Consiliul
Uniunii Europene

Bruxelles, 24 septembrie 2020
(OR. en)

11052/20
ADD 2

Dosar interinstituțional:
2020/0268 (COD)

EF 229
ECOFIN 847
TELECOM 160
CYBER 169
IA 62
CODEC 872

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală al Comisiei Europene, sub semnătura dlui Jordi AYET PUIGARNAU, Director
Data primirii:	24 septembrie 2020
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	SWD(2020) 204 final
Subiect:	DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI REZUMAT AL RAPORTULUI PRIVIND EVALUAREA IMPACTULUI care însoţeşte documentul Propunere de directivă a Parlamentului European și a Consiliului de modificare a Directivelor 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 și (UE) 2016/2341

În anexă, se pune la dispoziția delegațiilor documentul SWD(2020) 204 final.

Anexă: SWD(2020) 204 final

COMISIA
EUROPEANĂ

Bruxelles, 24.9.2020
SWD(2020) 204 final

This document corrects document SWD(2020) 204 final of 24.09.2020
Two references in the title of the cover page have been corrected.
Concerns the EN version only.
The text shall read as follows:

DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI

REZUMAT AL RAPORTULUI PRIVIND EVALUAREA IMPACTULUI

care însoţeşte documentul

Propunere de directivă a Parlamentului European și a Consiliului

de modificare a Directivelor 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 și (UE) 2016/2341

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

Fișă rezumat

Evaluarea impactului propunerii de regulament privind reziliența operațională digitală în sectorul financiar

A. Necesitatea de a acționa

De ce? Care este problema abordată?

Sectorul financiar se bazează în mare măsură pe tehnologiile informației și comunicațiilor (TIC). Actuala pandemie de COVID-19 va intensifica probabil această utilizare, având în vedere beneficiile asigurării unui acces continuu la distanță la serviciile financiare. Dependența de tehnologiile digitale presupune, totuși, și anumite motive de îngrijorare; întreprinderile trebuie să fie în măsură să suporte eventualele perturbări TIC, astfel încât să poată trata incidentele și amenințările digitale și să mențină serviciile. Într-un sector financiar foarte interconectat, care desfășoară servicii transfrontaliere vitale de care depinde economia reală, vulnerabilitățile care decurg din dependența de TIC, deși sunt aplicabile tuturor sectoarelor economice, sunt deosebit de pronunțate din cauza (1) utilizării profunde și extinse a TIC și (2) a potențialului ca efectele unui incident operațional în cadrul unei societăți financiare sau al unui subsector financiar să se răspândească rapid la alte întreprinderi sau părți ale sectorului financiar și, în cele din urmă, la restul economiei.

În pofida faptului că sectorul financiar este foarte avansat în ceea ce privește integrarea pieței și a cadrului de reglementare și prosperă pe baza unui set unic de norme armonizate — cadrul unic de reglementare al UE –, răspunsul UE la necesitățile sporite în materie de reziliență operațională, atât la nivel orizontal, cât și la nivel sectorial, a fost fie:

- bazat pe o armonizare minimă, lăsând astfel loc pentru interpretarea și fragmentarea la nivel național în cadrul pieței unice, fie
- prea general și cu aplicare limitată, abordând riscul operațional general într-o măsură variabilă, reglementând parțial unele componente ale rezilienței *operaționale digitale* (de exemplu, gestionarea riscurilor TIC, raportarea incidentelor și riscul asociat furnizorilor terți de servicii TIC) lăsând pe dinafară altele (testarea).

Intervenția UE nu a abordat până în prezent riscul operațional într-un mod care să corespundă nevoilor societăților financiare de a rezista, a răspunde vulnerabilităților în materie de TIC și a se redresa de pe urma acestora, și nici nu le oferă autorităților de supraveghere financiară instrumentele necesare pentru a-și îndeplini mandatul de a limita instabilitatea financiară generată de respectivele vulnerabilități în materie de TIC.

Lacunele și inconsecvențele actuale au condus la o proliferare a inițiativelor naționale (de exemplu, cu privire la testare) și a abordărilor în materie de supraveghere (de exemplu, în ceea ce privește dependențele de furnizori terți de servicii TIC) necoordonate, care se traduc fie prin suprapuneri, dublări ale cerințelor, costuri administrative și de asigurare a conformității ridicate pentru societățile financiare transfrontaliere, fie prin riscuri TIC rămase nedepistate și neremediate. Per ansamblu, stabilitatea și integritatea sectorului financiar nu sunt garantate, iar piața unică a serviciilor financiare rămâne fragmentată, astfel încât protecția consumatorilor și a investitorilor este slăbită.

