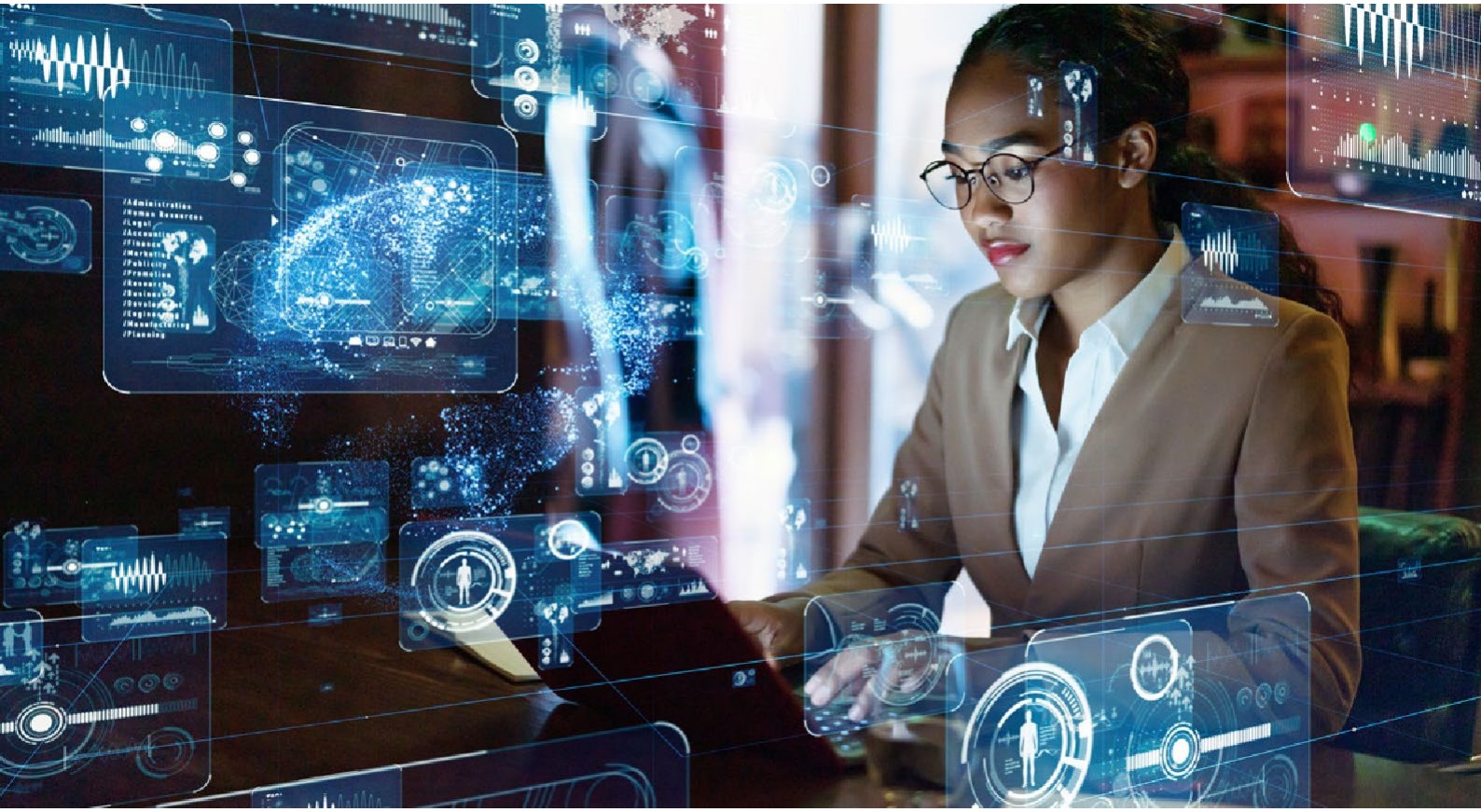
DIGITAL FINANCIAL SERVICES (DFS) WORKING GROUP

CONSUMER EMPOWERMENT AND MARKET CONDUCT (CEMC) WORKING GROUP

NOTA ORIENTADORA SOBRE PRIVACIDADE DE DADOS PARA SERVIÇOS FINANCEIROS DIGITAIS

Nota Orientadora nº 43 de
fevereiro de 2021



NOTA ORIENTADORA

ÍNDICE

CONFIRMAÇÕES

Esta Nota Orientadora é um produto conjunto dos membros do Grupo de Trabalho de Serviços Financeiros Digitais (GTSFD) e do Grupo de Trabalho de Empoderamento do Consumidor e Conduta de Mercado (PCGTCM).

