DORA
Tinhamos mesmo de ter mais este regulamento?

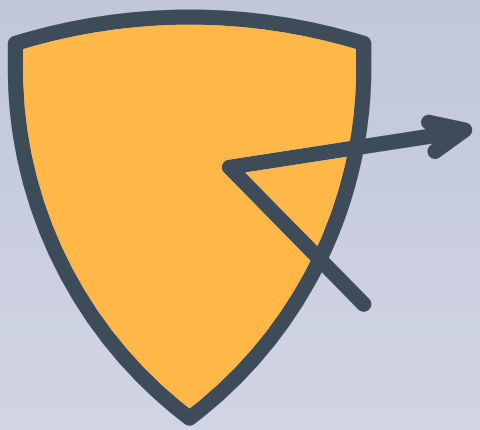
REGULATIONS

Nicole Fortunato

Nicole Fortunato é associada coordenadora na Morais Leitão. Integra a equipa de societário, comercial e M&A e a equipa de TMT.
Desenvolve a sua atividade essencialmente com empresas e transações orientadas para as novas tecnologias e tecnologias emergentes (*blockchain, smart contracts, AI – Artificial Intelligence, IoT - Internet of Things, RPA – Robotic Process Automation, edge computing*, etc.).
É especializada em *IT contracting*, desenvolvimento legal de *Apps*, contratação e desenvolvimento de *software* e marketing digital, tendo uma vasta experiência de assessoria legal nesta área de negócio, inclusive como advogada *in house* de grandes empresas do sector. Presta, ainda, assessoria em matérias de media e privacidade quando relacionadas com as suas áreas de atuação.

Ashick Remetula

Ashick Remetula é associado na Morais Leitão. Integra a equipa de bancário e financeiro e a Team Genesis.
Tem experiência na área de regulação e transações financeiras, e ainda em Projetos, no sector de Energia e Infraestruturas, incluindo em operações de M&A.
Desenvolve a sua atividade na área de Fintech com especial ênfase para empresas e transações que lidem com novas e emergentes tecnologias, matérias relacionadas com *blockchain* e *web3.0*, cripto-ativos e NFTs, *crowdfunding* e *ICOs*, em concreto quanto a regulação financeira e matérias societárias.
Conta ainda com experiência em operações financeiras, abrangendo financiamento estruturado e *project finance*, financiamentos sindicados, empréstimos garantidos e operações de refinanciamento.
Tem ainda experiência em *islamic finance* (*sharia compliant finance*).



O Regulamento DORA visa reforçar a resiliência operacional das instituições financeiras na UE, impondo normas rigorosas para gestão de riscos sistémicos no sector financeiro. O novo normativo exigirá que as entidades abrangidas implementem medidas de resiliência, como testes de penetração regulares e comunicação de incidentes. Além disso, estabelece requisitos rigorosos para a seleção e monitorização de prestadores de serviços TIC críticos. Entrando em vigor em janeiro de 2025, as instituições financeiras têm sensivelmente 4 meses para "porem as mãos na massa".

Novas preocupações para as instituições financeiras (que incluem, entre outros, instituições de crédito, de pagamento e seguradoras): falamos do Regulamento (UE) 2022/2554 relativo à resiliência operacional do sector financeiro, mais vulgarmente conhecido por Regulamento DORA, pelo que é assim que o vamos tratar aqui. E atenção: entra em vigor em janeiro de 2025, e exige preparação prévia das instituições financeiras em vários domínios.

O que é e do que trata?

