stabilire una serie di norme basate su principi che guidino le entità finanziarie nel monitoraggio dei rischi che si presentano nel contesto di funzioni esternalizzate a fornitori terzi di servizi ICT, in particolare per i servizi ICT a supporto di funzioni essenziali o importanti, nonché più in generale nel contesto di tutte le dipendenze da terzi nel settore delle ICT*" (*Considerando* n. 62 del *Regolamento*).

Lo sviluppo di un sistema interno funzionante per la gestione dei rischi derivanti dall'esternalizzazione dei servizi di *Information and Communication Technologies* è responsabilità primaria dell'Autorità capofila, nell'ambito della sana e prudente gestione dei fornitori dei suddetti servizi, in ragione dell'evidente

4 Vedi A. Portolano, J. Mazza, "Regolamento DORA: novità in arrivo per i contratti di fornitura dei servizi ICT", in *Agendadigitale.eu*, 28 giugno 2023.

vedi l'articolo online

rilevanza assunta da questi ultimi, per la stabilità del sistema finanziario[5].

A questo proposito, è particolarmente importante valutare se il servizio ICT esternalizzato supporta funzioni essenziali o importanti (servizio significativo) dell'entità finanziaria, poiché ciò determina l'entità dei requisiti di gestione del rischio associati.

Al riguardo, le tre Autorità europee di vigilanza (ESA's: *European Banking Authority; European Insurance and Occupational Pensions Authority; European Securities and Markets Authority*) hanno pubblicato, il 26 maggio 2023, un *discussion paper* - di seguito alla richiesta da parte della Commissione europea di una consulenza tecnica - per specificare i criteri per la valutazione dei **fornitori terzi di servizi di ICT critici** ("*Crithical Third Party Providers*" – CTPP).

Tra i criteri identificati: l'impatto sulle forniture di servizi finanziari (in termini di stabilità, continuità e qualità); l'importanza delle entità finanziarie (in termini di rilevanza e carattere sistemico); le funzioni critiche o importanti da affidare a fornitori esterni; il grado di sostituibilità del fornitore esterno.

Inoltre, per ciascuno dei suddetti criteri, si propongono indicatori quantitativi e qualitativi rilevanti, insieme alle informazioni necessarie per la loro costruzione e interpretazione.

I suddetti indicatori sono stati poi individuati e specificati, dalle stesse Autorità, in un successivo documento, del 29 settembre 2023, insieme alle informazioni necessarie per costruirli e interpretarli.

Le ESAs propongono, inoltre, soglie minime di rilevanza, per gli indicatori quantitativi, ove applicabili, da utilizzare come punti di partenza nel processo di valutazione per designare i fornitori terzi critici.

In proposito, DORA prescrive che gli enti finanziari saranno tenuti a notificare anticipatamente all'Autorità di vigilanza[6] la prevista conclusione di un contratto di *outsourcing*; a verificare il rispetto degli standard di sicurezza da parte dei fornitori di servizi terzi; e, infine, a mettere in atto una strategia per la risoluzione del rapporto contrattuale.

La suddetta strategia deve garantire che la risoluzione del rapporto contrattuale con il fornitore terzo non metta a repentaglio l'operatività dell'entità finanziaria e il rispetto dei requisiti normativi né comporti un deterioramento della qualità dei servizi forniti ai clienti durante la transizione periodo. In tale ambito, gli enti finanziari devono altresì stabilire un piano per migrare verso un fornitore di servizi terzo alternativo o per garantire la propria fornitura dei servizi pertinenti.

Con riferimento, poi, alla gestione interna del rischio, di particolare significatività la disposizione in base alla quale le entità finanziarie saranno tenute a effettuare una **valutazione preliminare** dei benefici e dei rischi dei servizi ICT significativi recentemente esternalizzati, in termini di potenziale sostituibilità del fornitore esternalizzato e di concentrazione di più servizi ICT significativi con il fornitore terzo, prestatore di servizi o prestatori di servizi ad esso strettamente legati.

Al riguardo, sarà plausibilmente compito dell'OdV verificare la sufficiente resilienza digitale per modelli di business, in cui la maggior parte dei servizi ICT significativi sono esternalizzati, ad esempio, a un unico fornitore di servizi terzo.

Un altro profilo di particolare rilievo è rappresentato dall'obbligo, da parte degli enti finanziari, di **monitorare** se: a) eventuali catene di subfornitura a terzi fornitori di servizi ICT significativi facciano riferimento a Paesi esterni all'Unione Europea; b) la lunghezza o complessità delle medesime comportino un rischio per la fornitura dei servizi concordati; c) ovvero, infine se compromettano un controllo efficace.

