DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

Esternalizzazioni ICT: tra Regolamento DORA e Orientamenti EBA

Marzo 2025

Emilio Fabbiani, , Ufficio Consulenza Legale, Banca Etica
Andrea Carnaccini, Ufficio Consulenza Legale, Banca Etica
Federico Bernardi,Ufficio Consulenza Legale, Banca Etica
Clelia Piscopo, Ufficio Consulenza Legale, Banca Etica

Emilio Fabbiani, Ufficio Consulenza Legale, Banca Etica

Andrea Carnaccini, Ufficio Consulenza Legale, Banca Etica

Federico Bernardi, Ufficio Consulenza Legale, Banca Etica

Clelia Piscopo, Ufficio Consulenza Legale, Banca Etica

Emilio Fabbiani
Emilio Fabbiani è Professore incaricato presso la Facoltà di Giurisprudenza Università Telematica Pegaso. Avvocato, già iscritto al Foro di Venezia. Socio AIGI – Associazione Giuristi d'Impresa. Ha collaborato e collabora con diverse riviste giuridiche ed è componente del Gruppo di Lavoro Abi in tema di governance.

Sommario: 1. Gerarchia delle fonti: poteri di *hard law* e *soft law* in capo ad EBA - 2. Il rapporto tra gli Orientamenti EBA e il Regolamento DORA - 3. Recepimento delle linee guida EBA da parte di Banca d'Italia - 4. Orientamenti EBA dell'11 febbraio 2025 – 5. Conclusioni

[*] 1. Gerarchia delle fonti: poteri di *hard law* e *soft law* in capo ad EBA

Preliminarmente è bene porre alla base del ragionamento in oggetto la struttura del sistema normativo europeo con particolare attenzione alle norme di rango primario (Trattati fondamentali), di rango secondario (Regolamenti UE - applicabili in sè per sè - e Direttive UE - lasciando liberi i singoli Stati sulle modalità di attuazione), dei poteri di *hard law* (RTS "*Regulatory Technical Standards*" e ITS "*Implementing Technical Standards*") e *soft law* (orientamenti, raccomandazioni, pareri, etc.) delle Autorità di Vigilanza europee (ESAs) o, nel caso di specie, dell'EBA (European Banking Authority)[1].

Più nel dettaglio, i poteri di ***hard law*** sono riferibili allo sviluppo di progetti di norme tecniche di regolamentazione (RTS), che la Commissione è chiamata a realizzare nell'ambito delle sue funzioni, seguendo le direttive delle normative UE sui servizi finanziari e in conformità con l'art. 290 TFUE (Trattato sul Funzionamento dell'Unione Europea). Quest'ultimo regola i limiti e l'ambito delle deleghe agli organi esecutivi riguardo l'adozione di atti non legislativi di natura generale.

La seconda categoria si riferisce al potere di redigere progetti delle norme tecniche di attuazione (ITS), quando la normativa europea conferisce alla Commissione il compito di stabilire condizioni uniformi per l'applicazione del diritto dell'UE, ai sensi dell'art. 291, paragrafo 2, del TFUE.

Tali atti sono di natura tecnica e non politica e l'EBA non detiene il potere di adottare atti finali in modo

---

* *Le opinioni qui espresse sono a puro titolo personale e non impegnano l'Istituto di appartenenza.*

1 Per una disamina completa sul ruolo e i poteri dell'EBA si consiglia la lettura dell'ottimo contributo di Vese D., *A Game of Thrones: ruolo e poteri dell'autorità bancaria europea alla luce degli orientamenti della Corte di Giustizia*, Rivista di Diritto Bancario, Fascicolo I, 2023, https://rivista.dirittobancario.it/game-thrones-ruolo-e-poteri-dellautorita-bancaria-europea-alla-luce-degli-orientamenti-della-corte .

autonomo. La sua funzione si limita infatti a presentare alla Commissione i progetti che ha redatto, la quale ha il potere di approvarli, (trasfondendoli in Regolamenti o Direttive), modificarli con emendamenti o respingerli del tutto.

Tuttavia, la rilevanza dei poteri riconosciuti all'EBA è confermata dalla forza vincolante delle norme tecniche di regolamentazione e attuazione da essa predisposte, che, nel caso in cui la Commissione ritenesse di non adottare dovrebbe motivarne le ragioni.