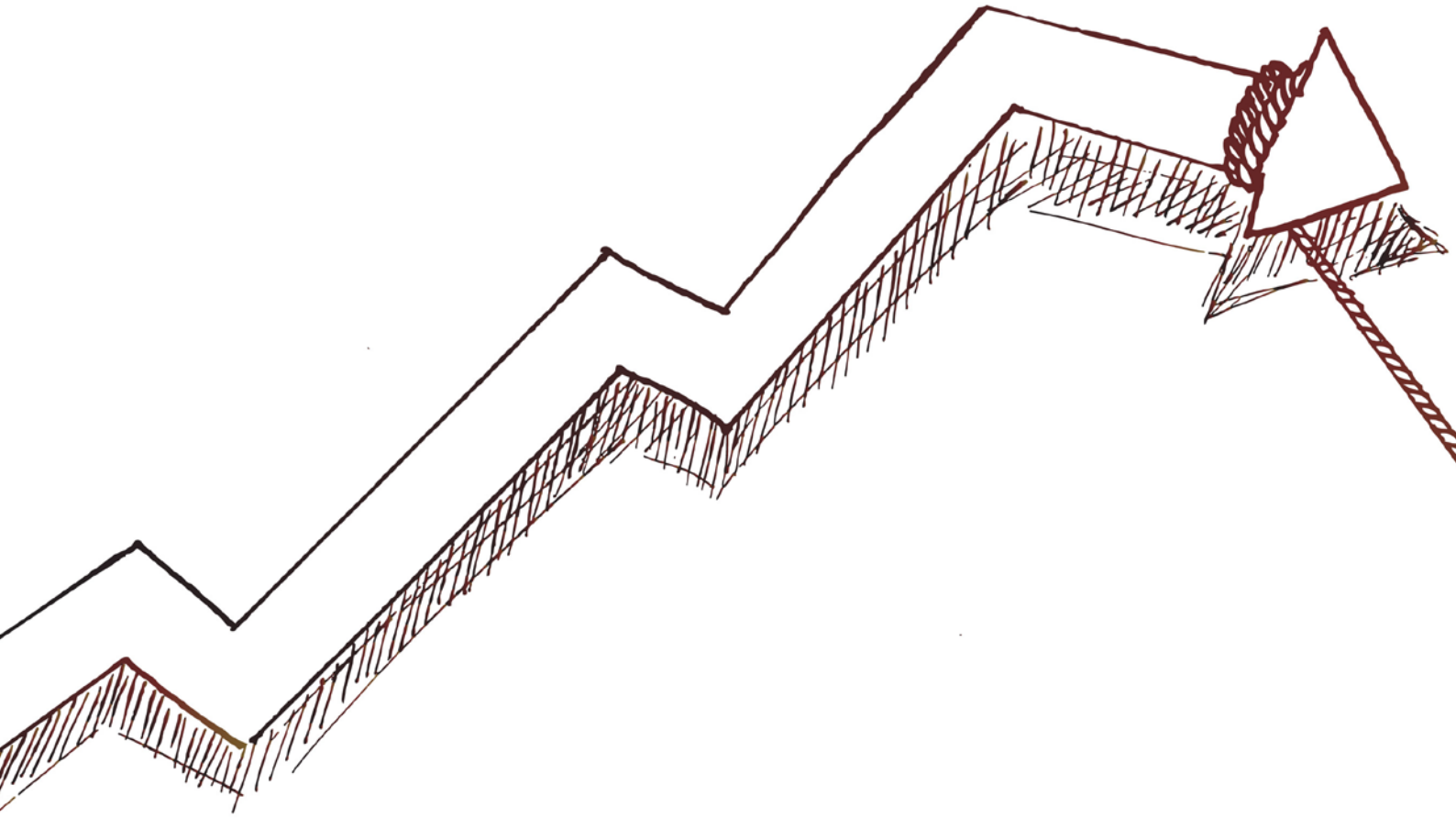
O Regulamento DORA vem impor normas em três áreas principais importantes para a gestão do risco sistémico do sector financeiro: resiliência operacional, risco de concentração e coordenação.

Um dos principais objetivos do Regulamento DORA é o reforço da capacidade de resiliência operacional das instituições financeiras. Ao impor um quadro de medidas e protocolos (*e.g.*, quadros de gestão do risco abrangentes, testes de resiliência regulares, comunicação de incidentes) destinados a fortalecer a resiliência operacional das instituições financeiras, o Regulamento DORA procura garantir que o sector esteja mais preparado para enfrentar e neutralizar ataques cibernéticos e perturbações tecnológicas, garantindo a continuidade dos serviços críticos a todo o momento.

A resiliência operacional em apreço não se limita à prevenção de incidentes isolados, mas à manutenção da integridade e continuidade de serviços críticos durante uma "crise". Exige que as instituições financeiras identifiquem as suas funções críticas e estabeleçam planos de contingência robustos, que incluam não apenas procedimentos internos, mas também respostas concertadas com os seus subcontratados. Ao fazê-lo, este novo quadro regulamentar visa instituir um ecossistema financeiro no qual a falha de uma entidade não conduza a um "efeito dominó", mitigando assim o risco sistémico.

