COMMISSIONE
EUROPEA

Bruxelles, 24.9.2020
SWD(2020) 204 final

NOTE

This language version reflects the corrections done to the original EN version retransmitted under SWD(2020) 204 final/2 of 16.10.2020

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA RELAZIONE SULLA VALUTAZIONE D'IMPATTO

che accompagna il documento

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che modifica le direttive 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 e UE 2016/2341

{COM(2020) 596 final} - {SEC(2020) 309 final} - {SWD(2020) 203 final}

Scheda di sintesi

Valutazione d'impatto sulla proposta di regolamento relativo alla resilienza operativa digitale nel settore finanziario

A. Necessità di intervento

Per quale motivo? Qual è il problema da affrontare?

Il settore finanziario dipende in larga misura dalle tecnologie dell'informazione e della comunicazione (TIC). È probabile che l'attuale pandemia di COVID-19 acceleri tale processo, dati i benefici derivanti dalla possibilità di accedere costantemente da remoto ai servizi finanziari. La dipendenza dalle tecnologie digitali desta tuttavia preoccupazione; le imprese devono essere in grado di resistere a potenziali perturbazioni delle TIC in modo da affrontare gli incidenti e le minacce digitali e continuare a erogare i servizi. In un settore finanziario altamente interconnesso che fornisce servizi transfrontalieri vitali da cui dipende l'economia reale, le vulnerabilità derivanti dalla dipendenza dalle TIC, che pure riguardano tutti i settori economici, sono particolarmente pronunciate a causa: 1) dell'uso ampio e radicato delle TIC e 2) della possibilità che gli effetti di un incidente operativo su un'impresa o su un sottosettore finanziario si propaghino rapidamente ad altre imprese o parti del settore finanziario e, infine, al resto dell'economia.

Sebbene il settore finanziario sia molto avanzato nell'integrazione normativa e di mercato e debba la sua prosperità a un unico insieme di norme armonizzate, il codice unico dell'UE, la risposta dell'UE alle crescenti esigenze di resilienza operativa a livello orizzontale e settoriale:

- si è basata su un'armonizzazione minima, lasciando così spazio alle interpretazioni nazionali e alla frammentazione nel mercato unico, oppure
- è stata troppo generica e ha avuto un'applicazione limitata, per cui ha affrontato il rischio operativo generale in misura variabile, regolamentando parzialmente alcune componenti della *resilienza* operativa digitale (per esempio la gestione del rischio TIC, la segnalazione degli incidenti e il rischio TIC di terzi) ma trascurandone altre (test).

Finora l'intervento dell'UE non ha affrontato il rischio operativo in misura corrispondente alle esigenze delle imprese finanziarie, che devono resistere e reagire alle vulnerabilità delle TIC e riprendersi dai loro effetti, e non fornisce alle autorità di vigilanza finanziaria gli strumenti per adempiere al loro mandato di contenere l'instabilità finanziaria derivante da tali vulnerabilità.

Le attuali lacune e incoerenze hanno provocato la proliferazione di iniziative nazionali (ad esempio in materia di test) e di approcci di vigilanza (ad esempio per quanto riguarda le dipendenze da terzi nel settore TIC) non coordinati, dando luogo a sovrapposizioni, duplicazione di requisiti ed elevati costi amministrativi e di conformità per le imprese finanziarie transfrontaliere o impedendo di individuare e affrontare i rischi connessi alle TIC. Nel complesso, la stabilità e l'integrità del settore finanziario non sono garantite e il mercato unico dei servizi finanziari rimane frammentato; di conseguenza la tutela dei consumatori e degli investitori ne risulta compromessa.

Qual è l'obiettivo dell'iniziativa?

L'obiettivo generale consiste nel rafforzare la resilienza operativa digitale del settore finanziario dell'UE, razionalizzando e aggiornando la vigente legislazione finanziaria dell'Unione e introducendo nuovi requisiti laddove si riscontrino lacune, allo scopo di:

- migliorare la gestione dei rischi TIC da parte delle imprese finanziarie;
- incrementare le conoscenze delle autorità di vigilanza in fatto di minacce e incidenti;
- migliorare i test che le imprese finanziarie effettuano sui propri sistemi TIC; e
- migliorare la vigilanza sui rischi derivanti dalla dipendenza delle imprese finanziarie da fornitori terzi di TIC.

