DIRETTIVA (UE) 2022/2556 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 14 dicembre 2022

che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 53, paragrafo 1, e l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere della Banca centrale europea ([1]),

visto il parere del Comitato economico e sociale europeo ([2]),

deliberando secondo la procedura legislativa ordinaria ([3]),

considerando quanto segue:

(1) L'Unione deve affrontare in modo adeguato e completo i rischi digitali cui sono esposte tutte le entità finanziarie a causa di un maggiore uso delle tecnologie dell'informazione e della comunicazione (TIC) nella fornitura e nel consumo di servizi finanziari, contribuendo così alla realizzazione del potenziale della finanza digitale in termini di stimolazione dell'innovazione e promozione della concorrenza in un ambiente digitale sicuro.

(2) Le entità finanziarie dipendono fortemente dall'uso delle tecnologie digitali nella loro attività quotidiana. È pertanto essenziale garantire la resilienza operativa delle loro operazioni digitali a fronte dei rischi informatici. Tale necessità è diventata ancora più pressante a causa della crescita delle tecnologie innovative nel mercato, in particolare le tecnologie che consentono di trasferire e archiviare elettronicamente le rappresentazioni digitali di valore o di diritti utilizzando il registro distribuito o tecnologie analoghe (cripto-attività), nonché della crescita dei servizi connessi a tali attività.

([1]) GU C 343 del 26.8.2021, pag. 1.
([2]) GU C 155 del 30.4.2021, pag. 38.
([3]) Posizione del Parlamento europeo del 10 novembre 2022 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 28 novembre 2022.

(3) A livello di Unione, i requisiti connessi alla gestione dei rischi informatici nel settore finanziario sono attualmente previsti dalle direttive 2009/65/CE ([4]), 2009/138/CE ([5]), 2011/61/UE ([6]), 2013/36/UE ([7]), 2014/59/UE ([8]), 2014/65/UE ([9]), (UE) 2015/2366 ([10]) e (UE) 2016/2341 ([11]) del Parlamento europeo e del Consiglio.

Tali requisiti sono diversi e talvolta incompleti. In alcuni casi, i rischi informatici sono stati affrontati solo implicitamente come parte del rischio operativo e in altri casi non sono stati affrontati affatto. A tale situazione si è posto rimedio con l'adozione del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio ([12]). È pertanto opportuno che tali direttive siano modificate per garantire la coerenza con detto regolamento. La presente direttiva attua una serie di modifiche che sono necessarie per apportare chiarezza giuridica e coerenza in relazione all'applicazione, da parte delle entità finanziarie autorizzate e sottoposte a vigilanza conformemente a tali direttive, dei vari requisiti di resilienza operativa digitale necessari per lo svolgimento delle loro attività e per la prestazione di servizi, garantendo in tal modo il corretto funzionamento del mercato interno. È necessario assicurare l'adeguatezza di tali requisiti agli sviluppi del mercato incoraggiando nel contempo la proporzionalità, in particolare per quanto riguarda le dimensioni delle entità finanziarie e dei regimi specifici ai quali sono soggetti, al fine di ridurre i costi di adeguamento alla normativa.

(4) Nel settore dei servizi bancari, la direttiva 2013/36/UE stabilisce attualmente solo norme generali di governance interna e disposizioni sul rischio operativo contenenti requisiti per i piani di emergenza e di continuità operativa che fungono implicitamente da base per affrontare i rischi informatici. Per affrontare i rischi informatici esplicitamente e chiaramente, è però opportuno modificare i requisiti per i piani di emergenza e di continuità operativa al fine di includere anche piani di continuità operativa e di risposta e ripristino riguardanti i rischi informatici, conformemente agli obblighi stabiliti dal regolamento (UE) 2022/2554 Inoltre, i rischi informatici sono inclusi solo implicitamente, nell'ambito del rischio operativo, nel processo di revisione e valutazione prudenziale (*Supervisory Review and Evaluation process* - SREP) svolto dalle autorità competenti, e i criteri per la sua valutazione sono attualmente definiti negli Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (*Information and Communication Technology* - ICT) a norma del processo di revisione e valutazione prudenziale (SREP), emessi dall'Autorità europea di vigilanza (Autorità bancaria europea) (ABE), istituita dal regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio ([13]). Al fine di fornire chiarezza giuridica e assicurare che le autorità di vigilanza bancaria individuino i rischi informatici e ne monitorino efficacemente la

([4]) Direttiva 2009/65/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, concernente il coordinamento delle disposizioni legislative, regolamentari e amministrative in materia di taluni organismi d'investimento collettivo in valori mobiliari (OICVM) (GU L 302 del 17.11.2009, pag. 32).