I poteri di ***soft law*** dell'EBA hanno la funzione di interpretazione del diritto positivo dell'UE al fine di indirizzare le autorità nazionali degli Stati membri verso prassi di vigilanza efficaci ed efficienti. Per tale motivo, l'EBA è responsabile dell'adozione di Orientamenti (*Guidelines* o Linee Guida) e raccomandazioni allo scopo di creare standard prudenziali per garantire l'attuazione uniforme del diritto dell'UE nel settore bancario.

A differenza delle norme secondarie UE, i poteri di *soft law* delle Autorità di Vigilanza europee non sono pienamente vincolanti per gli Stati membri, nonostante abbiano un valore rafforzato. Per assicurare l'efficacia di questi atti di *soft law*, il legislatore europeo ha introdotto il regime del cosiddetto "*comply or explain*". Secondo tale meccanismo, i soggetti destinatari sono tenuti a fare il massimo sforzo per allinearsi (*comply*) agli orientamenti e alle raccomandazioni. Tuttavia, se un'autorità decide di non conformarsi, è obbligata a informare l'EBA entro due mesi dalla pubblicazione degli atti, fornendo adeguate spiegazioni sul motivo del mancato adeguamento (*explain*); non sono previste, in questo caso, procedure sanzionatorie.

Per quanto oggetto del presente lavoro, ossia della prevalenza - o meno - del Regolamento DORA[2] per quanto riguarda i contratti di esternalizzazione ICT rispetto agli Orientamenti EBA in materia di *outsourcing*[3], già ad una prima analisi della gerarchia delle fonti si può ritenere, come si vedrà nel prosieguo, che la portata degli Orientamenti emanati dalle Autorità di Vigilanza Europee si ponga come residuale rispetto a quanto previsto da Regolamenti o Direttive.

2 Regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario - Digital Operational Resilience Act (DORA)

3 Per un approfondimento sulle EBA *Guidelines on Outsourcing arrangements* del 2019 cfr. Casamassima S., *Le regole di governance in tema di esternalizzazione delle funzioni*, in *L'outsourcing nei servizi bancari e finanziari*, Casamassima S., Nicotra M. (a cura di), Milano, 2021, 31.

2. Il rapporto tra gli Orientamenti EBA e il Regolamento DORA

I considerando introduttivi del Regolamento DORA manifestano lo scopo primario dell'atto, che è quello di compendiare la complessità di fonti europee in tema ICT (*Information Communication Technology)* e di istituire un "*quadro comune*"[4] di regolamentazione[5].

Nel considerando n. 10 del Regolamento, infatti, il legislatore europeo ravvisa una certa parzialità di trattazione dei rischi informatici e propone un'armonizzazione del mercato interno sul nuovo piano della "*digital resilience*", in linea con l'articolo 114 del TFUE sul ravvicinamento delle legislazioni degli Stati membri, già richiamato come base giuridica dalla NIS2[6].

Il DORA non si concentra più sulla mera gestione del rischio, ma - appunto - vuole tradurre in concreto il concetto di resilienza operativa, potenziando gli obblighi delle entità finanziarie al fine di una maggiore resistenza preventiva - e non solo nel porre rimedio successivamente - agli attacchi e incidenti informatici.

Se la "cybersicurezza" definita dall'articolo 2, punto 1), del Regolamento in materia (Reg. (UE) 2019/881)[7] era definita come il complesso degli interventi che messi in campo per la protezione dalle minacce informatiche, la "cyber resilienza" diviene la capacità dell'entità finanziaria di "*costruire, assicurare e riesaminare*" la propria integrità e affidabilità operativa[8].

4 Considerando n. 14 del Regolamento DORA.

5 Sulla gestione dei rischi ICT alla luce del nuovo Regolamento DORA, si segnala l'articolo di: Lucantoni P., Villani C., *La gestione e supervisione dei rischi ICT e di sicurezza nelle attività finanziarie esternalizzate tra DORA e CRD VI*, Dialoghi di diritto dell'Economia, Fascicolo 1, Gennaio 2025

6 *Network and Information Security directive*, (2022/2555)

7 Regolamento UE sulla cybersicurezza e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, (UE) 2019/881 pubblicato in GUCE in vigore dal 27.06.2019

8 Articolo 3 n. 1) del Regolamento DORA.

vedi l'articolo online

Peraltro, rispetto a tale disciplina sulla cybersicurezza e, in particolare, con riguardo alla direttiva NIS2, è lo stesso Regolamento DORA a definirsi *lex specialis*[9].

