Conselho da
União Europeia

Bruxelas, 24 de setembro de 2020
(OR. en)

11052/20
ADD 2

Dossiê interinstitucional:
2020/0268 (COD)

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

NOTA DE ENVIO

de:	Secretário-Geral da Comissão Europeia, assinado por Jordi AYET PUIGARNAU, Director
data de receção:	24 de setembro de 2020
para:	Jeppe TRANHOLM-MIKKELSEN, Secretário-Geral do Conselho da União Europeia
n.° doc. Com.:	SWD(2020) 204 final
Assunto:	DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO – RELATÓRIO DO RESUMO DA AVALIAÇÃO DE IMPACTO que acompanha o documento Proposta de Diretiva do Parlamento Europeu e do Conselho que altera as Diretivas 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, UE/2013/36, 2014/65/UE, (UE) 2015/2366 e UE/2016/2341

Envia-se em anexo, à atenção das delegações, o documento SWD(2020) 204 final.

Anexo: SWD(2020) 204 final

COMISSÃO
EUROPEIA

Bruxelas, 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:

DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO

RELATÓRIO DO RESUMO DA AVALIAÇÃO DE IMPACTO

que acompanha o documento

Proposta de Diretiva do Parlamento Europeu e do Conselho

que altera as Diretivas 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, UE/2013/36, 2014/65/UE, (UE) 2015/2366 e UE/2016/2341

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

Ficha de síntese

Avaliação de impacto sobre a proposta de regulamento relativo à resiliência operacional digital no setor financeiro

A. Necessidade de agir

Porquê? Qual é o problema em causa?

O setor financeiro depende amplamente das tecnologias da informação e comunicação (TIC). É provável que a atual pandemia de COVID-19 venha a intensificar esta dependência, tendo em conta os benefícios da garantia de um acesso remoto contínuo aos serviços financeiros. Contudo, a dependência das tecnologias digitais é motivo de preocupação; as empresas precisam de ser capazes de enfrentar possíveis perturbações no domínio das TIC, por forma a dar resposta às ameaças e aos incidentes digitais e a manter os seus serviços. Num setor financeiro extremamente interligado, que presta serviços vitais transfronteiriços de que a economia real depende, as vulnerabilidades decorrentes da dependência das TIC, embora aplicáveis a todos os setores económicos, são especialmente acentuadas devido: 1) à forte e ampla utilização das TIC; e 2) à possibilidade de os efeitos de um incidente operacional numa empresa financeira ou subsetor financeiro rapidamente se propagarem a outras empresas ou partes do setor financeiro e, em última instância, ao resto da economia.

Embora o setor financeiro esteja bastante avançado na sua integração de mercado e regulamentar e esteja a prosperar com base num conjunto único de regras harmonizadas — o conjunto único de regras da UE — a resposta da UE face às necessidades acrescidas de resiliência operacional tanto a nível horizontal como setorial tem:

- vindo a basear-se na harmonização mínima, deixando assim margem para interpretação nacional e fragmentação no mercado único, ou
- sido demasiado geral e de aplicação limitada, dando resposta ao risco operacional global de forma variável, através da regulamentação parcial de alguns componentes de *resiliência* operacional digital (por exemplo, a gestão do risco associado às TIC, a comunicação de incidentes e o risco relacionado com entidades terceiras no domínio das TIC), excluindo outros componentes (realização de testes).

Até à data, a intervenção da UE não deu resposta ao risco operacional de uma forma que satisfaça as necessidades de as empresas financeiras enfrentarem, responderem e recuperarem de vulnerabilidades no domínio das TIC, nem fornece aos supervisores financeiros as ferramentas necessárias para cumprirem o seu mandato de contenção da instabilidade financeira decorrente dessas vulnerabilidades no domínio das TIC.