([5]) Direttiva 2009/138/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, in materia di accesso ed esercizio delle attività di assicurazione e di riassicurazione (solvibilità II) (GU L 335 del 17.12.2009, pag. 1).

([6]) Direttiva 2011/61/UE del Parlamento europeo e del Consiglio, dell'8 giugno 2011, sui gestori di fondi di investimento alternativi, che modifica le direttive 2003/41/CE e 2009/65/CE e i regolamenti (CE) n. 1060/2009 e (UE) n. 1095/2010 (GU L 174 dell'1.7.2011, pag. 1).

([7]) Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (GU L 176 del 27.6.2013, pag. 338).

([8]) Direttiva 2014/59/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, che istituisce un quadro di risanamento e risoluzione degli enti creditizi e delle imprese di investimento e che modifica la direttiva 82/891/CEE del Consiglio, e le direttive 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE e 2013/36/UE e i regolamenti (UE) n. 1093/2010 e (UE) n. 648/2012, del Parlamento europeo e del Consiglio (GU L 173 del 12.6.2014, pag. 190).

([9]) Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (GU L 173 del 12.6.2014, pag. 349).

([10]) Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE (GU L 337 del 23.12.2015, pag. 35).

([11]) Direttiva (UE) 2016/2341 del Parlamento europeo e del Consiglio, del 14 dicembre 2016, relativa alle attività e alla vigilanza degli enti pensionistici aziendali o professionali (EPAP) (GU L 354 del 23.12.2016, pag. 37).

([12]) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (cfr. pagina 1 della presente Gazzetta ufficiale).

([13]) Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità bancaria europea), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/78/CE della Commissione (GU L 331 del 15.12.2010, pag. 12).

gestione da parte delle entità finanziarie, in linea con il nuovo quadro sulla resilienza operativa digitale, l'ambito di applicazione dello SREP dovrebbe essere modificato anche per fare riferimento esplicitamente agli obblighi stabiliti dal regolamento (UE) 2022/2554 e coprire in particolare i rischi evidenziati dalle segnalazioni di incidenti gravi connessi alle TIC e dai risultati delle verifiche della resilienza operativa digitale effettuate dalle entità finanziarie conformemente a tale regolamento.

(5) La resilienza operativa digitale è fondamentale per preservare le funzioni essenziali e le linee di business principali di un'entità finanziaria in caso di risoluzione ed evitare in tal modo di perturbare l'economia reale e il sistema finanziario. Gli incidenti operativi gravi possono ostacolare la capacità di un'entità finanziaria di continuare a operare e possono compromettere gli obiettivi della risoluzione. Taluni accordi contrattuali per l'utilizzo di servizi TIC sono essenziali per garantire la continuità operativa e fornire i dati necessari in caso di risoluzione. Al fine di rispettare gli obiettivi del quadro dell'Unione per la resilienza operativa, la direttiva 2014/59/UE dovrebbe essere modificata di conseguenza per garantire che le informazioni relative alla resilienza operativa siano prese in considerazione nel contesto della pianificazione della risoluzione e della valutazione della possibilità di risoluzione delle entità finanziarie.

(6) La direttiva 2014/65/UE stabilisce norme più rigorose in materia di rischi informatici per le imprese di investimento e le sedi di negoziazione che effettuano negoziazioni algoritmiche. Requisiti meno dettagliati si applicano ai servizi di comunicazione dei dati e ai repertori di dati sulle negoziazioni. Inoltre, la direttiva 2014/65/UE contiene solo riferimenti limitati ai dispositivi di controllo e di salvaguardia per sistemi di elaborazione delle informazioni e all'uso di sistemi, risorse e procedure adeguati per garantire la continuità e la regolarità dei servizi alle imprese. Inoltre, tale direttiva dovrebbe essere allineata al regolamento (UE) 2022/2554 per quanto riguarda la continuità e la regolarità nell'erogazione di servizi e nello svolgimento delle attività di investimento, la resilienza operativa, la capacità dei sistemi di negoziazione e l'efficacia dei dispositivi di continuità operativa e della gestione del rischio.

