BANCO DE PORTUGAL
EUROSISTEMA

XXIX ENCONTRO DE LISBOA

Entre os Bancos Centrais dos Países de Língua Portuguesa

IMPLICAÇÕES DA INOVAÇÃO TECNOLÓGICA NA ATIVIDADE FINANCEIRA

Workshops

11 de outubro de 2019

1 Os novos modelos de negócio

Introdução

Contexto e trabalho realizado

Contexto económico e social

Contextos diferentes mas igualmente desafiantes.

Evolução à escala global da tecnologia e das preferências e comportamentos das populações.

Transformação da atividade financeira com implicações a vários níveis.

O Grupo do *Workshop* 1 – Novos Modelos de Negócio

Participantes de praticamente todos os Bancos Centrais dos BCPLP.
(Angola, Brasil, Guiné-Bissau, Moçambique, Portugal, São Tomé e Príncipe, Timor-Leste).

Colaboração ativa, discussão de ideias, partilha de experiências e formulação de ações futuras.

Foco: implicações na atividade e nos agentes de intermediação financeira e a resposta dos supervisores.

Principais conclusões (1/2)

Desafios

Mercado

- Diferentes novos agentes de serviços financeiros (e.g. **operadoras móveis**).
- Sistemas com projeção internacional (BigTechs) e com potencial disruptivo: "**serviços sem fronteiras**"
- **Interoperabilidade** da infraestrutura (pagamentos).

Regulação

- Regulação **abrangente** (novas tecnologias)
- Identificação de clientes e abertura de conta (KYC, **bancarização**).
- Atuar num regime de **cooperação** (e.g. nacional e internacional).

Supervisão

- Novos desafios de negócio e **rentabilidade** e avaliação de novos riscos (ciber).
- Literacia e **inclusão** financeiras.
- ***Level playing field.***
- Organização interna de estrutura, governo e processos (e cooperação), **recursos** (formação e capacitação) e novas práticas / atividades.

Principais conclusões (2/2)

Soluções, melhores práticas, recomendações e conclusões

Mercado

- Papel das operadoras móveis na inclusão e bancarização, enquadradas na regulação e nas práticas de **supervisão** dos Bancos Centrais.
- Infraestruturas que promovam a proliferação dos serviços através da interoperabilidade e a **concorrência** de mercado necessária.

Regulação

- **Regulação clara** de atividades financeiras que permita incluir as inovações (IME).
- Atividades de experimentação e comunicação com o mercado (**sandboxes**).
- Avaliação e adoção de mecanismos uniformes para identificação de clientes e abertura de conta que garantam a segurança e cumprimento dos requisitos regulatórios e promovam a **inclusão**.

Supervisão

- Foco da **regulação sobre a atividade e não entidade**, garantindo a segurança dos consumidores e estabilidade financeira.
- Estabelecimento ou revisão de **acordos de cooperação**, para acomodar as novas políticas e desafios.

Propostas

Ideias chave e ações futuras

Ideias chave

- **Missão comum** de garantir a proteção dos consumidores, estabilidade do sistema financeiros e funcionamento das infraestruturas de mercado.
- **Desafio comum** de não impedir a inovação garantindo ao mesmo o cumprimento regulatório justo e adequado.
- **Desafios específicos** em torno dos novos modelos de negócio do sistema financeiro.

Ações futuras

- Contribuições **regulamentares** específicas sobre matérias inovadoras de supervisão (serviços de pagamentos).
- Partilha de melhores práticas de **organização** e atuação interna entre os Bancos Centrais, de forma a permitir a sua adoção e implementação.
- Ações de cooperação sobre **formação** específica para recursos especializados.
- Programas de **intercâmbio** temporário de colaboradores em áreas inovadoras de conhecimento.
- Partilha de **ferramentas** práticas de supervisão, monitorização e avaliação e regulação.