As lacunas e inconsistências atuais conduziriam à proliferação de iniciativas nacionais não coordenadas (por exemplo, relativamente à realização de testes) e a abordagens de supervisão (por exemplo, dependências de entidades terceiras no domínio das TIC) que se traduzem em sobreposições ou duplicações de requisitos e em elevados custos administrativos e de conformidade para as empresas financeiras transfronteiriças ou em riscos associados às TIC não detetados nem abordados. De um modo geral, a estabilidade e integridade do setor financeiro não estão garantidas e o mercado único dos serviços financeiros permanece fragmentado, o que enfraquece a proteção do consumidor e do investidor.

O que se espera alcançar com a iniciativa?

O objetivo geral consiste em fortalecer a resiliência operacional digital do setor financeiro da UE através da simplificação e atualização da legislação financeira da UE existente e da introdução de novos requisitos quando existam lacunas, com vista a:

- melhorar a gestão dos riscos associados às TIC pelas empresas financeiras;
- aprofundar o conhecimento dos supervisores sobre as ameaças e incidentes;
- melhorar a realização pelas empresas financeiras de testes dos seus sistemas de TIC; e
- supervisionar de forma mais eficaz os riscos decorrentes da dependência das empresas financeiras em relação às entidades terceiras prestadoras de serviços no domínio das TIC.

Mais concretamente, a proposta pretende criar mecanismos de comunicação de incidentes mais coerentes e consistentes e, assim, reduzir os encargos administrativos das instituições financeiras e melhorar a eficácia de supervisão.

Qual o valor acrescentado da ação a nível da UE?

O mercado único da UE para os serviços financeiros é regulado por um vasto conjunto de regras definidas a nível da UE que permite que as empresas financeiras autorizadas num Estado-Membro prestem serviços em todo o mercado único graças a um passaporte da UE. Consequentemente, as regras a nível nacional não constituiriam uma forma eficaz de reforçar a resiliência operacional das empresas financeiras que utilizem o passaporte. Além disso, o conjunto único de regras da UE contém, como resultado da crise financeira, regras extremamente detalhadas e prescritivas que abordam os riscos mais «tradicionais», como riscos associados ao crédito, ao mercado, às contrapartes e à liquidez. As disposições existentes relativas ao risco operacional

permanecem gerais. O reforço da resiliência operacional digital requer ajustes nas disposições relativas aos riscos operacionais que já estão definidas a nível da UE e, consequentemente, apenas podem ser atualizadas e complementadas a nível da UE.

B. Soluções

Que opções legislativas e não legislativas foram ponderadas? É dada preferência a alguma das opções? Porquê?

A avaliação de impacto considerou três opções além do cenário de base de nenhuma ação no que diz respeito à legislação referente aos serviços financeiros da UE. Mais especificamente:

- «**Nenhuma ação**»: as regras relativas à resiliência operacional continuariam a ser estabelecidas pelo atual conjunto divergente de disposições referentes aos serviços financeiros da UE, parcialmente pela Diretiva SRI e pelos regimes nacionais existentes ou futuros;
- **Opção 1 – reforço das reservas de capital**: seria introduzida uma reserva de capital adicional com vista a aumentar a capacidade das empresas financeiras para absorverem perdas que pudessem surgir devido à falta de resiliência operacional;
- **Opção 2 – um ato relativo à resiliência operacional digital dos serviços financeiros**: seria introduzido um quadro abrangente a nível da UE com regras referentes à resiliência operacional digital para todas as instituições financeiras, que permitiria
    - abordar os riscos associados às TIC de forma mais abrangente,
    - facilitar o acesso dos supervisores financeiros a informações sobre os incidentes relacionados com as TIC,
    - garantir que as empresas financeiras avaliam a eficácia das suas medidas preventivas e de resiliência e identificam as vulnerabilidades no domínio das TIC;
    - reforçar as regras de externalização que regem a fiscalização indireta das entidades terceiras prestadoras de serviços no domínio das TIC;
    - facilitar a fiscalização direta das atividades de entidades terceiras prestadoras de serviços no domínio das TIC sempre que prestem os seus serviços a empresas financeiras e,
    - adicionalmente, incentivar o intercâmbio de informações sobre as ameaças no setor financeiro.
- **Opção 3 – ato relativo à resiliência combinado com a supervisão centralizada das entidades terceiras prestadoras de serviços consideradas críticas**: além de um ato relativo à resiliência operacional (opção 2), seria criada uma nova autoridade com vista a supervisionar as entidades terceiras prestadoras de serviços considerados críticos no domínio das TIC a empresas financeiras. De igual modo, iria delinear de forma mais clara o setor financeiro do âmbito de aplicação da Diretiva SRI.