In materia di servizi ICT, il DORA attua una regolamentazione anche sui contratti di fornitura da parte di terzi[10], materia su cui l'Autorità Bancaria Europea aveva già emanato appositi orientamenti (EBA/GL/2019/02 Orientamenti EBA in materia di esternalizzazione; EBA/GL/2019/04 Orientamenti EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione e di sicurezza), con particolare riguardo alle esternalizzazioni.

Tali orientamenti[11] affrontavano - già prima del DORA - alcuni dei temi connessi al rischio di esternalizzazione dei servizi, valutandoli sia nel campo delle esternalizzazioni di servizi ICT (*Information Communication Tecnology*) che in quelle di servizi non ICT.

Gli orientamenti EBA precisano infatti che i destinatari delle norme debbano occuparsi dei rischi connessi alle esternalizzazioni, "***anche***" - e dunque non soltanto - relativamente ai servizi informatici[12].

Di contro, il DORA pone l'obiettivo di disciplinare la gestione del rischio informatico in tutti gli aspetti in cui i servizi ICT possano essere coinvolgibili e dunque di regolamentare la dipendenza delle entità finanziarie dagli stessi.

In tema di subappalto, ad esempio, l'articolo 31 del Regolamento DORA prescrive che, per la designazione dei fornitori critici, le entità finanziarie devono tenere in conto anche la propria dipendenza dai servizi prestati dal fornitore terzo di servizi ICT, in rapporto alle funzioni essenziali o importanti, **indipendentemente** dal fatto che la dipendenza dell'entità finanziaria da tali servizi sia diretta o indiretta tramite accordi di subappalto (*subcontractors*).

Il rischio va dunque valutato complessivamente, considerando potenziali *default* dei servizi ICT di cui beneficia a propria volta il fornitore terzo mediante *subcontracting arrangements* e di cui l'entità finanziaria si serva anche indirettamente.

Le *Guidelines* EBA in materia di esternalizzazioni adottano poi una visione meno estesa rispetto al DORA e più concentrata sulla difficoltà di controllo da parte dei destinatari in caso di sub esternalizzazioni a catena coinvolgenti funzioni essenziali o importanti (FEI).

Un differente approccio disciplinare del nuovo Regolamento si rileva anche rispetto agli orientamenti EBA/GL/2019/04 sulla gestione dei rischi ICT. In tali orientamenti, l'Autorità di Vigilanza Europea definisce il rischio ICT di sicurezza come rischio operativo di perdita dovuto ad eventi specifici quali: la violazione della riservatezza, la carente integrità dei sistemi e dei dati, l'inadeguatezza o l'indisponibilità degli stessi o l'incapacità di sostituire la tecnologia dell'informazione (IT) e gli attacchi informatici.

Rispetto alle suddette *Guidelines*, l'articolo 3 ("*Definizioni*") del Regolamento presenta una definizione notevolmente più aperta di rischio ICT, con conseguente maggior ampiezza del perimetro di applicazione: il rischio informatico è infatti individuato come una "*qualunque circostanza*", ragionevolmente identificabile come rischio in relazione all'uso dei sistemi informatici anche nella previsione che, qualora si concretizzi, l'evento sia idoneo a compromettere la sicurezza dei sistemi informatici.

Le definizioni del Regolamento DORA hanno allo stesso tempo un carattere molto più analitico rispetto ai precedenti orientamenti[13]. Difatti il legislatore europeo dettaglia le tipologie di rischio informatico che le entità finanziarie devono impegnarsi a prevenire.

Maggiore analiticità del DORA rispetto agli orientamenti EBA si riscontra anche sul piano della disciplina dei contratti con i fornitori terzi dei servizi ICT.

9 Vedasi combinato disposto tra l'articolo 4 co. 1 della NIS2 e articolo 1 par. 2 DORA, nonché considerando n. 16 DORA.

10 Per una sintesi dei principali obblighi applicabili alle entità finanziarie sui requisiti applicabili ai fornitori terzi di servizi ITC, Cfr. La Sala E., Ghiandai G., *DORA: caratteristiche e focus sulla gestione del rischio di terze parti*, Il Quotidiano Giuridico, 31 luglio 2024.

11 Si ricorda la definizione di *esternalizzazione* contenuta negli Orientamenti EBA (EBA/GL/2019/02) consistente in *Un accordo di qualsiasi forma tra un ente, un istituto di pagamento o un istituto di moneta elettronica e un fornitore di servizi in base al quale quest'ultimo svolge un processo, un servizio o un'attività che sarebbe altrimenti svolto/a dall'ente, dall'istituto di pagamento o dall'istituto di moneta elettronica stesso*.