2 A inclusão financeira e a proteção do cliente dos serviços financeiros

1. Quadro Vigente

a. Organização Institucional

- Avanços notórios quanto à organização institucional, sendo de destacar a **criação e fortalecimento de unidades de estrutura que respondem pelas áreas de inclusão e educação financeira bem como de supervisão da conduta das inovações tecnológicas** no sistema financeiro

b. Quadro de Políticas e Estratégias

- **Cooperação com organismos e iniciativas internacionais que velam pela implementação de boas práticas visando o equilíbrio entre inclusão, protecção do consumidor, estabilidade e integridade financeiras** (exemplos: FinCoNet, AFI, CYFI, GPFI, FATAF, ESAAMLG, WSD)
- Existência por parte de alguns BCPLP de uma **Estratégia Nacional de Inclusão ou Educação Financeira**

1. Quadro Vigente

c. Quadro Legal e Regulamentar

- Revisão do quadro legal e regulamentar com vista a **responder aos avanços da tecnologia e inovações financeiras**

- Principais reformas para garantir o equilíbrio entre oportunidades e riscos resultantes das tecnologias financeiras (FinTechs):

  i. **Regulamentação sobre a prestação de serviços de pagamento e a emissão de moeda eletrónica** tendo como base a Lei das Instituições de Crédito e Sociedades Financeiras ou a Lei do Sistema Nacional de Pagamentos

  ii. **Normas sobre os serviços financeiros digitais no geral, incluindo as tecnologias financeiras (fintechs)**

  iii. **Normas sobre a conduta do mercado e protecção do consumidor**

  iv. **Normas sobre a interoperabilidade** entre os pagamentos electrónicos realizados pelas instituições bancárias, instituições de moeda electrónica e demais prestadores de serviços de pagamento

  v. **Normas sobre o funcionamento dos agentes bancários e Microfinanças** com vista a assegurar a expansão dos serviços financeiros paras as zonas com fraca cobertura de bancos

1. Quadro Vigente

d. Quadro das Inovações (soluções fintech/Suptech)

i. **Adoção e implementação de incubadoras regulamentares (*sandbox* regulatório e *hubs* de inovação)** para testes de inovação financeira não previstos a nível da regulamentação

ii. **Disponibilização de serviços financeiros digitais incluindo por *fintech*** (abertura de conta e crédito nos canais digitais e pagamentos por telemóvel)

iii. **Iniciativas de supervisão baseadas em tecnologia (*suptech*)**

iv. **Procedimentos de captação de dados de inclusão financeira baseada em tecnologia**

2. Principais Desafios e Recomendações

a. No âmbito de Inclusão Financeira

Nº	Desafio	Recomendação
1.	**Definir e melhorar a implementação de uma Estratégia Nacional de Inclusão Financeira**	• Adotar, implementar e melhorar uma Estratégia Nacional de Inclusão Financeira, com especial enfoque nos Serviços Financeiros Digitais e no Empoderamento do Consumidor/ Literacia Financeira • Criar um Departamento/ Núcleo de Inclusão Financeira a nível dos Bancos Centrais
2.	**Acompanhar a inovação e adequar o quadro legal e regulamentar**	• Dinamizar o processo de interoperabilidade multilateral entre as instituições de pagamento e de moeda eletrónica e/ou bancos • Garantir a definição de requisitos de KYC em níveis (tiered KYC) para os diferentes segmentos e níveis de risco de cliente • Criar produtos financeiros para atender ao segmento de baixa renda
3.	**Melhorar a colaboração internacional**	• Participar nos encontros de trabalho e fóruns internacionais • Reforçar competências para a promoção da inclusão, educação financeira e nivelamento dos objetivos de inclusão e integridade financeira

2. Principais Desafios e Recomendações

b. No âmbito de protecção ao consumidor e educação financeira

Nº	Desafio	Recomendação
1.	**Desenvolver uma estratégia nacional de educação financeira**	• Identificar e envolver os principais intervenientes • Disponibilizar informação atualizada e em linguagem simples sobre produtos e serviços financeiros (ex. Portais dos BCPLP) • Promover a literacia financeira digital
2.	**Criar e aprimorar o quadro legal de protecção do consumidor**	• Regulamentar o quadro publicitário das instituições financeiras • Adequar o quadro legal e regulamentar sobre (a) Proteção do Consumidor de Produtos e Serviços Financeiros; e (b) Garantias Mobiliárias.
3.	**Melhorar a organização institucional**	• Elaborar e adequar o Manual de Supervisão de Conduta