Più specificamente, la proposta introdurrebbe meccanismi di segnalazione degli incidenti più coerenti e uniformi, riducendo in tal modo gli oneri amministrativi per gli istituti finanziari e rafforzando l'efficienza della vigilanza.

Qual è il valore aggiunto dell'intervento a livello dell'UE?

Il mercato unico dei servizi finanziari dell'UE è disciplinato da un ampio insieme di norme stabilite a livello UE, che consentono alle imprese finanziarie autorizzate in uno Stato membro di prestare servizi in tutto il mercato unico grazie a un passaporto dell'UE. Di conseguenza, le norme stabilite a livello nazionale non costituirebbero un metodo efficace per rafforzare la resilienza operativa delle imprese finanziarie che utilizzano il passaporto. Inoltre il codice unico dell'UE contiene, a seguito della crisi finanziaria, norme estremamente dettagliate e prescrittive che affrontano rischi più "tradizionali" quali i rischi di credito, di mercato, di controparte e di liquidità. Le disposizioni vigenti in materia di rischio operativo sono di carattere puramente generale. Il rafforzamento della resilienza operativa digitale richiede adeguamenti delle disposizioni sui rischi operativi già definite a livello UE, pertanto miglioramenti e integrazioni sono possibili solo a livello dell'Unione.

B. Soluzioni

Quali opzioni strategiche legislative e di altro tipo sono state prese in considerazione? Ne è stata prescelta una? Per quale motivo?

Riguardo alla legislazione dell'UE in materia di servizi finanziari, la valutazione d'impatto ha preso in considerazione tre opzioni, oltre a uno scenario di base, ossia la rinuncia a prendere provvedimenti. Più specificatamente:

- **"Nessun provvedimento"**: le norme sulla resilienza operativa continuerebbero a fondarsi sull'attuale insieme delle disposizioni dell'UE in materia di servizi finanziari (che registra varie divergenze), in parte sulla direttiva sulla sicurezza delle reti e dell'informazione (NIS) e sui regimi nazionali vigenti o futuri;
- **Opzione 1 – rafforzamento delle riserve di capitale**: si introdurrebbe una riserva di capitale aggiuntiva per rafforzare la capacità delle imprese finanziarie di assorbire le perdite che potrebbero verificarsi a causa della mancanza di resilienza operativa;
- **Opzione 2 – un atto sulla resilienza operativa digitale dei servizi finanziari**: si introdurrebbe in tal modo un quadro globale a livello dell'UE tale da stabilire norme sulla resilienza operativa digitale per tutti gli istituti finanziari regolamentati che
    - affronterebbe in modo più completo i rischi legati alle TIC;
    - consentirebbe alle autorità di vigilanza finanziaria di accedere alle informazioni relative agli incidenti legati alle TIC;
    - garantirebbe alle imprese finanziarie di valutare l'efficacia delle proprie misure di prevenzione e resilienza e di individuare le vulnerabilità delle TIC;
    - rafforzerebbe le norme in materia di esternalizzazione che disciplinano la sorveglianza indiretta dei fornitori terzi di TIC;
    - consentirebbe una sorveglianza diretta delle attività dei fornitori terzi di TIC quando prestano i loro servizi a imprese finanziarie e
    - inoltre incoraggerebbe lo scambio di informazioni sulle minacce nel settore finanziario.
- **Opzione 3 – atto sulla resilienza unita alla vigilanza centralizzata dei fornitori terzi critici**: oltre a introdurre un atto sulla resilienza operativa (opzione 2) si istituirebbe una nuova autorità incaricata di vigilare sui fornitori terzi di servizi TIC critici alle imprese finanziarie. Ciò distinguerebbe anche più chiaramente il settore finanziario dal campo di applicazione della direttiva NIS.

È stata preferita l'opzione 2. Rispetto alle altre opzioni, questa realizza la maggioranza degli obiettivi dell'iniziativa, tenendo conto dei criteri di efficienza e coerenza. Quest'opzione, inoltre, riscuote il sostegno più vasto tra i portatori di interessi.