12 Rif. Titolo III. *Quadro di governance* par. 5 n. 32 degli Orientamenti EBA (EBA/GL/2019/02).

13 Si veda la distinzione fatta dal Regolamento DORA tra *"incidente operativo o di sicurezza dei pagamenti"*, *"attacco informatico"* e *"minaccia informatica"*, non presente invece negli Orientamenti EBA sul rischio informatico.

vedi l'articolo online

L'articolo 30 del Regolamento in commento sembra riprendere quanto già previsto negli Orientamenti EBA in materia di esternalizzazioni di funzioni essenziali o importanti (rif. par. 28) e arricchirlo di ulteriori dettagli e clausole che il contratto con il fornitore terzo deve prevedere. Nel DORA sono indicate infatti le principali disposizioni contrattuali dei contratti sottoscritti con tutti i fornitori terzi di servizi ICT, specificando eventualmente le clausole ulteriori da prevedere ove siano coinvolte funzioni essenziali o importanti (FEI).

Il Regolamento si dota quindi di una "doppia lente".

Da un lato viene applicata una disciplina *grandangolare* a tutti i contratti che coinvolgono fornitori terzi di servizi ICT; dall'altro lato il contratto con il fornitore è passato al vaglio *microscopicamente*, imponendo l'inserimento di determinate clausole e con l'introduzione di diverse novità rispetto agli orientamenti EBA, alzando il livello di presidio nel caso di contratti a supporto di funzioni essenziali. Tra queste si pensi all'obbligo in capo al fornitore di servizi ICT - previsto nell'articolo 30 del DORA co. 3 lett. d) - di partecipare e cooperare pienamente al test avanzato di simulazione di cyber attacchi (TLPT - *Threat Led Penetration Testing*) dell'entità finanziaria, disposizione che mostra di nuovo l'approccio di maggior prevenzione rispetto alle precedenti *Guidelines* EBA.

Considerata la gerarchia delle fonti sopra riportata e il grado di fonte "primaria" del diritto europeo del Regolamento DORA rispetto agli orientamenti EBA di natura secondaria, deve anche notarsi che il ruolo di *lex specialis* del DORA è evidente in diversi altri punti e non solo sul piano dei contratti (ad es. il diritto di accesso, di informazione e di audit, previsto già da EBA e ampliato in DORA).

Il subentro del Regolamento ha pertanto determinato l'ancillarità degli Orientamenti dell'EBA in materia di esternalizzazioni e di rischi ICT, che restano di riferimento per quanto non regolato dal *Digital Operational Resilience Act*.

Ferma restando quindi la volontà di colmare la carenza di omogeneità della normativa nel settore ICT, è lo stesso Regolamento a definire i propri principi fondamentali come "complementari" rispetto alle norme generali già presenti in ambito europeo in materia di esternalizzazioni (considerando 29)[14].

In accordo con gli *statement* del DORA, il 30 dicembre 2024 Banca d'Italia ha pubblicato una comunicazione in cui il *framework* armonizzato in materia di *governance*[15] del rischio ICT viene definito in continuità con gli Orientamenti dell'EBA in materia[16].

3. Recepimento delle linee guida EBA da parte di Banca d'Italia

In data 25 febbraio 2019 l'EBA ha pubblicato il documento contenente gli **"Orientamenti in materia di esternalizzazione"** (*Guidelines on outsourcing arrangements* - EBA/GL/2019/02) che "*specificano i dispositivi di governance interna, tra cui una rigorosa gestione dei rischi, che gli enti, gli istituti di pagamento e gli istituti di moneta elettronica dovrebbero attuare quando esternalizzano le proprie funzioni, in particolare in caso di esternalizzazione di funzioni essenziali o importanti.*"

Tali orientamenti hanno trovato applicazione a far data dal 30 settembre 2019[17] a tutti gli accordi di

14 Considerando n. 29 Reg. Dora: "*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 TIC, 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 TIC a supporto delle loro funzioni essenziali o importanti. Tali principi dovrebbero essere accompagnati da una serie di diritti contrattuali di base concernenti vari elementi dell'esecuzione e della risoluzione degli accordi contrattuali, al fine di fornire alcune garanzie minime per rafforzare la capacità delle entità finanziarie di monitorare efficacemente tutti i rischi informatici che insorgano a livello di fornitori di servizi terzi. Tali principi sono complementari alla normativa settoriale applicabile all'esternalizzazione*".