2. Principais Desafios e Recomendações

c. No âmbito da supervisão e fiscalização das inovações financeiras

Nº	Desafio	Recomendação
1	**Assegurar a supervisão e fiscalização das inovações financeiras**	• **Repensar o perímetro de supervisão**, no sentido de assegurar que todos os prestadores de serviços financeiros (incluindo Telcos) sejam integrados • **Repensar as ferramentas de supervisão**, estabelecendo mecanismos que garantam a avaliação do cumprimento do quadro normativo • **Capacitar o supervisor** com o *know-how* tecnológico necessário para a prossecução das respetivas atividades • **Incrementar a colaboração entre as diferentes autoridades** de supervisão e ainda com as entidades responsáveis pela fiscalização dos Telcos

3. Ações Futuras

- **Desenvolver iniciativas de cooperação** a nível regional e internacional
- **Realizar pesquisas/inquérito de avaliação nacional do lado da oferta e da procura** de produtos e serviços financeiros
- **Garantir a capacitação institucional** nas áreas ligadas à inovação financeira e à proteção do consumidor de serviços financeiros
- **Promover inovações favoráveis à inclusão financeira** e proveito dos segmentos de população excluída (jovens, mulheres, PME, populações rurais e pessoas com baixa educação financeira, etc.)
- **Assegurar a interoperabilidade multilateral** com destaque para os serviços financeiros digitais

3 Cibersegurança

Contexto

- A crescente oferta de produtos e serviços financeiros, suportados em TI, tornam as instituições financeiras mais vulneráveis a ciberataques. No atual contexto dinâmico e de múltiplas interligações, a cibersegurança deve constituir uma das **prioridades de topo**.

- **Falhas de segurança** colocam em causa a Inclusão Financeira, promovendo a desconfiança e desmotivação na utilização de serviços eletrónicos financeiros.

- Investir na cibersegurança é **investir no futuro**, como suporte de uma estratégia de desenvolvimento com forte aposta nas tecnologias digitais.

Desafios

RECURSOS – HUMANOS E TECNOLÓGICOS

- Dispor de **colaboradores especializados** em cibersegurança, para assegurar as várias funções de ciberproteção das instituições; existe atualmente uma grande lacuna a este nível.

- Fazer de cada pessoa da instituição um **agente ativo e informado** nos objetivos de cibersegurança; a ausência de consciencialização e de literacia digital em cibersegurança traduzem-se em vulnerabilidades críticas em várias organizações.

- Dispor dos **meios tecnológicos** o mais avançados e adequados possível, no sentido de diminuir a disparidade de recursos técnicos entre atacantes e atacados.

Desafios

ORGANIZAÇÃO E REGULAÇÃO

- Encontrar os **modelos, estruturas e processos organizativos e de gestão de risco** que melhor respondam aos desafios de cibersegurança.
- Criar uma **cultura** interna adequada às necessidades de Cibersegurança.
- Responder da melhor forma ao cenário de constante evolução e **complexidade das ameaças.**
- Interligações e dependências de **terceiras partes**, nomeadamente de prestadores de serviços digitais, pode baixar o risco tecnológico das instituições a nível individual, mas contribuir para um risco sistémico elevado.
- Encontrar e promover **enquadramentos regulatórios e de supervisão** que melhor respondem às necessidades do setor financeiro, em matéria de cibersegurança, eliminando lacunas existentes.

Soluções

RECURSOS – HUMANOS E TECNOLÓGICOS

- Aposta forte em recrutar e manter profissionais especializados em cibersegurança, que suportem as várias funções críticas associadas dentro da instituição.
- Trabalhar com as instituições académicas, apoiando-as e promovendo a formação de profissionais especializados em cibersegurança, face às necessidades e procura crescentes que se verificam nesta área.
- Realização de ações internas de formação e sensibilização em cibersegurança, de forma contínua e incluindo a generalidade dos colaboradores, especialmente os que ocupam funções chave dentro da organização e os que mais interagem com sistemas de informação.
- Investir fortemente em tecnologia, com a implementação de controlos de segurança tecnológicos e suporte à automatização de processos, como forma de diminuição do ciber-risco.