A opção 2 é a preferida. Em comparação com as outras opções, é aquela que atinge a maioria dos objetivos da iniciativa, tendo em conta os critérios de eficiência e da coerência. Esta opção também é a mais apoiada pelas partes interessadas.

Quem apoia cada uma das opções?

A maioria das partes interessadas (privadas e públicas) aceita que a ação da UE é necessária por forma a melhor salvaguardar a resiliência operacional das empresas financeiras. Várias acreditam que a ação da UE é necessária para dar resposta aos encargos regulamentares decorrentes do facto de as empresas financeiras estarem sujeitas a regras duplicadas e inconsistentes estabelecidas na Diretiva SRI, em legislação relativa aos serviços financeiros da UE e em regimes nacionais (por exemplo, no que diz respeito à comunicação de incidentes). Em conformidade, poucas partes interessadas apoiam a opção «Nenhuma ação». Poucas partes interessadas veem vantagens em garantir a resiliência operacional através do aumento das reservas de capital (opção 1). De qualquer modo, esta é a abordagem tradicional face ao risco operacional, nomeadamente no setor bancário, e é, como tal, considerada pelos organismos de normalização internacionais, por exemplo. O tipo de medidas qualitativas definidas na opção 2 que irão simplificar e atualizar a legislação financeira da UE e introduzir novos requisitos onde existam lacunas mantendo simultaneamente as ligações à Diretiva SRI horizontal reúne o apoio abrangente das partes interessadas que responderam à consulta pública. Enquanto algumas partes interessadas (nomeadamente públicas) veem vantagens na supervisão reforçada das entidades terceiras prestadores de serviços no domínio TIC da opção 3, a criação de uma nova autoridade para esse fim apenas tem um apoio limitado das partes interessadas, tal como uma rutura mais completa com o quadro da Diretiva SRI.

C. Impacto da opção preferida

Quais são os benefícios da opção preferida (se existir; caso contrário, das principais opções)?

A opção 2 irá abordar os **riscos associados às TIC** no setor financeiro através da melhoria das capacidades das instituições financeiras para enfrentarem os incidentes no domínio das TIC. Tal reduzirá o risco de um

incidente cibernético se disseminar rapidamente nos mercados financeiros. Embora seja difícil estimar os custos dos incidentes operacionais no setor financeiro (nem todos os incidentes são comunicados; âmbito dos custos incerto), as avaliações do setor sugerem que os custos para o setor financeiro da UE podem variar entre 2 e 27 mil milhões de EUR por ano. A opção preferida irá atenuar estes custos diretos e quaisquer impactos mais vastos que incidentes cibernéticos graves possam ter na estabilidade financeira. A eliminação da sobreposição de **requisitos de comunicação** reduzirá os encargos administrativos. Por exemplo, para alguns dos maiores bancos as poupanças associadas podem variar entre 40 e 100 milhões de EUR por ano. A comunicação direta de informações também aprofundará o conhecimento dos supervisores sobre os incidentes no domínio das TIC. As práticas de **harmonização dos testes** melhorarão a deteção de vulnerabilidades e riscos desconhecidos. Tal reduzirá também os custos, principalmente para as empresas transfronteiriças. Por exemplo, para os 44 maiores bancos transfronteiriços, os benefícios totais previstos de uma abordagem comum de realização de testes poderão variar entre 11 e 88 milhões de EUR. Com a introdução de um conjunto coerente de regras em matéria de gestão de riscos de **entidades terceiras prestadoras de serviços no domínio das TIC**, as empresas financeiras poderão controlar melhor o modo como as entidades terceiras prestadoras de serviços cumprem o quadro regulamentar, o que poderá tranquilizar os supervisores. Existirão ainda benefícios prudenciais decorrentes da fiscalização de entidades terceiras prestadoras de serviços no domínio das TIC pelas entidades de supervisão. De um modo geral, a opção preferida traduz-se em benefícios societais mais abrangentes, decorrentes de um ambiente operacional mais resiliente para todos os participantes do mercado financeiro e da proteção reforçada do consumidor e do investidor.