15 Per un'agile trattazione in materia dell'impatto DORA sulla governance bancaria si legga: Casamassima S., *Cybersecurity: l'impatto della Regolamentazione DORA sulla governance bancaria e finanziaria*, Il Quotidiano Giuridico, 06 giugno 2024.

16 https://www.bancaditalia.it/media/approfondimenti/2024/regolamento-dora/index.html

17 Il paragrafo 63, lettera b), si applica a partire dal 31 dicembre 2021. Nell specifico ivi si specifica che "*Gli enti e gli istituti di pagamento dovrebbero assicurare che l'esternalizzazione di funzioni relative alle attività bancarie o ai servizi di pagamento, nella misura in cui lo svolgimento di tali funzioni richiede l'autorizzazione o la registrazione da parte di un'autorità competente nello Stato membro in cui essi sono autorizzati, a un fornitore di servizi situato in un paese terzo, avvenga solo se sono soddisfatte le seguenti condizioni: ...(omissis)...b) esiste un apposito accordo di*

vedi l'articolo online

esternalizzazione conclusi, rivisti o modificati a partire da tale data. Gli Orientamenti prevedevano che gli enti e gli istituti di pagamento avrebbero dovuto revisionare e conformare ad essi gli accordi di esternalizzazione esistenti e che, qualora le scadenze previste per tale aggiornamento non fossero state rispettate, avrebbero dovuto informare la propria autorità competente. segnalando le misure previste per completare la revisione o l'eventuale *exit strategy*.

L'Autorità di Vigilanza italiana ha accolto i suddetti orientamenti pubblicando sul proprio sito in data 23 settembre 2020 il 34° aggiornamento della Circolare n. 285 del 17 dicembre 2013 "Disposizioni di Vigilanza per le banche" e prevedendone l'entrata in vigore dal giorno successivo per tutti gli accordi di esternalizzazione conclusi, rinnovati o modificati a partire da tale data.

Le modifiche più rilevanti in materia di esternalizzazioni sono state le seguenti:

- l'istituzione e l'aggiornamento del c.d. "Registro delle attività esternalizzate", documento destinato a contenere informazioni salienti tra cui la data di inizio e di rinnovo del contratto di esternalizzazione, la data di scadenza, la descrizione dettagliata della funzione esternalizzata, l'indicazione se la funzione esternalizzata va considerata "Funzione Essenziale o Importante" o meno ed i relativi criteri adottati per tale catalogazione;

- la previsione di un'analisi degli accordi di esternalizzazione e la valutazione dei relativi complessivi rischi;

- l'inserimento nei contratti di esternalizzazione di apposite clausole contrattuali (ad esempio, in caso di "Funzione Essenziale o Importante", che indichino la possibilità di sub-esternalizzare, i luoghi in cui sarà effettuata l'attività esternalizzata e/o in cui verranno conservati e trattati i relativi dati, disciplinino l'attuazione e la verifica dei piani di continuità operativa nonché il diritto di controllo e di audit sull'attività svolta dal fornitore, definiscano, con riguardo all'esternalizzazione delle "Funzioni Essenziali o Importanti", *exit strategies* in linea anche con i piani di emergenza e di continuità operativa della banca;

- specifici obblighi di notifica all'Autorità di Vigilanza, comprensivi del caso in cui un'attività già esternalizzata venga riclassificata come "Funzione Essenziale o Importante";

- la previsione, senza restrizioni e nel rispetto del principio di proporzionalità, dell'esternalizzazione al di fuori dal gruppo bancario di appartenenza dei compiti operativi delle funzioni aziendali di controllo.

L'Autorità di Vigilanza ha inoltre fissato un regime transitorio, esteso fino al 31 dicembre 2021, per dare la possibilità alle banche di completare il c.d. "Registro delle attività esternalizzate" con la documentazione inerente agli accordi di esternalizzazione già esistenti e di adeguare i relativi contratti, con la previsione di poter eventualmente comunicare alla BCE o alla Banca d'Italia lo sforamento della suddetta scadenza e la successiva data prevista per il completamento delle attività di adeguamento oppure l'eventuale strategia di uscita dal contratto di esternalizzazione.

Successivamente, in data 28 novembre 2019, l'EBA ha pubblicato dei nuovi Orientamenti denominati "**Orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology – ICT) e di sicurezza**" (*Guidelines on ICT and security risk management* - EBA/GL/2019/04) in adempimento del mandato dall'articolo 95, paragrafo 3, della direttiva 2015/2366 (PSD2)[18].