Soluções

ORGANIZAÇÃO E REGULAÇÃO

- Adoção dum quadro legal de cibersegurança, com integração de modelos de referência ao nível da organização de cibersegurança e gestão de risco (como a NIST, o COBIT ou ISO).
- Autonomia/independência da função de controlo interno de cibersegurança face ao departamento TI.
- Cooperação e partilha de conhecimento com entidades intra e extra setoriais.
- Desenvolvimento de planos de recuperação e continuidade de negócio e testes regulares aos mesmos.
- Integração de testes de segurança nos processos internos de desenvolvimento e manutenção.
- No caso das autoridades de supervisão, realizar uma supervisão efetiva e direcionada, com uma abordagem faseada e foco no risco.

Conclusões

- Fundamental uma aposta clara na formação e sensibilização de todos os colaboradores, especialmente aqueles com papéis chave na organização.
- Necessidade de uma estruturação organizacional que valorize o tema da cibersegurança e que promova a sua autonomia e independência.
- Importante existir uma definição adequada da gestão de risco de cibersegurança, suportada em modelos de referência internacionais; adoção e vinculação a modelos reconhecidos pela indústria.
- Deve existir uma intensificação da cooperação nacional e internacional (aposta na colaboração e partilha de informações com outras entidades, especialmente dos setores bancário e financeiro).
- A crescente dependência nas TI exigirá a adoção dum quadro legal de cibersegurança. A ausência deste quadro poderá promover o surgimento de conflitos legais.

Propostas de ação

- Definir uma framework de referência em cibersegurança para os BCPLP, de acordo com as boas práticas e trabalhos realizados noutros fórum importantes, incluindo também framework de testes de intrusão.

- Adotar medidas internas de reorganização, que potenciem uma maior autonomia e independência das funções de cibersegurança, assim como o reforço dos recursos materiais e humanos associados (em número e competências).

- Estabelecer protocolos de colaboração, incluindo partilha de informação e um programa de intercâmbio de técnicos entre BCPLP, com integração em ambiente laboral por determinados períodos, para uma melhor partilha de conhecimentos e experiências.

4 A prevenção do branqueamento de capitais e do financiamento do terrorismo

Acesso ao sistema financeiro - *FinTech*

De um modo geral, em todos os bancos centrais vigora o entendimento que a sujeição das *FinTech* à autorização (licenciamento) ou ao registo por um supervisor do sistema financeiro depende da subsunção da atividade a exercer por tais entidades a um dos tipos de atividade financeira sob a sua supervisão - BCB, BCV, BdP, BM, BNA, BCEAO.

No entanto, houve a revisão e atualização do quadro legal e regulamentar de modo a acomodar as novas tecnologias e novos modelos de negócio e assegurar uma efetiva supervisão, sem, contudo, prejudicar a inovação tecnológica. Exemplo: Regime das Sociedades de Crédito Direto e das Sociedades de Empréstimo entre Pessoas (Brasil); Os novos Regimes Jurídicos de Serviços de Pagamento e Moeda Eletrónica/ Instituições de Pagamento e Moeda Eletrónica (já existentes em praticamente todos os países de língua oficial portuguesa).

Para além de condições de acesso para novas instituições, soluções *FinTech* podem ser desenvolvidas pelas instituições incumbentes, caso em que a avaliação dos riscos deve ser efetuada, num primeiro momento pela instituição, e posteriormente acompanhada pelo supervisor.

Supervisão

Sendo a entidade sujeita ao licenciamento ou ao registo, ficará adstrita à apreciação pelo supervisor da adequação e suficiência dos mecanismos de controlo interno estabelecidos para dar cumprimento ao quadro normativo AML/CFT e para gerir o risco BC/FT a que a entidade venha a estar exposta, assim como os participantes qualificados (acionistas) e os membros dos órgãos de administração e fiscalização estão sujeitos à verificação da sua adequação (*fit and proper*).

Os supervisores devem avaliar os sistemas de gestão de risco e controlo no momento de acesso à atividade, bem como durante a supervisão *ongoing*.