(7) La direttiva (UE) 2015/2366 stabilisce norme specifiche per quanto riguarda le misure di controllo e di mitigazione in materia di sicurezza delle TIC ai fini di ottenere un'autorizzazione a erogare servizi di pagamento. È opportuno modificare tali norme in materia di autorizzazione per allinearle al regolamento (UE) 2022/2554 Inoltre, al fine di ridurre gli oneri amministrativi ed evitare la complessità e la duplicazione degli obblighi di segnalazione, le norme in materia di segnalazione degli incidenti di cui a tale direttiva dovrebbero cessare di applicarsi ai prestatori di servizi di pagamento disciplinati da tale direttiva e soggetti al regolamento (UE) 2022/2554 in modo da permettere a tali prestatori di servizi di pagamento di beneficiare di un meccanismo unico, pienamente armonizzato di notifica degli incidenti per tutti gli incidenti operativi o relativi alla sicurezza dei pagamenti, indipendentemente dal fatto che si tratti di incidenti connessi alle TIC.

(8) Le direttive 2009/138/CE e (UE) 2016/2341 tengono parzialmente conto dei rischi informatici nelle rispettive disposizioni generali in materia di governance e gestione del rischio, lasciando che determinati requisiti siano specificati mediante atti delegati con o senza riferimenti specifici ai rischi informatici. Analogamente, ai gestori di fondi di investimento alternativi soggetti alla direttiva 2011/61/UE e alle società di gestione soggette alla direttiva 2009/65/CE si applicano soltanto norme molto generali. È pertanto opportuno allineare tali direttive agli obblighi stabiliti nel regolamento (UE) 2022/2554 per quanto riguarda la gestione dei sistemi e degli strumenti TIC.

(9) In molti casi, ulteriori requisiti in materia di rischi informatici sono già stati stabiliti in atti delegati e di esecuzione, adottati sulla base di progetti di norme tecniche di regolamentazione e di attuazione elaborati dalla competente autorità europea di vigilanza. Dato che le disposizioni del regolamento (UE) 2022/2554 costituiscono la base giuridica in materia di rischi informatici nel settore finanziario, è opportuno modificare determinate competenze ad adottare atti delegati e di esecuzione di cui alle direttive 2009/65/CE, 2009/138/CE, 2011/61/UE e 2014/65/EU al fine di eliminare le disposizioni in materia di rischi informatici dall'ambito di applicazione di tali competenze.

(10) Al fine di garantire un'attuazione coerente del nuovo quadro sulla resilienza operativa digitale per il settore finanziario, gli Stati membri dovrebbero applicare le disposizioni di diritto nazionale che recepiscono la presente direttiva a decorrere dalla data di applicazione del regolamento (UE) 2022/2554

(11) Le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 sono state adottate sulla base dell'articolo 53, paragrafo 1, o dell'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE) o di entrambi. Le modifiche contenute nella presente direttiva sono state incluse in un unico atto legislativo a causa dell'interconnessione dell'oggetto e degli obiettivi delle modifiche. Di conseguenza, la presente direttiva dovrebbe essere adottata sulla base dell'articolo 53, paragrafo 1, e dell'articolo 114 TFUE.

(12) Poiché gli obiettivi della presente direttiva non possono essere conseguiti in misura sufficiente dagli Stati membri in quanto comportano l'armonizzazione degli obblighi già contenuti nelle direttive ma, a motivo della portata e degli effetti dell'azione, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(13) Conformemente alla dichiarazione politica comune del 28 settembre 2011 degli Stati membri e della Commissione sui documenti esplicativi ([14]), gli Stati membri si sono impegnati ad accompagnare, in casi giustificati, la notifica delle loro misure di recepimento con uno o più documenti che chiariscano il rapporto tra gli elementi costitutivi di una direttiva e le parti corrispondenti degli strumenti nazionali di recepimento. Per quanto riguarda la presente direttiva, il legislatore ritiene che la trasmissione di tali documenti sia giustificata,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

Articolo 1

Modifiche della direttiva 2009/65/CE

Il testo dell'articolo 12 della direttiva 2009/65/CE è così modificato:

1) al paragrafo 1, secondo comma, la lettera a) è sostituita dalla seguente:

«a) abbia una buona organizzazione amministrativa e contabile, meccanismi di controllo e di salvaguardia in materia di elaborazione elettronica dei dati, anche per quanto riguarda sistemi informatici e di rete istituiti e gestiti ai sensi del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*), nonché procedure adeguate di controllo interno che comprendano, in particolare, regole per le operazioni personali dei dipendenti o per la detenzione o la gestione di investimenti in strumenti finanziari a scopo di investimento in conto proprio e che assicurino, quanto meno, che qualunque transazione in cui intervenga l'OICVM possa essere ricostruita per quanto riguarda l'origine, le controparti, la natura nonché il luogo e il momento in cui è stata effettuata e che il patrimonio degli OICVM gestito dalla società di gestione sia investito conformemente al regolamento del fondo o al suo atto costitutivo e alle norme in vigore;

(*) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).»;

2) il paragrafo 3 è sostituito dal seguente:

«3. Fatto salvo l'articolo 116, la Commissione adotta, mediante atti delegati conformemente all'articolo 112 *bis*, misure che precisano:

a) le procedure e le disposizioni di cui al paragrafo 1, secondo comma, lettera a), diverse dalle procedure e dagli strumenti relativi ai sistemi informatici e di rete;

b) le strutture e i requisiti organizzativi volti a ridurre al minimo i conflitti di interesse di cui al paragrafo 1, secondo comma, lettera b).».

([14]) GU C 369 del 17.12.2011, pag. 14.

Articolo 2

Modifiche della direttiva 2009/138/CE

La direttiva 2009/138/CE è così modificata:

1) all'articolo 41, il paragrafo 4 è sostituito dal seguente:

«4. Le imprese di assicurazione e di riassicurazione adottano misure ragionevoli atte a garantire la continuità e la regolarità dello svolgimento delle loro attività, tra cui l'elaborazione di piani di emergenza. A tal fine, le imprese in questione utilizzano sistemi, risorse e procedure adeguati e proporzionati e, in particolare, istituiscono e gestiscono sistemi informatici e di rete conformemente al regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*).

(*) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).»;

2) all'articolo 50, paragrafo 1, le lettere a) e b) sono sostituite dalle seguenti:

«a) gli elementi dei sistemi di cui all'articolo 41, all'articolo 44, in particolare i settori elencati all'articolo 44, paragrafo 2, e agli articoli 46 e 47, diversi dagli elementi relativi alla gestione dei rischi informatici;

b) le funzioni di cui agli articoli 44, 46, 47 e 48, diverse dalle funzioni relative alla gestione dei rischi informatici.».

Articolo 3

Modifica della direttiva 2011/61/UE

L'articolo 18 della direttiva 2011/61/UE è sostituito dal seguente:

«*Articolo 18*

Principi generali

1. Gli Stati membri impongono ai GEFIA di ricorrere in ogni momento a risorse umane e tecniche adeguate e adatte per la buona gestione dei FIA.

In particolare, le autorità competenti dello Stato membro d'origine del GEFIA, considerata anche la natura del FIA gestito dal GEFIA, impongono a quest'ultimo di possedere una buona organizzazione amministrativa e contabile, modalità di controllo e di salvaguardia in materia di elaborazione elettronica dei dati, anche per quanto riguarda i sistemi informatici e di rete istituiti e gestiti ai sensi del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*), nonché procedure di controllo interno adeguate che comprendano, in particolare, regole per le operazioni personali dei dipendenti o per la detenzione o la gestione di investimenti a scopo di investimento in conto proprio e che assicurino, quanto meno, che qualunque operazione in cui intervenga il FIA possa essere ricostruita per quanto riguarda l'origine, le parti, la natura nonché il luogo e il momento in cui è stata effettuata e che le attività del FIA gestito dal GEFIA siano investite conformemente al regolamento o ai documenti costitutivi del FIA e alle disposizioni normative in vigore.

2. La Commissione adotta, mediante atti delegati in conformità dell'articolo 56 e alle condizioni di cui agli articoli 57 e 58, misure che specifichino le procedure e le modalità di cui al paragrafo 1 del presente articolo diverse dalle procedure e modalità relative ai sistemi informatici e di rete.

(*) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).».