Em segundo lugar, o DORA estabelece requisitos rigorosos para a seleção e monitorização de prestadores de serviços críticos. As instituições financeiras devem realizar avaliações detalhadas dos riscos associados a esses fornecedores e garantir que os contratos incluem cláusulas que permitam uma resposta eficaz em caso de falhas. Além disso, o Regulamento DORA introduz um regime de supervisão para prestadores de serviços de tecnologias da informação e comunicação (TIC) críticos, o que significa que esses estarão sujeitos a uma supervisão direta por parte das autoridades europeias competentes.

Em terceiro, o DORA promove a coordenação e a transparência entre instituições financeiras, reguladores e prestadores de serviços TIC. Essa colaboração, orientada por normas comuns e partilha de informação, assegura uma resposta rápida e coordenada a qualquer ameaça, reforçando a estabilidade do sistema financeiro.



Desejável ou evitável?

Na maioria das matérias que regula, arriscamos dizer "desejável", e não é só porque somos os "suspeitos do costume" que (pensará o leitor!) gosta de novas leis. Este fazia falta. E explicamos porquê.

À medida que o sector financeiro se foi tornando cada vez mais dependente de infraestruturas e sistemas digitais, as várias autoridades de supervisão, e principalmente as europeias, foram emitindo orientações e recomendações às entidades por si supervisionadas sobre o recurso a terceiros para desempenho de funções críticas ou importantes, designadamente pelo recurso a computação em nuvem que, como se sabe, implica uma migração dos dados controlados pela instituição financeira para espaços na *cloud* controlados por terceiros. No entanto, sendo meras recomendações ou orientações, estas podiam ser acolhidas por cada Estado-membro de forma distinta, e logo por aí, o grau de exigência das autoridades de supervisão era também divergente. Para além disso, muitos prestadores de serviços de TIC recusavam-se (e alguns ainda se recusam!) a aceitar a incorporação das mesmas nos seus serviços.

Ora, entre a falta de consistência na aplicação europeia (reconhecida pelos próprios considerandos do Regulamento) e a falta de reconhecimento destas "recomendações" como obrigatórias, estavam reunidas condições suficientes para se criar (mais um) regulamento europeu. Mas há outras razões, e uma que nos parece particularmente importante: a dependência das entidades financeiras da utilização de serviços TIC. Esta ocorre tanto a nível interno – há atualmente clientes bancários que só utilizam os canais digitais – como a nível de contratação de terceiros (prestadores de serviços TIC). E esta última, pela nossa experiência como assessores legais, tem desafios e preocupações que justificam mesmo uma intervenção regulatória.

E porquê?

Vejamos um exemplo: o cliente bancário comum não tem visibilidade sobre a complexidade de sistemas que estão por detrás de um (aparentemente simples) canal digital bancário. E se inicialmente estes canais digitais apareceram como uma oferta acessória (e quase inutilizada!) de alguns bancos ditos mais modernos, atualmente podemos afirmar que será praticamente impossível que um banco sobreviva sem um. E, para que isso aconteça, há todo um conjunto de sistemas, dados, API's, protocolos de comunicação, *software* e *hardware* que se interligam entre si para que uma simples página de *home banking* seja possível, fiável e útil. Desde os mecanismos de acesso, até aos *terabytes* de informação armazenada em *clouds*, e aos mecanismos de deteção de fraude sobre transações, tudo se liga numa complexa teia de ligações, dados e sistemas que quase sempre envolvem a contratação de serviços a terceiros.

E a pergunta é: e se os serviços técnicos da instituição financeira falham? E se esse prestador terceiro falha? E se, de repente, o serviço que a instituição financeira contratou a terceiro se torna de tal maneira uma peça fundamental nesta rede complexa de sistemas e dados que, falhando, põe em causa todo o sistema? E mesmo que esse serviço não falhe, poderá essa dependência pôr em causa a independência e autonomia da instituição financeira, colocando-a como refém de um serviço de terceiro para funções absolutamente essenciais da sua atividade?