Ce se așteaptă de la această inițiativă?

Obiectivul general este de a consolida reziliența operațională digitală a sectorului financiar al UE prin simplificarea și actualizarea legislației financiare existente a UE și prin introducerea de noi cerințe acolo unde există lacune, care să vizeze:

- îmbunătățirea gestionării de către societățile financiare a riscurilor TIC;
- o mai bună cunoaștere de către autoritățile de supraveghere a amenințărilor și a incidentelor;
- îmbunătățirea testării de către societățile financiare a propriilor sisteme TIC; și
- o mai bună supraveghere a riscurilor care decurg din dependența societăților financiare de furnizorii terți de servicii TIC.

Mai precis, propunerea ar crea mecanisme mai coerente și mai consecvente de raportare a incidentelor și, prin urmare, ar reduce sarcina administrativă pentru instituțiile financiare și ar consolida eficiența în materie de supraveghere.

Care este valoarea adăugată a acțiunii la nivelul UE?

Piața unică a UE pentru servicii financiare este reglementată de un număr mare de norme stabilite la nivelul UE, care le permit întreprinderilor financiare autorizate dintr-un stat membru să furnizeze servicii în cadrul întregii piețe unice cu ajutorul unui pașaport UE. Prin urmare, normele la nivel național nu ar fi o modalitate eficace de a consolida reziliența operațională a societăților financiare care utilizează pașaportul. În plus, cadrul unic de reglementare al UE conține, ca urmare a crizei financiare, norme foarte detaliate și prescriptive care abordează riscuri mai „tradiționale”, cum ar fi riscul de credit, riscul de piață, riscul de contraparte și riscul de lichiditate. Dispozițiile existente privind riscul operațional rămân generale. Consolidarea rezilienței operaționale digitale necesită ajustări ale dispozițiilor privind riscurile operaționale care sunt deja definite la nivelul UE — și, prin

urmare, pot fi actualizate și completate numai la nivelul UE.

B. Soluții

Ce opțiuni de politică legislative și fără caracter legislativ au fost luate în considerare? Există sau nu o opțiune preferată? De ce?

Evaluarea impactului a luat în considerare trei opțiuni, în plus față de scenariul de referință care nu implică nicio acțiune în ceea ce privește legislația UE privind serviciile financiare. Mai exact:

- **„Nicio acțiune”**: normele privind reziliența operațională ar fi stabilite în continuare de setul actual, divergent de dispoziții ale UE privind serviciile financiare, parțial de Directiva NIS, precum și de regimurile naționale existente sau viitoare;
- **Opțiunea 1 — consolidarea amortizoarelor de capital**: ar fi introdus un amortizor de capital suplimentar pentru a spori capacitatea societăților financiare de a absorbi pierderile care ar putea apărea din cauza lipsei de reziliență operațională;
- **Opțiunea 2 — un act privind reziliența operațională digitală a serviciilor financiare**: aceasta ar introduce un cadru cuprinzător la nivelul UE care să stabilească norme privind reziliența operațională digitală pentru toate instituțiile financiare reglementate, care
  - ar aborda riscurile TIC în mod mai cuprinzător,
  - le-ar permite autorităților de supraveghere financiară să aibă acces la informații cu privire la incidentele legate de TIC;
  - ar asigura că societățile financiare evaluează eficacitatea măsurilor lor de prevenire și de reziliență și identifică vulnerabilitățile în materie de TIC;
  - ar consolida normele privind externalizarea care reglementează supravegherea indirectă a furnizorilor terți de servicii TIC;
  - ar permite o supraveghere directă a activităților furnizorilor terți de servicii TIC atunci când aceștia le furnizează servicii societăților financiare și
  - în plus, ar stimula schimbul de informații privind amenințările în sectorul financiar.
- **Opțiunea 3 — un act privind reziliența combinat cu supravegherea centralizată a furnizorilor terți critici**: pe lângă un act privind reziliența operațională (opțiunea 2), ar fi creată o nouă autoritate care să supravegheze furnizorii terți de servicii TIC esențiale pentru societățile financiare. De asemenea, s-ar delimita mai clar sectorul financiar față de domeniul de aplicare al Directivei NIS.