Articolo 4

Modifiche della direttiva 2013/36/UE

La direttiva 2013/36/UE è così modificata:

1) all'articolo 65, paragrafo 3, lettera a), il punto vi) è sostituito dal seguente:

«vi) terze parti cui le entità di cui ai punti da i) a iv) hanno esternalizzato funzioni o attività, compresi i fornitori terzi di servizi TIC di cui al capo V del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*);

(*) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).;»

2) all'articolo 74, paragrafo 1, il primo comma è sostituito dal seguente:

«Gli enti sono dotati di solidi dispositivi di governance, ivi compresa una chiara struttura dell'organizzazione con linee di responsabilità ben definite, trasparenti e coerenti, di processi efficaci per l'identificazione, la gestione, la sorveglianza e la segnalazione dei rischi ai quali sono o potrebbero essere esposti, e di adeguati meccanismi di controllo interno, ivi compresi valide procedure amministrative e contabili, sistemi informatici e di rete istituiti e gestiti conformemente al regolamento (UE) 2022/2554 , nonché politiche e prassi di remunerazione che riflettano e promuovano una sana ed efficace gestione del rischio.»;

3) all'articolo 85, il paragrafo 2 è sostituito dal seguente:

«2. Le autorità competenti assicurano che gli enti dispongano di adeguati politiche e piani di emergenza e di continuità operativa, compresi le politiche e i piani di continuità operativa delle TIC e piani di risposta e ripristino relativi alle TIC per la tecnologia che utilizzano per comunicare le informazioni e che tali piani siano istituiti, gestiti e testati a norma dell'articolo 11 del regolamento (UE) 2022/2554, affinché gli enti possano continuare a operare in caso di grave interruzione dell'operatività e limitare le perdite subite a seguito di tale interruzione.»;

4) all'articolo 97, paragrafo 1, è aggiunta la lettera seguente:

«d) i rischi evidenziati dalla verifica della resilienza operativa digitale conformemente al capo IV del regolamento (UE) 2022/2554;».

Articolo 5

Modifiche della direttiva 2014/59/UE

La direttiva 2014/59/UE è così modificata:

1) l'articolo 10 è così modificato:

a) al paragrafo 7, la lettera c) è sostituita dalla seguente:

«c) la dimostrazione di come le funzioni essenziali e le linee di business principali possano essere separate dalle altre funzioni, sul piano giuridico ed economico, nella misura necessaria, in modo da garantire la continuità e la resilienza operativa digitale in caso di dissesto dell'ente;»;

b) al paragrafo 7, la lettera q) è sostituita dalla seguente:

«q) una descrizione delle operazioni e dei sistemi essenziali per assicurare la continuità del funzionamento dei processi operativi dell'ente, compresi i sistemi informatici e di rete di cui al regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*);

(*) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).»;

c) al paragrafo 9 è aggiunto il comma seguente:

«A norma dell'articolo 10 del regolamento (UE) n. 1093/2010, l'ABE rivede e, se del caso, aggiorna le norme tecniche di regolamentazione per tenere conto, tra l'altro, delle disposizioni del capo II del regolamento (UE) 2022/2554.»;

2) l'allegato è così modificato:

a) nella sezione A, il punto 16) è sostituito dal seguente:

«16) dispositivi e misure necessari per assicurare la continuità del funzionamento dei processi operativi dell'ente, compresi i sistemi informatici e di rete istituiti e gestiti a norma del regolamento (UE) 2022/2554;»;

b) la sezione B è modificata come segue:

i) il punto 14) è sostituito dal seguente:

«14) l'identificazione dei proprietari dei sistemi individuati al punto 13), i relativi accordi sul livello di servizio ed eventuali software e sistemi o licenze, compresa l'attribuzione alle persone giuridiche, operazioni essenziali e linee di business principali dell'ente, nonché un'identificazione dei fornitori terzi critici di servizi TIC definiti all'articolo 3, punto 23), del regolamento (UE) 2022/2554;»;

ii) è inserito il punto seguente:

«14 bis) i risultati delle prove di resilienza operativa digitale a norma del regolamento (UE) 2022/2554;»

c) la sezione C è modificata come segue:

i) il punto 4) è sostituito dal seguente:

«4) la misura in cui i contratti di servizio, compresi gli accordi contrattuali per l'utilizzo di servizi TIC, mantenuti dall'ente sono solidi e pienamente opponibili in caso di risoluzione dell'ente;»;

ii) è inserito il punto seguente:

«4 bis) la resilienza operativa digitale dei sistemi informatici e di rete che sostengono le funzioni essenziali e le linee di business principali dell'ente, tenendo conto delle segnalazioni di incidenti gravi connessi alle TIC e dei risultati delle prove di resilienza operativa digitale a norma del regolamento (UE) 2022/2554».