O acompanhamento e a compreensão de modelos de negócio inovadores criados por instituições autorizadas fazem parte da rotina de supervisão – BdP, BCB, BM.

Para a identificação e a avaliação dos riscos todos os supervisores concordam que os países devem incluir nas suas avaliações nacionais de risco análises relacionadas com o tema das *FinTechs*. No que tange a trabalhos já desenvolvidos, concorreram por exemplo, a avaliação supranacional de riscos (SNRA) da Comissão Europeia e as iniciativas do BM junto das instituições de crédito relativamente aos novos produtos.

Medidas preventivas do branqueamento capitais e do financiamento do terrorismo

- As *FinTech* autorizadas pelos supervisores do sistema financeiro são consideradas entidades sujeitas ao cumprimento dos deveres preventivos do branqueamento de capitais e do financiamento do terrorismo, bem como ao cumprimento do regime das medidas restritivas - "*same risks, same rules*."

- *Enquanto entidades sujeitas, as FinTech devem* ***definir e implementar as políticas, os procedimentos e os controlos*** *que se mostrem adequados a gerir eficazmente os riscos de BC/FT.*

- Se determinada entidade se propuser exercer atividade financeira, independentemente da tecnologia associada, terá de se adequar, consoante o seu objeto, à regulamentação vigente. Os sistemas de gestão de risco e controlos devem ser proporcionais à **natureza, complexidade e dimensão da atividade**.

Ativos Virtuais e prestadores de serviço em ativos virtuais

- Os ativos virtuais (*Bitcoin, Criptoativos*, etc.) são considerados produtos de elevado risco BC/FT.
- Devidos aos riscos associados (BC/FT e para os consumidores), foram emitidos comunicados alertando para os riscos decorrentes de operações de guarda e negociação desses ativos – BCB, BCV, BdP, BM, BCTL.
- Os serviços com moedas/ativos virtuais não constituem atividades reguladas ou supervisionadas *per si* pelos Bancos Centrais de língua oficial portuguesa.
- No Brasil, se algum criptoativo for considerado um valor mobiliário, pode ser necessária a observância de dispositivos da regulamentação da Comissão de Valores Mobiliários.
- Portugal irá transpor a 5AMLD, até 10 de janeiro de 2020, em virtude da transposição, alguns prestadores de serviços com moedas virtuais — os **prestadores de serviços de câmbio entre moedas virtuais e moedas fiduciárias** ("*exchangers*") e os **prestadores de serviços de custódia de carteiras** ("*custodian wallet providers*") passarão a ser entidades sujeitas ao cumprimento dos deveres preventivos BC/FT.

Uso da tecnologia para o cumprimento de normativos – *Regulatory Technology*

- O uso da tecnologia, nomeadamente ***RegTech, blockchain, data analytics tools*** pode facilitar a conformidade ABC/CFT, auxiliar no processo KYC, no monitoramento dos riscos e na identificação de operações suspeitas - o desenvolvimento e a aplicação eficientes de *RegTech* podem criar oportunidades para, por exemplo, automatizar relatórios regulatórios e requisitos de conformidade, além de facilitar uma cooperação mais setorial e jurisdicional para melhorar a conformidade (por exemplo, ABC/CFT).
- As *RegTech* não são diretamente reguladas pelos bancos centrais de língua oficial portuguesa.
- No entanto, o BdP, o BCB, o BM já têm em pauta a discussão sobre como a tecnologia poderá ser usada para melhorar os processos de conformidade.
- Por exemplo: o **BdP** , nas aplicações desenvolvidas *in house*, preocupa-se em (i) garantir que as entidades sujeitas à sua supervisão conhecem os riscos das soluções que adotam e têm implementadas medidas mitigadoras relativamente às mesmas; (ii) garantir um quadro regulatório dinâmico. No recurso ao *outsoucing* – garantir o cumprimento do normativo aplicável.
- No **BCB** - iniciativa RegTech - APS-Siscom do Banco Central.
- O **BM** poderá adequar os mecanismos e ferramentas de supervisão baseada no risco (por exemplo, o *Banking Supervision Application*) – *SupTech*.