Opțiunea preferată este opțiunea 2. În comparație cu celelalte opțiuni, este cea care contribuie la îndeplinirea celui mai mare număr de obiective ale inițiativei, ținând seama, în același timp, de criteriile de eficiență și coerență. Această opțiune se bucură, de asemenea, de cel mai mare sprijin din partea părților interesate.

Care sunt susținătorii fiecărei opțiuni?

Majoritatea părților interesate (private, publice) sunt de acord că este necesară o acțiune a UE pentru a proteja mai bine reziliența operațională a societăților financiare. Mulți consideră, de asemenea, că este necesar să se ia măsuri la nivelul UE pentru a aborda sarcinile de reglementare care decurg din faptul că societățile financiare fac obiectul unor norme repetitive și inconsecvente prevăzute în Directiva NIS, în legislația UE privind serviciile financiare și în regimurile naționale (de exemplu, în ceea ce privește raportarea incidentelor). În consecință, puține părți interesate sprijină opțiunea „nicio acțiune”. Puține părți interesate consideră că este necesară protejarea rezilienței operaționale prin intermediul unor amortizoare de capital sporite (opțiunea 1). Totuși, aceasta este abordarea tradițională a riscului operațional, în special în sectorul bancar, și prin urmare, este avută în vedere, de exemplu, de către organismele internaționale de standardizare. Tipul de măsuri calitative prevăzute la opțiunea 2, care ar simplifica și ar actualiza legislația financiară a UE și ar introduce noi cerințe în cazul în care există lacune, menținând în același timp legăturile cu Directiva orizontală NIS, beneficiază de un sprijin larg din partea părților interesate care au participat la consultarea publică. În timp ce unele părți interesate (în special publicul) recunosc valoarea unei supravegheri mai stricte a furnizorilor terți de servicii TIC de la opțiunea 3, crearea unei noi autorități a UE în acest scop se bucură doar de un sprijin limitat din partea părților interesate, ca și excluderea completă de la aplicarea cadrului NIS.

C. Impactul opțiunii preferate

Care sunt beneficiile opțiunii preferate (sau ale opțiunilor principale, dacă nu există o opțiune preferată)?

Opțiunea 2 ar aborda **riscurile TIC** în întregul sector financiar prin consolidarea capacităților instituțiilor financiare de a face față incidentelor TIC. Acest lucru ar reduce riscul răspândirii rapide a unui incident cibernetic pe piețele financiare. Deși este dificil să se estimeze costurile incidentelor operaționale din sectorul financiar (nu toate incidentele sunt raportate; sfera de cuprindere a costurilor este incertă), potrivit evaluărilor realizate de sector, costurile pentru sectorul financiar al UE s-ar putea situa între 2 și 27 de miliarde EUR pe an. Opțiunea

preferată ar atenua aceste costuri directe și orice impact mai extins pe care l-ar putea avea incidentele cibernetice majore asupra stabilității financiare. Eliminarea **cerințelor de raportare** care se suprapun ar reduce sarcinile administrative. De exemplu, pentru unele dintre cele mai mari bănci, economiile aferente pot varia între 40 și 100 de milioane EUR pe an. Raportarea directă ar spori, de asemenea, cunoștințele autorităților de supraveghere cu privire la incidentele TIC. Practicile de **testare armonizate** ar spori gradul de detectare a vulnerabilităților și riscurilor necunoscute. Aceasta ar reduce, de asemenea, costurile, în special pentru societățile transfrontaliere. De exemplu, pentru cele mai mari 44 de bănci transfrontaliere, beneficiile totale preconizate ale unei abordări comune în materie de testare s-ar putea situa între 11 și 88 milioane EUR. Prin introducerea unui set coerent de norme privind gestionarea riscurilor asociate **furnizorilor terți de servicii TIC**, societățile financiare ar avea mai mult control asupra modului în care furnizorii terți respectă cadrul de reglementare, ceea ce ar putea ajuta autoritățile de supraveghere. De asemenea, ar exista avantaje prudențiale care decurg din supravegherea prudențială a furnizorilor terți de servicii TIC. Per ansamblu, opțiunea preferată se traduce prin beneficii societale mai ample, generate de un mediu operațional mai rezilient pentru toți participanții la piața financiară și printr-o protecție sporită a consumatorilor și a investitorilor.