Articolo 6

Modifiche della direttiva 2014/65/UE

La direttiva 2014/65/UE è così modificata:

1) l'articolo 16 è così modificato:

a) il paragrafo 4 è sostituito dal seguente:

«4. Le imprese di investimento adottano misure ragionevoli per garantire la continuità e la regolarità nella prestazione di servizi e nell'esercizio di attività di investimento. A tal fine le imprese di investimento utilizzano sistemi appropriati e proporzionati, compresi sistemi di tecnologie dell'informazione e della comunicazione (TIC) istituiti e gestiti conformemente all'articolo 7 del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*), nonché risorse e procedure appropriate e proporzionate.

(*) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).»;

b) al paragrafo 5, il secondo e il terzo comma sono sostituiti dal testo seguente:

«Le imprese di investimento dispongono di procedure amministrative e contabili sane, di meccanismi di controllo interno e di procedure efficaci per la valutazione del rischio.

Ferma restando la facoltà delle autorità competenti di ottenere accesso alle comunicazioni conformemente alla presente direttiva e al regolamento (UE) n. 600/2014, le imprese di investimento adottano efficaci meccanismi di sicurezza finalizzati a garantire, conformemente agli obblighi stabiliti da regolamento (UE) 2022/2554, la sicurezza e l'autenticazione dei mezzi per il trasferimento delle informazioni, a minimizzare i rischi di corruzione dei dati e di accesso non autorizzato e a prevenire la fuga di informazioni tutelando in ogni momento la riservatezza dei dati.»;

2) l'articolo 17 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

«1. Le imprese di investimento che effettuano negoziazione algoritmica pongono in essere controlli dei sistemi e del rischio efficaci e idonei per l'attività esercitata volti a garantire che i propri sistemi di negoziazione siano resilienti e dispongano di sufficiente capacità conformemente agli obblighi stabiliti al capo II del regolamento (UE) 2022/2554, siano soggetti a soglie e limiti di negoziazione appropriati e impediscano l'invio di ordini erronei o comunque un funzionamento dei sistemi tale da creare un mercato disordinato o contribuirvi.

Tali imprese pongono in essere anche controlli efficaci dei sistemi e del rischio per garantire che i sistemi di negoziazione non possano essere utilizzati per finalità contrarie al regolamento (UE) n. 596/2014 o alle regole di una sede di negoziazione a cui esse sono collegate.

Tali imprese di investimento dispongono di meccanismi efficaci di continuità operativa per rimediare a malfunzionamenti dei sistemi di negoziazione, compresi politica e piani di continuità operativa delle TIC e piani di risposta e ripristino relativi alle TIC istituiti a norma dell'articolo 11 del regolamento (UE) 2022/2554 e provvedono affinché i loro sistemi siano verificati a fondo e soggetti a un monitoraggio adeguato per garantirne la conformità agli obblighi generali stabiliti nel presente paragrafo e agli obblighi specifici stabiliti ai capi II e IV del regolamento (UE) 2022/2554.»;

b) al paragrafo 7, la lettera a) è sostituita dalla seguente:

«a) precisare i requisiti organizzativi di cui ai paragrafi da 1 a 6, diversi da quelli connessi alla gestione dei rischi informatici, da imporre alle imprese di investimento che prestano diversi servizi di investimento, attività di investimento, servizi accessori o combinazioni degli stessi; le informazioni che precisano i requisiti organizzativi di cui al paragrafo 5 indicano i requisiti specifici per l'accesso diretto al mercato e per l'accesso sponsorizzato in modo tale da garantire che i controlli applicati all'accesso sponsorizzato siano almeno equivalenti a quelli applicati all'accesso diretto al mercato;»;

3) all'articolo 47, il paragrafo 1 è così modificato:

a) la lettera b) è sostituita dalla seguente:

«b) siano adeguatamente attrezzati per gestire i rischi ai quali sono esposti, compresi i rischi informatici ai sensi del capo II del regolamento (UE) 2022/2554, si dotino di dispositivi e sistemi adeguati per identificare i rischi che possano comprometterne il funzionamento e prendano misure efficaci per attenuare tali rischi;»;

b) la lettera c) è soppressa;