Con tali orientamenti vengono definite:

- le misure di gestione dei rischi che gli istituti finanziari[19] sono tenuti ad adottare per la gestione

cooperazione, ad esempio sotto forma di memorandum of understanding o di accordo a livello di collegio, tra le autorità competenti responsabili della vigilanza dell'ente e le autorità di vigilanza responsabili della vigilanza del fornitore di servizi;"

18 All'art. 95, par. 3 della PSD2 si legge quanto segue: "*Entro il 13 luglio 2017 l'ABE, in stretta collaborazione con la BCE e previa consultazione di tutti i portatori di interessi, anche quelli del mercato dei servizi di pagamento, tenendo conto di tutti gli interessi coinvolti, emana, in conformità dell'articolo 16 del regolamento (UE) n. 1093/2010, orientamenti relativi alla definizione, all'attuazione e al controllo delle misure di sicurezza comprese, se del caso, le procedure di certificazione.*".

19 Così come identificati al par. 9 degli orientamenti, essi ricomprendono: "*1) i prestatori di servizi di pagamento, quali definiti all'articolo 4, paragrafo 11, della PSD2 e 2) gli enti, vale a dire gli enti creditizi e le imprese di investimento secondo la definizione di cui all'articolo 4, paragrafo 1, punto 3), del regolamento (UE) n. 575/2013. I presenti orienta-*

vedi l'articolo online

dei rischi relativi all'uso delle tecnologie dell'informazione e della comunicazione (*Information and Communication Technology – ICT*) e alla sicurezza per tutte le attività;

- le misure di gestione dei rischi operativi e di sicurezza relativi ai servizi di pagamento che i prestatori di servizi di pagamento sono chiamati ad adottare ai sensi dell'articolo 95, paragrafo 1, della PSD2[20].

La decorrenza dell'applicazione di tali orientamenti è stata fissata da EBA al 30 giugno 2020 con richiamo a quanto previsto dal Regolamento UE n. 1093 del 2010[21].

La Banca d'Italia ha accolto tali orientamenti pubblicando sul proprio sito, in data 3 novembre 2022, il 40° aggiornamento della citata Circolare n. 285 e fissandone l'entrata in vigore dal 4 novembre 2022 per le banche. Invece per gli IP (Istituti di Pagamento) e per il IMEL (Istituti di Moneta Elettronica) la data di inizio dell'applicazione dei nuovi orientamenti è stata posticipata al 12 novembre 2022[22]. (vedi Banca d'Italia Regolamento del 2/11/2022 modificativo le Disposizioni di Pagamento istituzioni e moneta elettronica istituzioni del 20 giugno 2012).

Con particolare riguardo al 40° aggiornamento della Circolare, sono state apportate modifiche al Capitolo 4 "Il sistema informativo" ed al Capitolo 5 "La continuità operativa" della Parte Prima, Titolo IV.

Tra le variazioni più rilevanti introdotte si evidenziano:

- la necessità per le banche di dotarsi di una funzione di controllo di secondo livello per la gestione e il controllo dei rischi ICT e di sicurezza;

- il rafforzamento dei compiti degli organi sociali, con particolare riguardo al Consiglio di Amministrazione quale Organo con Funzione di Supervisione Strategica (OFSS);

- l'importanza data alla c.d. "Strategia ICT" con la predisposizione di appositi piani di azione;

- la previsione di una revisione annuale di tutto il *framework* di gestione dei rischi ICT;

- la predisposizione di un inventario degli *asset* ICT e delle relative responsabilità ai fini della valutazione dei rischi ad essi afferenti;

- la previsione di misure di mitigazione dei rischi;

- l'opportunità di dotarsi di una policy di sicurezza dell'informazione;

- l'introduzione di nuovi adempimenti per i fornitori ICT non catalogati come esternalizzazioni;

- la necessità di garantire contrattualmente l'efficacia delle misure di attenuazione dei rischi definite dal proprio quadro di gestione dei rischi quando si fa ricorso a fornitori terzi, prevedendo in essi in particolare "*a) misure e obiettivi adeguati e proporzionati in materia di sicurezza dell'informazione, compresi i requisiti minimi di sicurezza informatica, specifiche relative al ciclo di vita dei dati dell'istituto finanziario ed eventuali requisiti relativi alla cifratura dei dati, alla sicurezza di rete e ai processi di monitoraggio della sicurezza, e l'ubicazione dei centri dati; b) procedure di gestione degli incidenti operativi e di sicurezza, tra cui notifica e attivazione dei livelli successivi*

menti si applicano inoltre alle autorità competenti quali definite all'articolo 4, paragrafo 1, punto 40), del regolamento (UE) n. 575/2013, compresa la Banca centrale europea relativamente ai compiti ad essa attribuiti dal regolamento (UE) n. 1024/2013, e alle autorità competenti ai sensi della PSD2, come indicato all'articolo 4, paragrafo 2, lettera i), del regolamento (UE) n. 1093/2010.".