Principais conclusões

i. Verificam-se níveis de maturidade diferentes nesta matéria, pelo que iniciativas de cooperação entre os diferentes BCPLP são fundamentais para reduzir os *gaps* existentes e discutir oportunidades;

ii. Identificar o mercado *FinTech* é um passo essencial para as outras etapas (avaliar e monitorizar eventuais riscos);

iii. O arcabouço normativo de quase todos os ordenamentos jurídicos dos países de língua oficial portuguesa cobre parte relevante dos modelos de negócio inovadores criados nos últimos anos, com destaque para serviços de pagamento e moeda eletrónica. Várias iniciativas legislativas foram levadas a cabo nos últimos anos de modo a garantir que tais realidades estejam sujeitas à supervisão e regulação de um supervisor do sistema financeiro. Exemplos: *Crowdfunding* e *P2P lending*;

iv. A maioria dos BCPLP tem adequado a sua estrutura interna, recrutando, alocando novos recursos e capacitando os seus colaboradores face às novas exigências do mercado. No entanto, em matéria específica de prevenção do BC/FT, tal adaptação ainda se encontra numa fase embrionária;

v. A discussão relativa ao uso da tecnologia, designadamente *RegTech*, *blockchain*, *data analytics tools* no caso específico de facilitar a conformidade ABC/CFT, de auxiliar no processo KYC, no monitoramento dos riscos e na identificação de operações suspeitas iniciou-se em Portugal, Brasil e Moçambique.

Recomendações

i. **Capacitar ou continuar a capacitar os recursos humanos** dos BCPLP, de modo a que possam identificar, avaliar e monitorar os riscos das novas tecnologias e modelos de negócio. Para outros, iniciar a identificação do seu mercado *FinTech*;

ii. **Alargar o âmbito da cooperação entre os BCPLP** para as matérias relacionadas com a transformação digital com impacto na regulação e supervisão do sistema financeiro, considerando as boas práticas, os avanços individuais alcançados, com vista à redução dos *gaps* identificados;

iii. **Rever o quadro legal/regulamentar em matéria de prevenção do BC/FT** de modo a incluir novas realidades:

   a. prestadores de serviços de câmbio entre moedas virtuais e moedas fiduciárias ("*exchangers*") e os prestadores de serviços de custódia de carteiras ("*custodian wallet providers*");

   b. plataformas de financiamento entre pessoas (P2P *lending)*, como no Brasil; e

   c. outros

iv. **Colocar em prática iniciativas para melhorar a interação com os novos *players* de modo a fomentar a compreensão e mitigação dos riscos BC/FT;**

v. **Conhecer e monitorar o uso da tecnologia**, nomeadamente *RegTech, blockchain, data analytics tools* utilizadas pelas entidades sujeitas para auxiliar cumprimento dos deveres preventivos de BC/FT.

Ideias para reflexão

1. Como podem os Bancos Centrais, enquanto reguladores e **supervisores**, garantir que a inovação tecnológica promove melhores serviços financeiros, **mais inclusivos, integrantes e eficientes**, atuando de forma equitativa e isenta, em cumprimento da sua **missão** de proteção dos consumidores, das infraestruturas de mercado e da **estabilidade financeira**?

2. Como assegurar a **inclusão** e **proteção** do cliente dos serviços financeiros sem comprometer a estabilidade e integridade financeira em face da inovação tecnológica?

3. Há a consciência de que uma estratégia **sustentável** de desenvolvimento em tecnologias digitais implicará um correspondente investimento em **cibersegurança**, assente num quadro legal adequado, que pressuponha uma estruturação organizacional que valorize o tema e que promova a sua autonomia e **independência**?

4. Terão os supervisores **recursos** adequados para entender e **monitorar** o uso da tecnologia (*RegTech*, *blockchain*, *data analytics tools* e soluções de *SupTech*) em matéria de **prevenção** do BC/FT?

BANCO DE PORTUGAL
EUROSISTEMA

Obrigado.

Technology always has, and always will, spur innovation in finance.

The question is whether these innovations will benefit all, or only a few.

Opening Remarks by **Christine Lagarde,**
G20 High Level Seminar: "Our Future in the Digital Age", June 8 2019, Fukuoka-Japan