2.2 RTS e ITS

Pubblicati, il 19 giugno 2023, da parte delle ESA's, quattro *documenti di consultazione* relativi a progetti di norme tecniche di regolamentazione e di attuazione - bozze di *Regulatory technical standards* (RTS)

5 "*L'Autorità di sorveglianza capofila può, con semplice richiesta o mediante decisione, imporre ai fornitori terzi critici di servizi ICT di trasmettere tutte le informazioni necessarie all'Autorità di sorveglianza capofila per adempiere i propri compiti ai sensi del presente regolamento, tra cui tutti i pertinenti documenti aziendali od operativi, contratti, documentazione strategica, relazioni di audit sulla sicurezza delle ICT, segnalazioni di incidenti informatici, nonché qualsiasi informazione relativa ai soggetti cui il fornitore terzo critico di servizi ICT ha esternalizzato attività o funzioni operative.*" (art. 37, co. 1, del Regolamento)

6 Cfr., con riferimento all'Italia, il *Provvedimento BI del maggio 2023*, "Segnalazione in materia di esternalizzazione di funzioni aziendali per gli intermediari vigilati".

vedi l'articolo online

e di *Implementing Technical Standards* (ITS) - ai sensi del Regolamento DORA.

1) Il primo documento afferisce la determinazione dei requisiti delle *policy* degli enti finanziari, in materia di utilizzo di **fornitori di servizi ICT di Terze Parti**, e ribadisce il concetto secondo cui tale circostanza non può ridurre la responsabilità diretta degli enti finanziari e dei loro organi amministrativi nel gestire i propri rischi e rispettare i requisiti normativi, specialmente quando si tratti di funzioni critiche e importanti.

In proposito, pertanto, si dispone che le entità finanziarie assegnino chiaramente le responsabilità interne per l'approvazione, la gestione, il controllo e la documentazione degli accordi contrattuali sull'uso dei servizi ICT forniti da terzi.

2) Il secondo documento mira a definire modelli standard in relazione al **Registro delle informazioni**[7] su tutti gli accordi contrattuali per l'utilizzo di servizi ICT prestati da fornitori terzi.

Il suddetto fascicolo deve essere sempre reso disponibile per la consultazione su richiesta delle Autorità di vigilanza, in modo da ottenere informazioni essenziali per acquisire una più ampia comprensione delle dipendenze delle entità finanziarie in materia di ICT.

3) Il terzo documento mira alla definizione dei criteri per la classificazione degli **incidenti in ambito ICT**, delle soglie di rilevanza per gli incidenti gravi e le minacce informatiche significative.

Il progetto è dettagliato in tre sezioni, le quali contengono: una classificazione degli incidenti ICT in base a determinati criteri; le caratteristiche per cui determinati incidenti debbano ritenersi di una certa gravità e determinate minacce debbano essere qualificate come significative; la portata, la rilevanza o l'impatto più o meno significativo che un incidente connesso alle ICT possa determinare su un altro Stato membro.

4) Infine, l'ultimo documento è emanato ai fini di un'ulteriore armonizzazione di strumenti, metodi, processi e politiche di **gestione del rischio informatico**.

7 Ai sensi dell'art. 28 del DORA, che richiede la detenzione del suddetto Registro da parte di tutti gli enti finanziari.

Segnatamente, il suddetto ITS, particolarmente articolato: individua le politiche di gestione del suddetto rischio, al fine di garantire la sicurezza delle reti, introdurre salvaguardie adeguate contro l'uso improprio dei dati e preservare l'integrità e la riservatezza degli stessi; specifica i requisiti sui contratti, sulla gestione dell'identità e dell'accesso, al fine di sviluppare la politica sulle risorse umane; determina i meccanismi per individuare tempestivamente le attività anomale; specifica le componenti della politica di continuità operativa delle ICT; individua i test sui piani di continuità operativa delle ICT; determina le componenti dei piani di risposta e ripristino relativi alle ICT.

I riscontri della *consultazione pubblica* che ne è seguita - accogliendo una buona parte delle osservazioni e delle preoccupazioni specifiche del settore - hanno positivamente impattato sull'originaria trama normativa: con modifiche specifiche delle richiamate disposizioni tecniche, che hanno conseguito una maggiore semplificazione e razionalizzazione dei requisiti richiesti, nonché un più spiccato rispetto del principio di proporzionalità.