20 L'articolo 95, paragrafo 1, della PSD2 dispone che "*Gli Stati membri assicurano che i prestatori di servizi di pagamento istituiscano un quadro di misure di mitigazione e meccanismi di controllo adeguati per gestire i rischi operativi e di sicurezza, relativi ai servizi di pagamento che prestano. Nell'ambito di tale quadro i prestatori di servizi di pagamento stabiliscono e gestiscono procedure efficaci di gestione degli incidenti, anche per quanto concerne l'individuazione e la classificazione degli incidenti operativi e di sicurezza gravi*".

21 L'art. 16, par. 3 dispone che "*Le autorità e gli istituti finanziari competenti compiono ogni sforzo per conformarsi agli orientamenti e alle raccomandazioni. Entro due mesi dall'emanazione di un orientamento o di una raccomandazione, ciascuna autorità nazionale di vigilanza competente conferma se è conforme o intende conformarsi all'orientamento o alla raccomandazione in questione. Nel caso in cui un'autorità competente non sia conforme o non intenda conformarsi, ne informa l'Autorità motivando la decisione. L'Autorità pubblica l'informazione secondo cui l'autorità competente non è conforme o non intende conformarsi agli orientamenti o alla raccomandazione. L'Autorità può anche decidere, caso per caso, di pubblicare le ragioni fornite da un'autorità competente riguardo alla mancata conformità all'orientamento o alla raccomandazione in questione. L'autorità competente riceve preliminarmente comunicazione di tale pubblicazione. Ove richiesto dall'orientamento o dalla raccomandazione in questione, gli istituti finanziari riferiscono, in maniera chiara e dettagliata, se si conformano all'orientamento o alla raccomandazione in parola.*".

22 Provvedimento della Banca d'Italia - Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica del 2 novembre 2022.

vedi l'articolo online

di intervento".

A seguito dell'introduzione nell'Ordinamento delle disposizioni DORA, la Banca d'Italia, al fine di dare continuità e coerenza alle varie disposizioni in materia, ha emanato una comunicazione (datata 30.12.2024) nella quale riportava l'attenzione degli intermediari sulle nuove norme in vigore.

In particolare, nella suddetta comunicazione si legge, tra le altre cose, che il Regolamento DORA disciplina la gestione del rischio ICT introducendo "*un framework armonizzato in materia di governance del rischio ICT, in continuità con gli Orientamenti dell'EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza (EBA/GL/2019/04) rivolti a banche, IP e IMEL e già recepiti nelle disposizioni di vigilanza della Banca d'Italia applicabili a questi intermediari*" ed inoltre che con riguardo alla gestione del rischio di terze parti derivante dal ricorso ai service provider ICT "*si sottopongono le entità finanziarie a presidi in linea con quelli previsti dagli Orientamenti dell'EBA in materia di esternalizzazione (EBA/GL/2019/02) e si introduce un regime europeo di oversight sui provider ICT critici*".

4. Orientamenti EBA dell'11 febbraio 2025

Abbiamo quindi visto da quanto precede che il quadro normativo in tema di esternalizzazioni e di rischio ICT è sicuramente complicato in relazione a quali norme si debbano applicare alle diverse situazioni, coesistendo norme di diverso rango e con *range* di applicazione a volte sovrapponibili.

Se la normativa predisposta da EBA in materia di "ICT *and security risk management*" (EBA/GL/2019/04) rappresentava una specificazione degli ulteriori presidi di sicurezza ed organizzativi previsti dai precedenti Orientamenti in materia di esternalizzazione (EBA/GL/2019/02) che ne costituivano il quadro di applicazione[23], oggi la disciplina contenuta nel Regolamento DORA si può definire come autonoma e indipendente, tale da poter essere utilizzata direttamente per tutto il perimetro degli accordi che riguardano il campo ICT.

Questa conclusione si può già trarre dalle norme esistenti che trattano di tutti gli aspetti già interessati

23 Si veda tutta la sezione 1.2.3 degli Orientamenti.

dai due Orientamenti citati; sia per per la parte generale di esternalizzazione (e in particolare ci riferiamo al contenuto degli accordi contrattuali) che per la parte di assetti organizzativi.