Quais os custos da opção preferida (ou, caso contrário, das opções principais)?

A opção preferida dará origem a custos pontuais e recorrentes. No que respeita aos primeiros, estes devem-se aos investimentos em sistemas de TI e são difíceis de quantificar tendo em conta o diferente estado dos sistemas já existentes das empresas. Na ausência de uma intervenção regulamentar, algumas empresas financeiras já investiram consideravelmente em sistemas TIC. Tal significa que para grandes empresas financeiras, a aplicação das medidas da presente proposta será provavelmente reduzida. Para empresas mais pequenas, prevê-se que os custos também sejam inferiores, uma vez que estarão sujeitas a medidas menos rigorosas, proporcionadas ao seu menor risco. No que se refere à realização de testes, as Autoridades Europeias de Supervisão preveem que os custos relacionados com a realização de testes de penetração motivados por ameaças variem entre os 0,1 % e os 0,3 % do orçamento total no domínio das TIC das empresas em questão. Os custos relacionados com a notificação de incidentes serão drasticamente reduzidos, visto que deixará de haver sobreposições com a comunicação de informações no âmbito da SRI. Os supervisores também incorrerão em alguns custos devido às tarefas adicionais que assumirão. Por exemplo, no caso dos supervisores envolvidos na fiscalização direta de entidades terceiras prestadoras de serviços no domínio das TIC, o aumento estimado em equivalentes a tempo inteiro (ETI) pode variar entre 1 e 5 ETI para a autoridade principal e cerca de 0,25 ETI para as autoridades participantes.

Como serão afetadas as empresas, as PME e as microempresas?

A opção preferida abrangerá todas as empresas financeiras, com vista a aumentar a resiliência operacional da totalidade do setor. Este âmbito abrangente é importante à luz da natureza interligada do setor financeiro e da correspondente necessidade de assegurar um nível sólido de resiliência operacional global. No entanto, na definição dos requisitos principais em todas as principais áreas de intervenção, o princípio de proporcionalidade será aplicável a todos os subsetores, bem como a cada um dos subsetores. Serão tidas em conta, entres outras, as diferenças em termos de modelos empresariais, tamanho, perfil de risco, importância sistémica, etc. Por exemplo, as medidas referentes à comunicação de incidentes e realização de testes serão menos rigorosas para as empresas financeiras mais pequenas.

Haverá impactos significativos nos orçamentos e administrações públicas nacionais?

Não. A fiscalização adicional pode, conforme demonstrado anteriormente, exigir um nível limitado de recursos de supervisão adicionais que podem ser total ou parcialmente (se existirem taxas de supervisão) suportados pelos orçamentos públicos.

Haverá outros impactos significativos?

As consequências socioeconómicas da pandemia de COVID-19 ilustram a natureza crítica dos mercados financeiros digitais e da sua resiliência operacional. A opção preferida irá estabelecer uma base sólida com vista a aproveitar a transformação digital, assegurando que o mercado único dos serviços financeiros, incluindo no setor bancário e nas uniões de mercados de capitais, é operacionalmente resiliente, com base num conjunto comum de regras e requisitos que visam a segurança, o desempenho, a estabilidade e condições equitativas. Tal irá também reforçar a posição da Europa enquanto líder financeiro e digital no mundo, um objetivo estabelecido pela Comissão na sua Comunicação «Construir o futuro digital da Europa».

D. Acompanhamento
Quando será revista a política?
A primeira revisão deverá ter lugar três anos após a entrada em vigor do instrumento jurídico. A Comissão apresentará um relatório ao Parlamento Europeu e ao Conselho relativo à sua revisão. A revisão pode ser fundamentada através de uma consulta pública, de estudos, discussões de peritos, inquéritos, seminários, conforme adequado.