Care sunt costurile opțiunii preferate (sau ale opțiunilor principale, dacă nu există o opțiune preferată)?

Opțiunea preferată ar genera atât costuri punctuale, cât și costuri recurente. În ceea ce privește prima categorie, acestea se datorează investițiilor în sistemele informatice și sunt dificil de cuantificat, având în vedere starea diferită a sistemelor preexistente ale societăților. În absența unei intervenții de reglementare, unele societăți financiare au făcut deja investiții semnificative în sisteme TIC. Aceasta înseamnă că, pentru societățile financiare mari, costurile cu punerea în aplicare a măsurilor din prezenta propunere vor fi probabil scăzute. În cazul societăților mai mici, costurile ar trebui să fie, de asemenea, mai mici, deoarece acestea ar face obiectul unor măsuri mai puțin stricte, proporționale cu riscul lor mai scăzut. În ceea ce privește testarea, autoritățile europene de supraveghere au estimat că nivelul costurilor legate de testele de rezistență la intruziuni bazate pe amenințări variază între 0,1 % și 0,3 % din totalul bugetului TIC al societăților în cauză. Costurile legate de raportarea incidentelor ar fi reduse drastic, deoarece nu ar exista suprapuneri cu raportarea NIS. Autoritățile de supraveghere vor suporta, de asemenea, unele costuri, din cauza sarcinilor suplimentare pe care și le-ar asuma. De exemplu, în cazul autorităților de supraveghere care participă la supravegherea directă a furnizorilor terți de servicii TIC, creșterea estimată a ENI ar putea fi preconizată a se încadra între 1 și 5 ENI pentru autoritatea principală și aproximativ 0,25 ENI pentru autoritățile participante.

Care va fi impactul asupra societăților, a IMM-urilor și a microîntreprinderilor?

Opțiunea preferată ar viza toate societățile financiare, pentru a crește reziliența operațională a sectorului în ansamblul său. Acest domeniu de aplicare extins este important, având în vedere natura interconectată a sectorului financiar și nevoia corespunzătoare de a dispune de un nivel solid de reziliență operațională globală. Cu toate acestea, atunci când se definesc cerințele de bază în principalele domenii de intervenție, principiul proporționalității s-ar aplica atât pentru subsectoare, cât și pentru fiecare subsector. Aceasta ar lua în considerare, printre altele, diferențele în ceea ce privește modelele de afaceri, dimensiunea, profilul de risc, importanța sistemică etc. De exemplu, măsurile privind raportarea incidentelor și testarea ar fi mai puțin severe pentru societățile financiare mai mici.

Va exista un impact semnificativ asupra bugetelor și asupra administrațiilor naționale?

Nu. Supravegherea suplimentară poate necesita, după cum s-a demonstrat mai sus, un grad limitat de resurse suplimentare de supraveghere, care ar putea fi suportate integral sau parțial (dacă ar exista taxe de supraveghere) de bugetele publice.

Vor exista și alte efecte semnificative?

Consecințele socioeconomice ale pandemiei de Covid-19 ilustrează natura critică a piețelor financiare digitale și reziliența lor operațională. Opțiunea preferată ar crea o bază solidă pentru exploatarea transformării digitale, asigurându-se că piața unică a serviciilor financiare, inclusiv în sectorul bancar și al piețelor de capital, este rezilientă din punct de vedere operațional, bazată pe un set comun de norme și cerințe care urmăresc să asigure securitatea, performanța, stabilitatea și condiții de concurență echitabile. Aceasta va consolida, de asemenea, poziția Europei de lider financiar și digital în lume, un obiectiv stabilit de Comisie în comunicarea sa intitulată „Conturarea viitorului digital al Europei”.

D. Acțiuni ulterioare

Când va fi revizuită politica?

Prima revizuire va avea loc la 3 ani după intrarea în vigoare a instrumentului juridic. Comisia va prezenta un raport Parlamentului European și Consiliului cu privire la revizuirea realizată. Revizuirea ar putea fi sprijinită de o

consultare publică, studii, discuții la nivel de experți, anchete, ateliere, după caz.