Il Regolamento DORA ripercorre e ridisegna le "strategie, politiche, procedure, protocolli e strumenti in materia di ICT necessari per proteggere debitamente ed adeguatamente tutti i patrimoni informativi"[24], senza quindi alcuna altra necessità di rifarsi agli Orientamenti EBA.

Questo è particolarmente vero in materia di contratti, posto che il Regolamento - all'articolo 30 - dispone una disciplina completa delle clausole minime necessarie da inserire negli accordi contrattuali, distinguendo tra contratti per l'utilizzo di servizi ICT e contratti per l'utilizzo di servizi ICT a supporto di funzioni essenziali, con ciò superando i contenuti degli orientamenti EBA (EBA/GL/2019/02) che al capitolo 13 prevede tutta una serie di prescrizioni per la maggior parte sovrapponibili alle indicazioni del Regolamento e da questo applicabili agli accordi in tema ICT: l'articolo 13 - Fase contrattuale - degli Orientamenti e l'articolo 30 del Regolamento utilizzano a volte le stesse espressioni e le stesse formulazioni giuridiche nel definire i contenuti minimi del contratto.

A questo si aggiunga che la materia contrattuale è trattata anche dal Regolamento Delegato 2024/1773 del 13 marzo 2024, riferito specificamente agli accordi contrattuali per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti prestate da fornitori terzi.

A livello ermeneutico risulterebbe quindi accertato non solo che la normativa di rango superiore prevalga su quella meramente regolamentare e peraltro facoltativa, ma anche che si debbano evitare sovrapposizioni, ripetizioni o eccessivi aggravi nell'inserire nei contratti ICT norme estrapolate da fonti diverse, dando quindi sostanza alla previsione dei Considerando 8, 10, 12 e 14 del Regolamento che ne fanno la principale fonte regolatrice della materia.

A rafforzare questa evidenza interpretativa, è intervenuta la stessa EBA che, con la comunicazione EBA/GL/2025/02 del 11/02/2025[25], ha ritenuto di dover esplicitare i propri dubbi relativamente alla ne-

24 Sez. II, Art. 6 par. 2 Regolamento DORA
25 *Guidelines amending Guidelines EBA/GL/2019/04 on ICT and security risk management.*

vedi l'articolo online

cessità di mantenere gli Orientamenti in essere[26] o di eliminarli del tutto, giungendo poi alla salomonica decisione di mantenerli solo in parte e per quei soggetti non rientranti nel perimetro della normativa DORA.

Ecco quindi che viene eliminata gran parte delle norme introdotte dagli Orientamenti del 2019: cambia l'oggetto, con l'integrale sostituzione degli articoli 5 e 6 degli Orientamenti, viene eliminato l'ambito di applicazione rappresentato dagli articoli 7 e 8[27]; si modificano radicalmente i destinatari; vengono eliminate tutte le definizioni di cui all'articolo 10 nonchè tutti i paragrafi (da 1 a 91) delle successive sezioni, compreso il paragrafo 7 che richiamava espressamente gli Orientamenti in tema di esternalizzazioni (EBA/GL/2019/02).

5. Conclusioni

A questo punto è lecito pensare che la normativa europea in materia di esternalizzazioni si sia divisa in due parti ben distinte: da un lato le esternalizzazioni che non riguardano processi e funzioni ICT, per le quali continua ad applicarsi la normativa precedente, e i contratti di fornitura di servizi ICT per i quali l'unica normativa applicabile è costituita dal Regolamento DORA.

In questo modo si raggiungerebbe quello scopo di uniformità e chiarezza nella gestione dei contratti e dei rapporti con i fornitori che è una, se non la principale, finalità del Regolamento.

26 Paragrafi 6 e 7 delle *Guidelines*.

27 *"7. I presenti orientamenti si applicano alla gestione dei rischi ICT e di sicurezza all'interno degli istituti finanziari (quali definiti al paragrafo 9). Ai fini dei presenti orientamenti, il termine «*rischi *ICT e di sicurezza» si riferisce ai rischi operativi e di sicurezza di cui all'articolo 95 della PSD2 per la prestazione di servizi di pagamento. 8. Per i prestatori di servizi di pagamento (quali definiti al paragrafo 9) i presenti orientamenti si applicano alla prestazione di servizi di pagamento, in linea con l'ambito di applicazione e il mandato di cui all'articolo 95 della PSD2. Per gli enti (quali definiti al paragrafo 9) i presenti orientamenti si applicano a tutte le attività da essi svolte"*.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it