Di seguito, le tre Autorità di Vigilanza hanno pubblicato, il 17 gennaio 2024, la prima serie di *progetti definitivi di norme tecniche*[8] - elaborati ai sensi del Regolamento DORA[9] - volti a migliorare la **resilienza operativa digitale** del settore finanziario dell'UE, rafforzando i quadri delle tecnologie dell'informazione e della comunicazione (ICT) delle entità finanziarie e dei quadri di gestione dei rischi e di segnalazione degli incidenti di Terze Parti[10].

8 Si tratta, in particolare, dei seguenti 4 documenti:
- *"Final Report on Draft RTS to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554"*;
- *"Final Report on Draft ITS to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554"*;
- *"Final Report on Draft RTS on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554"*;
- *"Final Report on Draft RTS to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554"*.

9 Segnatamente, gli artt. 15, 16, par. 3, 18, par. 3, 28, parr. 9 e 28.

10 I suddetti progetti finali di norme tecniche dovranno essere sottoposti alla Commissione europea per l'approvazione, per poi passere al vaglio finale del Parlamento europeo e del Consiglio, prima della pubblicazione definitiva nella Gazzetta Ufficiale dell'Unione europea.

vedi l'articolo online

L'articolazione delle norme segue lo stesso schema utilizzato nei documenti di consultazione sopra dettagliatamente richiamati.

2.3 *Toolkit*

Nel novembre 2020, il *Financial Stability Board* ha pubblicato un *discussion paper,* su questioni regolamentari e di vigilanza relative all'esternalizzazione e ai rapporti di servizi con terzi.

Sulla base dei riscontri ricevuti in materia, nel settembre 2021, il Comitato permanente per la cooperazione in materia di vigilanza e regolamentazione (SRC) del FSB, ha deciso di sviluppare un kit di strumenti per le Autorità finanziarie, incentrato sulla **vigilanza sui fornitori di servizi critici**.

Nel giugno 2023, l'Autorità ha avviato una consultazione pubblica sul kit di strumenti proposto.

Infine, il 4 dicembre 2023, FSB ha pubblicato il suddetto *toolkit*, a beneficio, appunto, di Autorità e istituzioni finanziarie, per la gestione e la supervisione dei rischi da parte di terzi.

Lo strumentario in parola è stato sviluppato in risposta alle preoccupazioni circa l'entità e la natura delle interazioni degli istituti finanziari con un ecosistema ampio e diversificato di fornitori di servizi terzi, che potrebbero avere implicazioni per la stabilità finanziaria.

Non a caso, l'enfasi principale del suddetto strumentario è sui **servizi critici** di Terze Parti, dato il potenziale impatto della loro interruzione sulle operazioni critiche e sulla stabilità finanziaria degli istituti finanziari.

Al riguardo, occorre tener presente che la concentrazione nella fornitura di servizi di terzi non comporta, di per sé, rischi sistemici, né è intrinsecamente o invariabilmente problematica. Tuttavia, maggiore è la quota del settore finanziario che si affida a una Terza Parte, più significativo è il rischio per il sistema finanziario, in caso di fallimento o interruzione dei servizi forniti dalla terza parte.

Un altro fattore potenzialmente rilevante è rappresentato dalla sostituibilità dei servizi di terzi, che può derivare da: la mancanza di fornitori alternativi validi per uno o più servizi; le potenziali difficoltà (compresi i rischi) che le imprese possono incontrare durante la migrazione tempestiva dei servizi, in particolare dei servizi materiali, da un terzo all'altro (ovvero nuovamente all'interno dell'azienda).

La suddetta "cassetta degli attrezzi" mira a: i) ridurre la frammentazione degli approcci normativi e di vigilanza alla gestione del rischio di terzi nelle giurisdizioni e nelle diverse aree del settore dei servizi finanziari; ii) rafforzare la capacità degli istituti finanziari di gestire i rischi di terzi e la capacità delle Autorità finanziarie di monitorare e rafforzare la resilienza del sistema finanziario; iii) facilitare il coordinamento tra le parti interessate (ossia le Autorità finanziarie, gli istituti finanziari e i fornitori terzi di servizi).

Il *toolkit* promuove, inoltre, la comparabilità e l'interoperabilità degli approcci normativi e di vigilanza tra settori e giurisdizioni. Con tale finalità, esso comprende:

-un elenco di **termini e definizioni comuni** per migliorare la chiarezza e la coerenza in merito alla gestione del rischio di Terze Parti tra gli istituti finanziari;

- strumenti per aiutare gli istituti finanziari a **identificare i servizi critici** e a **gestire i potenziali rischi**, durante l'intero ciclo di vita di una relazione di servizio di Terze Parti;

- strumenti per la **supervisione**: segnatamente per l'identificazione, il monitoraggio e la gestione delle dipendenze sistemiche da Terze Parti e dei potenziali rischi sistemici.