Chi sono i sostenitori delle varie opzioni?

La maggior parte dei portatori di interessi (privati, pubblici) concorda sulla necessità di un'azione dell'UE tesa a salvaguardare più efficacemente la resilienza operativa delle imprese finanziarie. Inoltre molti ritengono necessaria l'azione dell'UE per affrontare gli oneri normativi derivanti dal fatto che le imprese finanziarie sono soggette a norme duplicate e incoerenti stabilite dalla NIS, dalla normativa UE sui servizi finanziari e dai regimi nazionali (ad esempio per quanto riguarda la segnalazione degli incidenti). Di conseguenza, pochi portatori di interessi sono favorevoli ad astenersi dall'azione. Pochi portatori di interessi ritengono opportuno salvaguardare la resilienza operativa tramite l'aumento delle riserve di capitale (opzione 1). Questo è tuttavia l'approccio tradizionale al rischio operativo, in particolare nel settore bancario, e pertanto è preso in considerazione, ad esempio, dagli organismi internazionali di normazione. Il tipo di misure qualitative previste dall'opzione 2, che razionalizzerebbero e migliorerebbero la legislazione finanziaria dell'UE e introdurrebbero nuovi requisiti laddove esistano lacune mantenendo nel contempo i collegamenti con la direttiva orizzontale NIS, ottiene un vasto sostegno tra i portatori di interessi che hanno risposto alla consultazione pubblica. Mentre alcuni portatori di interessi (in particolare quelli pubblici) ritengono opportuno rafforzare la vigilanza sui fornitori terzi di TIC, come prevede l'opzione 3, l'istituzione a tale scopo di una nuova autorità dell'UE incontra solo un limitato favore tra i portatori di interessi, così come la discontinuità più netta rispetto al quadro NIS.

C. Impatto dell'opzione prescelta

Quali sono i vantaggi dell'opzione prescelta (o in mancanza di quest'ultima, delle opzioni principali)?

L'opzione 2 affronterebbe i **rischi connessi alle TIC** in tutto il settore finanziario, rafforzando la capacità degli istituti finanziari di resistere agli incidenti legati alle TIC. Diminuirebbe così il rischio che un incidente informatico si propaghi rapidamente tra i mercati finanziari. Mentre è difficile stimare i costi degli incidenti operativi nel settore finanziario (non tutti gli incidenti sono segnalati e l'entità dei costi è incerta), le valutazioni del settore indicano che i costi per il settore finanziario dell'UE potrebbero oscillare tra i 2 e i 27 miliardi di EUR all'anno.

L'opzione prescelta ridurrebbe questi costi diretti e gli eventuali impatti più ampi che gli incidenti informatici gravi potrebbero esercitare sulla stabilità finanziaria. Eliminando le sovrapposizioni tra **obblighi di segnalazione** si ridurrebbero gli oneri amministrativi. Ad esempio, per alcune delle maggiori banche il risparmio prodotto da quest'iniziativa potrebbe oscillare tra i 40 e i 100 milioni di EUR all'anno. La segnalazione diretta amplierebbe anche le conoscenze delle autorità di vigilanza in merito agli incidenti legati alle TIC. **L'armonizzazione delle pratiche in materia di test** renderebbe più facile individuare vulnerabilità e rischi sconosciuti. Diminuirebbe anche i costi, in particolare per le imprese transfrontaliere. Ad esempio, per le 44 maggiori banche transfrontaliere i benefici complessivi attesi da un approccio comune ai test potrebbero oscillare tra 11 e 88 milioni di EUR. L'introduzione di un insieme coerente di norme sulla gestione dei rischi legati ai **fornitori terzi di servizi TIC** conferirebbe alle imprese finanziarie un maggior controllo sul modo in cui i fornitori terzi si conformano al quadro normativo, aspetto apprezzabile per le autorità di vigilanza. Vi sarebbero inoltre vantaggi prudenziali derivanti dalla vigilanza delle autorità preposte sui fornitori terzi di TIC. Nel complesso l'opzione prescelta si traduce in benefici sociali più ampi, derivanti da un contesto operativo più resiliente per tutti i partecipanti ai mercati finanziari e da una maggiore tutela dei consumatori e degli investitori.