4) l'articolo 48 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

«1. Gli Stati membri garantiscono che i mercati regolamentati istituiscano e mantengano la loro resilienza operativa, conformemente agli obblighi stabiliti al capo II del regolamento (UE) 2022/2554, per garantire che i loro sistemi di negoziazione siano resilienti, abbiano capacità sufficiente per gestire i picchi di volume di ordini e messaggi, siano in grado di garantire negoziazioni ordinate in condizioni di mercato critiche, siano pienamente testati per garantire il rispetto di tali condizioni, siano soggetti a efficaci disposizioni in materia di continuità operativa, compresi politica e piani di continuità operativa delle TIC e piani di risposta e di ripristino relativi alle TIC istituiti ai sensi dell'articolo 11 del regolamento (UE) 2022/2554, per garantire la continuità dei servizi in caso di malfunzionamento dei loro sistemi di negoziazione.»;

b) il paragrafo 6 è sostituito dal seguente:

«6. Gli Stati membri si assicurano che i mercati regolamentati dispongano di sistemi, procedure e dispositivi efficaci, anche chiedendo ai membri o ai partecipanti di realizzare prove adeguate degli algoritmi e fornendo ambienti per facilitare la realizzazione di tali prove conformemente agli obblighi stabiliti ai capi II e IV del regolamento (UE) 2022/2554, per garantire che i sistemi algoritmici di negoziazione non possano creare o contribuire a creare condizioni di negoziazione anormali sul mercato e per gestire qualsiasi condizione di negoziazione anormale causata da tali sistemi algoritmici di negoziazione, tra cui sistemi per limitare il rapporto tra ordini non eseguiti e operazioni inserite nel sistema da un membro o partecipante, al fine di poter rallentare il flusso di ordini in caso di rischio che sia raggiunta la capacità del sistema e per limitare la dimensione minima dello scostamento di prezzo che può essere eseguita sul mercato e garantirne il rispetto.»;

c) il paragrafo 12 è così modificato:

i) la lettera a) è sostituita dalla seguente

«a) gli obblighi volti a garantire che i sistemi di negoziazione dei mercati regolamentati siano resilienti e abbiano una capacità adeguata, a eccezione degli obblighi relativi alla resilienza operativa digitale;»;

ii) la lettera g) è sostituita dalla seguente:

«g) gli obblighi volti a garantire una verifica adeguata degli algoritmi, diversa dalla verifica della resilienza operativa digitale, in modo da assicurare che i sistemi di negoziazione algoritmica, inclusi i sistemi di negoziazione algoritmica ad alta frequenza, non possano creare o contribuire a creare condizioni di negoziazione anormali sul mercato.».

Articolo 7

Modifiche della direttiva (UE) 2015/2366

La direttiva (UE) 2015/2366 è così modificata:

1) all'articolo 3, la lettera j) è sostituita dalla seguente:

«j) ai servizi forniti da prestatori di servizi tecnici, che supportano la prestazione dei servizi di pagamento, senza mai entrare in possesso dei fondi da trasferire, compresi l'elaborazione e la registrazione di dati, i servizi fiduciari e di protezione della riservatezza, l'autenticazione dei dati e delle entità, la fornitura di reti di tecnologie dell'informazione e della comunicazione (*information and communication technology* – TIC) e di comunicazione, la fornitura e la manutenzione di terminali e dispositivi utilizzati per i servizi di pagamento a esclusione dei servizi di disposizione di ordine di pagamento e dei servizi di informazione sui conti;»;

2) all'articolo 5, il paragrafo 1 è così modificato:

a) il primo comma è così modificato:

i) la lettera e) è sostituita dalla seguente:

«e) una descrizione dei dispositivi di governo societario e dei meccanismi di controllo interno, ivi comprese le procedure amministrative, di gestione del rischio e contabili, del richiedente, nonché gli accordi per l'utilizzo di servizi di TIC a noma del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*), che dimostri che tali dispositivi di governo societario e meccanismi di controllo interno siano proporzionati, appropriati, validi e adeguati;

(*) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).";

ii) la lettera f) è sostituita dalla seguente:

«f) una descrizione della procedura esistente per monitorare e gestire gli incidenti relativi alla sicurezza e i reclami dei clienti in materia di sicurezza e per darvi seguito, compreso un meccanismo di notifica degli incidenti che tenga conto degli obblighi di notifica dell'istituto di pagamento di cui al capo III del regolamento (UE) 2022/2554»

iii) la lettera h) è sostituita dalla seguente:

«h) una descrizione delle disposizioni in materia di continuità operativa, tra cui l'individuazione chiara delle operazioni critiche, politica e piani di continuità operativa delle TIC e piani di risposta e di ripristino relativi alle TIC efficaci nonché una procedura per testare periodicamente e riesaminare l'adeguatezza e l'efficacia di tali piani a norma del regolamento (UE) 2022/2554;»;

b) il terzo comma è sostituito dal seguente:

«Le misure di controllo e di mitigazione in materia di sicurezza di cui al primo comma, lettera j), indicano in che modo garantiscono un elevato livello di resilienza operativa digitale conformemente al capo II del regolamento (UE) 2022/2554, in particolare, in relazione alla sicurezza tecnica e protezione dei dati, anche per il software e i sistemi TIC utilizzati dal richiedente o dalle imprese alle quali questi esternalizza la totalità o parte delle sue attività. Tali misure comprendono anche le misure di sicurezza di cui all'articolo 95, paragrafo 1, della presente direttiva. Tali misure tengono conto degli orientamenti dell'ABE relativi alle misure di sicurezza di cui all'articolo 95, paragrafo 3, della presente direttiva una volta emanati.»;

3) all'articolo 19, paragrafo 6, il secondo comma è sostituito dal seguente:

«L'esternalizzazione di funzioni operative importanti, tra cui i sistemi TIC, non deve mettere materialmente a repentaglio la qualità del controllo interno dell'istituto di pagamento né la capacità delle autorità competenti di controllare e documentare che l'istituto di pagamento adempia a tutti gli obblighi definiti dalla presente direttiva.»;

4) all'articolo 95, paragrafo 1, è aggiunto il comma seguente:

«Il primo comma lascia impregiudicata l'applicazione del capo II del regolamento (UE) 2022/2554:

a) ai prestatori di servizi di pagamento di cui all'articolo 1, paragrafo 1, lettere a), b) e d), della presente direttiva;

b) ai prestatori di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, della presente direttiva;

c) agli istituti di pagamento esentati a norma dell'articolo 32, paragrafo 1, della presente direttiva; e

d) agli istituti di moneta elettronica che beneficiano di un'esenzione ai sensi dell'articolo 9, paragrafo 1, della direttiva 2009/110/CE.»;

5) all'articolo 96 è aggiunto il paragrafo seguente:

«7. Gli Stati membri assicurano che i paragrafi da 1 a 5 del presente articolo non si applichino:

a) ai prestatori di servizi di pagamento di cui all'articolo 1, paragrafo 1, lettere a), b) e d), della presente direttiva;

b) ai prestatori di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, della presente direttiva;

c) agli istituti di pagamento esentati a norma dell'articolo 32, paragrafo 1, della presente direttiva; e

d) agli istituti di moneta elettronica che beneficiano di un'esenzione ai sensi dell'articolo 9, paragrafo 1, della direttiva 2009/110/CE.»;

6) all'articolo 98, il paragrafo 5 è sostituito dal seguente:

«5. A norma dell'articolo 10 del regolamento (UE) n. 1093/2010, l'ABE periodicamente rivede e, se del caso, aggiorna le norme tecniche di regolamentazione, tra l'altro, per tenere conto dell'innovazione e dei progressi tecnologici, nonché delle disposizioni del capo II del regolamento (UE) 2022/2554».

Articolo 8

Modifica della direttiva (UE) 2016/2341

All'articolo 21 della direttiva (UE) 2016/2341, il paragrafo 5 è sostituito dal seguente:

«5. Gli Stati membri assicurano che gli EPAP adottino misure ragionevoli atte a garantire la continuità e la regolarità dello svolgimento delle loro attività, tra cui l'elaborazione di piani di emergenza. A tal fine gli EPAP utilizzano sistemi,

risorse e procedure adeguati e proporzionati e, in particolare, istituiscono e gestiscono sistemi informatici e di rete conformemente al regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (*), ove applicabile.

(*) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).».

Articolo 9

Recepimento

1. Entro il 17 gennaio 2025, gli Stati membri adottano e pubblicano le misure necessarie per conformarsi alla presente direttiva. Essi ne informano immediatamente la Commissione.

Essi applicano tali misure a decorrere dal 17 gennaio 2025.

Le misure adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di un siffatto riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono stabilite dagli Stati membri.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni principali di diritto interno che adottano nel settore disciplinato dalla presente direttiva.

Articolo 10

Entrata in vigore

La presente direttiva entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 11

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Strasburgo, il 14 dicembre 2022

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*Il presidente*
R. METSOLA	M. BEK