3. L'esperienza UK

3.1 *Discussion paper*

Con il *Documento di discussione* (DP) 3/22 (Resilienza operativa: Terze Parti critiche per il settore finanziario del Regno Unito), pubblicato congiuntamente dalle Autorità di regolamentazione, è stato chiesto parere al mercato, su potenziali misure politiche per **gestire i rischi sistemici** generati da alcune Terze Parti al settore finanziario del Regno Unito e su come i servizi da esse forniti potrebbero essere resi più resilienti al fine di promuovere gli obiettivi delle Autorità di regolamentazione.

Il suddetto documento, preliminarmente, non sottaceva i potenziali benefici che i servizi forniti da terzi possono apportare agli intermediari e, pertanto, sottolineava il sostegno dato delle Autorità di regola-

vedi l'articolo online

mentazione all'uso sicuro e sostenibile di tali servizi.

Tuttavia, contestualmente, osservava che il fallimento di alcune Terze Parti, o gravi perturbazioni dei servizi materiali che forniscono, avrebbe potuto comportare rischi per la stabilità finanziaria e che, pertanto, era opportuno un intervento normativo.

Il *feed-back* ricevuto dal mercato (tra cui intermediari finanziari, fornitori e organismi del settore) nonché da esperti indipendenti può essere ricondotto ai seguenti temi-chiave:

- ampio sostegno al ventilato **intervento normativo**: la crescente dipendenza degli intermediari dalle Terze Parti[11] (CTP) potrebbe, difatti, comportare un rischio sistemico per gli obiettivi delle Autorità di regolamentazione: da qui la necessità di una maggiore vigilanza regolamentare diretta, basata su principi e proporzionata, senza limitare indebitamente, tuttavia, la capacità delle imprese e degli enti bancari e finanziari di scegliere fornitori terzi di servizi;
- **coordinamento e cooperazione internazionale**, in materia di regolamentazione e vigilanza.
- interazione con il **quadro normativo esistente**: la richiesta è di non imporre requisiti aggiuntivi agli intermediari e definire i rispettivi ruoli e responsabilità (intermediari, da un lato; CTP, dall'altro);
- **standard minimi di resilienza**, per i servizi forniti dai CTP;
- **condivisione delle informazioni**, tra le Autorità di regolamentazione e vigilanza e i vigilati, rispettando, tuttavia, la riservatezza e la sicurezza.

3.2 *Consultation paper*

Di seguito al suddetto DP, il 7 Dicembre 2023, è stato pubblicato un *Documento di Consultazione* (CP26/23) – anche in questo caso, emesso congiuntamente da *Prudential Regulation Authority* (PRA), *Financial Conduct Authority* (FCA) e *Bank of England*[12] - con cui sono stabiliti i requisiti per i gestire i potenziali rischi per la stabilità o la fiducia nel sistema finanziario del Regno Unito, che possono derivare da un guasto o da un'interruzione dei servizi da parte di un CTP.

Al riguardo, occorre ricordare che il Comitato di politica finanziaria (FPC) della *Bank of England* supervisiona, ormai da diversi anni, i potenziali rischi sistemici posti dai CTP. Fin dalla *Relazione sulla stabilità finanziaria*, di giugno 2017, venivano, al riguardo, richiesti "aggiornamenti annuali alle Autorità finanziarie sulla resilienza informatica delle imprese che si trovano al di fuori del perimetro normativo, ma che sono importanti per il settore finanziario del Regno Unito".

Nel novembre 2018, FPC ha iniziato a monitorare attentamente i fornitori di servizi *cloud* (CSP), in particolare dopo aver osservato che, a causa dell'elevata concentrazione del mercato dei suddetti servizi, "l'interruzione di un fornitore, ad esempio a causa di un attacco informatico, potrebbe interferire con la fornitura di servizi vitali da parte di diverse imprese".

Successivamente, nel 2021, il suddetto consesso aveva concluso che "la crescente dipendenza da un numero limitato di CTP per servizi vitali potrebbe aumentare i rischi per la stabilità finanziaria in assenza di un maggiore controllo regolamentare diretto sulla resilienza dei servizi che forniscono".