Quali sono i costi dell'opzione prescelta (o in mancanza di quest'ultima, delle opzioni principali)?

L'opzione prescelta comporterebbe costi sia una tantum che ricorrenti. I primi dipendono dagli investimenti in sistemi informatici e sono difficili da quantificare, data la diversa situazione dei preesistenti sistemi delle imprese. In assenza di un intervento normativo, alcune imprese finanziarie hanno già effettuato cospicui investimenti nei sistemi TIC. Di conseguenza, per le grandi imprese finanziarie il costo delle misure contenute in questa proposta sarà probabilmente modesto. Anche per le imprese più piccole i costi dovrebbero essere inferiori, in quanto esse sarebbero soggette a misure meno rigorose proporzionate al minor rischio. Per quanto riguarda i test, le autorità europee di vigilanza hanno stimato che i costi relativi ai test di penetrazione effettuati sulla base delle minacce variano tra lo 0,1 % e lo 0,3 % del bilancio totale destinato dalle imprese interessate alle TIC. I costi relativi alla segnalazione degli incidenti sarebbero drasticamente ridotti, in quanto non vi sarebbero sovrapposizioni con la segnalazione NIS. Anche le autorità di vigilanza dovrebbero sostenere alcuni costi a causa dei compiti supplementari che dovrebbero assumersi. Ad esempio, per le autorità di vigilanza che partecipano direttamente alla vigilanza sui fornitori terzi di TIC, l'incremento stimato degli ETP potrebbe collocarsi tra 1 e 5 ETP per l'autorità capofila e intorno a 0,25 ETP per le autorità partecipanti.

Quale sarà l'incidenza su aziende, PMI e microimprese?

L'opzione prescelta riguarderebbe tutte le imprese finanziarie, al fine di aumentare la resilienza operativa dell'intero settore. Tale vasto ambito di applicazione è importante alla luce della natura interconnessa del settore finanziario e della corrispondente necessità di dotarsi di un solido livello di resilienza operativa complessiva. Nel definire i requisiti fondamentali nei principali settori di intervento il principio di proporzionalità si applicherebbe tuttavia sia a tutti i sottosettori che all'interno di ciascun sottosettore, tenendo conto, tra l'altro, delle differenze tra i modelli d'impresa, delle dimensioni, del profilo di rischio, dell'importanza sistemica, ecc. Le misure in materia di segnalazione degli incidenti e i test, per esempio, sarebbero meno rigorosi per le imprese finanziarie più piccole.

L'impatto sulle amministrazioni e sui bilanci nazionali sarà significativo?

No. Come si è illustrato in precedenza, la sorveglianza supplementare può comportare un limitato incremento delle risorse di vigilanza, che tuttavia può andare a carico in tutto o in parte (nel caso di commissioni di vigilanza) dei bilanci pubblici.

Sono previsti altri impatti significativi?

Le conseguenze socioeconomiche della pandemia di COVID-19 sottolineano l'importanza cruciale dei mercati finanziari digitali e della loro resilienza operativa. L'opzione prescelta costituirebbe una solida base per sfruttare la trasformazione digitale garantendo la resilienza operativa del mercato unico dei servizi finanziari, anche nell'Unione bancaria e nell'Unione dei mercati dei capitali, sulla base di un insieme comune di norme e requisiti che perseguano sicurezza, prestazioni, stabilità e parità di condizioni. Ne sarà rafforzata anche la posizione dell'Europa come leader mondiale nel campo finanziario e digitale, obiettivo indicato dalla Commissione nella comunicazione "Plasmare il futuro digitale dell'Europa".

D. Tappe successive

Quando saranno riesaminate le misure proposte?

Il primo riesame avrà luogo tre anni dopo l'entrata in vigore dello strumento giuridico. La Commissione presenterà al Parlamento europeo e al Consiglio una relazione sul riesame compiuto. Se del caso, il riesame potrebbe essere supportato da una consultazione pubblica, nonché da studi, discussioni tra esperti, indagini e seminari.