Uma falha nesta teia tão complexa pode facilmente levar a uma falha dos serviços essenciais que o sector financeiro presta. Operações tão simples como fazer um pagamento ou realizar uma transferência podem ficar comprometidas, e o Regulamento DORA procura garantir que tanto ao nível interno na instituição financeira como quando recorra a terceiros, esse risco de disrupção é anulado ou, pelo menos, mitigado, tanto ao nível da instituição como num potencial efeito sistémico.

O caso particular do risco de concentração: a dependência de prestadores terceiros

Nas negociações de serviços entre instituições financeiras e prestadores de serviços de TIC, o poder de negociação quase nunca é equilibrado. Pense-se, por exemplo, na negociação de qualquer serviço com uma das *big five* (Alphabet – dona da Google, Amazon, Apple, Meta e Microsoft)*:* é quase naturalmente aceite pela instituição financeira que terá pouca ou nenhuma margem de negociação. E as *big five* (ou qualquer outra empresa prestadora de serviços de TIC) não fazem isto, parece-nos, com qualquer intenção sórdida de não acautelar os interesses da instituição financeira sua cliente, mas apenas, espera-se, porque também elas precisam de algum nível de harmonização das suas condições contratuais ao nível global (sob pena de o processo de contratação se tornar ingerível). E o que um cliente pede quase nunca corresponde ao que outro, muitas vezes do mesmo sector, pede – lá está, por falta de harmonização de regras e da sua aplicação.

O serviço é necessário e muitas vezes difícil de substituir, ou substituível apenas por outro concorrente de igual gabarito. E é aí que o Regulamento DORA é útil: uniformiza regras, e essas regras procuram garantir que o recurso a prestadores de serviços de TIC não perturba (ou perturba o menos possível) o normal funcionamento das atividades essenciais de uma instituição financeira. Como? Obrigando, por exemplo, os prestadores de serviços de TIC a permitirem que as instituições financeiras os auditem nas suas funções, a criar mecanismos de cooperação com as autoridades de supervisão, a descrever níveis de serviço e a revê-los com regularidade, a permitir à instituição financeira um acesso imediato e permanente aos seus dados,

a criar planos de continuidade de negócio em caso de disrupção severa dos serviços e direitos especiais de cessação dos serviços, onde se inclui garantir uma transição ordenada dos serviços. A maioria destas regras já constavam das recomendações das autoridades que antecederam o Regulamento DORA, mas estas ressurgem agora com força (indiscutível) de lei e com uma distinção importante entre as que se exigem a serviços críticos e a serviços não críticos.

A implementação do Regulamento DORA marca, por isso, um desenvolvimento significativo no reforço da resiliência operacional e digital das instituições financeiras.

Em conclusão, o Regulamento DORA é desejável e, a bem de todo o sistema financeiro, inevitável. À medida que a transformação digital continua a remodelar o sector financeiro, a implementação do Regulamento DORA, bem como das suas normas técnicas regulamentares que vão sendo publicadas pelas Autoridades Europeias de Supervisão – *European Bank Authority (EBA), European Securities and Markets Authority (ESMA)* e *European Insurance and Occupational Pensions Authority (EIOPA)* são cruciais para garantir que o mesmo se mantém resiliente e estável, sem contudo por em causa a sua crescente inovação e digitalização.

O que falta fazer?

Dependendo, normalmente, do sector onde atua e da sua dimensão, as instituições financeiras e os prestadores de serviços TIC estarão atualmente mais ou menos preparados para cumprir o Regulamento DORA. Mas todos, sem exceção, precisam de verificar os seus processos e contratos atuais para perceberem, pelo menos, onde é que estão ou não estão a cumprir.

De um modo geral, a adaptação a este regulamento passa por um processo de cariz técnico (de revisão da arquitetura de sistemas de tecnologias de informação e das políticas e procedimentos internos associados à mesma) e outro de cariz legal (revisão dos contratos de TIC celebrados de maneira a garantir a inclusão das chamadas *key contractual provisions* previstas no Regulamento DORA). Como dizem os ingleses, *a stitch in time saves nine*, pelo que menos de cinco meses da eficácia plena deste regulamento, diríamos, em bom português, que está na altura de "por mãos à obra" Ø.