11 CTP è un'entità che sarà designata dal Dipartimento del Ministero del Tesoro (HMT), mediante un Regolamento emanato nell'esercizio del potere di cui all'articolo 312L, paragrafo 1, FSMA.
Al riguardo, HMT deve tenere conto de:
-la rilevanza dei servizi che il terzo fornisce agli intermediari, per la fornitura di attività, servizi o operazioni essenziali;
-il numero e il tipo di intermediari a cui la persona presta servizi.
Inoltre, HMT deve consultare ciascuna delle Autorità di regolamentazione prima della suddetta designazione. In pratica, ciò comporterà generalmente che le suddette Autorità raccomandino in modo proattivo a HMT di esercitare il suddetto potere, sulla base delle loro analisi dei dati e delle informazioni pertinenti.
Infine, come richiesto dall'articolo s312V FSMA, HMT presenterà al Parlamento il Memorandum d'intesa (MoU) delle Autorità di regolamentazione, che stabilirà come intendono coordinare l'esercizio delle rispettive funzioni in materia.

12 Ciascuna Autorità di regolamentazione ha il potere statutario di emanare norme per i CTP. Tuttavia, le medesime hanno anche il dovere, anch'esso statutariamente imposto, di coordinare l'esercizio delle rispettive funzioni di supervisione sui CTP (s312U della Legge sui servizi e i mercati finanziari del 2000 - FSMA), compresi i rispettivi poteri normativi.
Di conseguenza, sebbene le suddette Autorità abbiano obiettivi statutari diversi, i requisiti proposti per i CTP nel presente CP sono stabiliti in tre strumenti normativi identici ma distinti, emessi separatamente da ciascuna Autorità.

vedi l'articolo online

Con questa consapevolezza, sedimentata e rafforzata nel tempo, le Autorità di regolamentazione ritengono ora non più procrastinabile un intervento normativo: in tale ambito, le suddette proposte sembrano adeguate per il monitoraggio e la gestione dei rischi di cui sopra, in modo efficace ma proporzionato.

Ulteriore caratteristica positiva delle disposizioni in esame è rappresentato dalla circostanza che il regime di sorveglianza proposto per i CTP è stato concepito in modo da essere il più possibile interfacciabile con regimi analoghi esistenti e futuri, segnatamente con il *Regolamento DORA* e il BSA di cui sopra.

Le suddette proposte si tradurrebbero, in particolare, in:

- requisiti per i CTP nel *Bank Rulebook*, nel PRA *Rulebook* e nel FCA *Handbook*;
- una *Dichiarazione di vigilanza* congiunta Banca/PRA/FCA, che illustri le aspettative delle Autorità di regolamentazione in merito al modo in cui i CTP dovrebbero conformarsi e interpretare i requisiti proposti nelle loro norme.

La *Bank of England* e PRA intendono inoltre avviare, a tempo debito, una consultazione su una *Dichiarazione congiunta di policy*, in relazione all'uso dei loro **poteri disciplinari** nei confronti dei CTP, allineata al più ampio riesame in corso dell'applicazione delle norme.

Le Autorità di regolamentazione propongono di individuare i potenziali CTP, valutando i terzi in base a:

- **rilevanza** dei servizi forniti;
- **concentrazione** dei servizi: pertanto, più servizi distinti forniti dallo stesso fornitore rilevano in aggregato se la loro perturbazione o il loro fallimento combinati possano minacciare la stabilità o la fiducia nel sistema finanziario.

  Come peraltro indicato nel citato *toolkit* FSB (v. *supra,* par. 2.3) la concentrazione nella fornitura di servizi di terzi non comporta automaticamente rischi sistemici, né è intrinsecamente o invariabilmente problematica. La concentrazione può tuttavia riflettere la qualità, compresa la resilienza, dei servizi di terzi; inoltre, maggiore è la quota del settore finanziario che si affida a una Terza Parte, più spiccato è il rischio per il sistema finanziario nel suo complesso, in caso di fallimento o interruzione dei servizi forniti dal fornitore;
- **altri fattori** di potenziale impatto sistemico, ad esempio:

  a) la **sostituibilità** dei servizi (in particolare i servizi materiali), che può derivare da: la mancanza di fornitori alternativi validi per uno o più servizi; le potenziali difficoltà che le imprese possono incontrare durante la migrazione tempestiva dei servizi, da un terzo all'altro;

  b) l'**accesso diretto**, da parte del fornitore, alle persone, ai processi, alle tecnologie, alle strutture, ai dati e alle informazioni (le «risorse») degli intermediari che supportano la fornitura di importanti servizi alle imprese.

Le suddette Autorità esamineranno periodicamente se un CTP continua a soddisfare i criteri per tale denominazione - eventualmente segnalando eventuali modifiche (ad es. potenziali nuovi servizi materiali, o servizi precedentemente materiali che potrebbero non essere più rilevanti) - e aggiorneranno di conseguenza HMT.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it