Autores e contribuidores:
Os membros do GTSFD que contribuíram para a Nota Orientadora incluem:

Alejandro Medina (SBS Peru), Rushika Kumaraswamy (Banco Central do Sri Lanka), Mohamed Salem Ould Mamoun (Banco Central da Mauritânia), Rasool Roohy (Banco Da Afeganistão), Stephen Ambore (Banco Central da Nigéria), Anil Paul (Banco de Papua Nova Guiné), Khaled Barmawi (Banco Central da Jordânia), Rania Elshama (Banco Central do Egipto) e Pauline Moustache (Banco Central das Seicheles).

Da unidade de gestão da AFI, o projeto para desenvolver a Nota Orientadora foi liderado por Ali Ghiyazuddin Mohammad (Gestor Sénior de Políticas, Serviços Financeiros Digitais) e apoiado por Eliki Boletawa (Chefe de Programas Políticos e Iniciativas Regionais). Gostaríamos de agradecer à consultora Ros Grady pelo seu apoio na investigação e desenvolvimento relevantes da Nota Orientadora.

Gostaríamos de agradecer às instituições membros da AFI, parceiros e doadores por contribuírem generosamente para o desenvolvimento desta publicação.

Conceito de privacidade de dados. (Foto de metamorworks/Shutterstock)

RESUMO

Esta Nota Orientadora foi desenvolvida pelo Grupo de Trabalho de Serviços Financeiros Digitais (GTSFD) da AFI e pelo Grupo de Trabalho de Empoderamento do Consumidor e Conduta de Mercado (PCGTCM).

O mercado de serviços financeiros digitais (SFD) está a ser transformado a um ritmo exponencialmente rápido, impulsionado pelos desenvolvimentos de processamento de dados possibilitados pela FinTech. Estas mudanças levaram a inovações na conceção e fornecimento de produtos de SFD, que por sua vez ajudam a alcançar os objetivos de inclusão financeira e os seus benefícios de redução da pobreza e de crescimento económico.

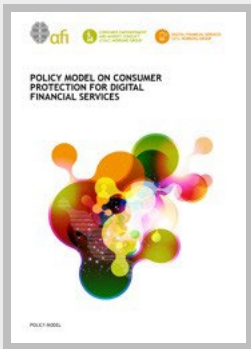
Por outro lado, estas inovações levantam questões significativas de privacidade de dados para os titulares dos dados - privacidade de dados para serviços financeiros digitais (PDSFD). Particularmente preocupantes são os prováveis desafios tecnológicos e de capacidade financeira dos titulares dos dados num contexto de inclusão financeira.

O objetivo da Nota Orientadora é fornecer orientação não vinculativa para um framework político e regulamentar abrangente, proporcional e baseado no risco para a PDSFD. O foco está nas questões de privacidade aplicáveis aos SFDs, em vez dos serviços financeiros tradicionais. Isso ocorre porque a maioria dos problemas de privacidade surge no contexto dos SFDs. Contudo, a Nota Orientadora também pode ser relevante de forma mais ampla.

A Nota Orientadora baseia-se em produtos de conhecimento anteriores da AFI, que abrangem questões de privacidade e proteção de dados. Ver especialmente os princípios orientadores relativos à privacidade e proteção de dados no Modelo de Política da AFI sobre Proteção do Consumidor para Serviços Financeiros Digitais (2020) (Princípio 2.1) e no Framework de Política da AFI para Crédito Digital Responsável (2020) (Princípio 6).
Outros Produtos de Conhecimento AFI relevantes são mencionados em outras partes da Nota Orientadora e todos estão listados no Anexo 5.

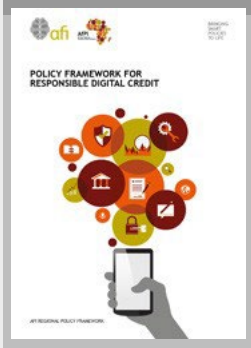
Uma ampla gama de orientações políticas e regulamentares aplicáveis à PDSFD foi sintetizada para efeitos da Nota Orientadora. Além dos produtos de conhecimento da AFI mencionados acima, as fontes consideradas incluem uma secção transversal diversificada de frameworks regulamentares nacionais e normas, diretrizes e boas práticas internacionais. Pesquisas e
e comentários relacionados de organizações internacionais, académicos e especialistas também foram considerados.

LEITURA ADICIONAL



Modelo de Política AFI sobre Proteção ao Consumidor para Serviços Financeiros Digitais (2020) (Princípio 2.1)

> Veja aqui



Framework de Política AFI para Crédito Digital Responsável (2020) (Princípio 6)

> Veja aqui

O resultado deste trabalho foi o desenvolvimento dos seguintes Princípios Orientadores. As principais recomendações para cada Princípio Orientador estão incluídas posteriormente nesta Nota Orientadora.

PILAR 1: FRAMEWORK POLÍTICO E REGULATÓRIO DA PDSFD

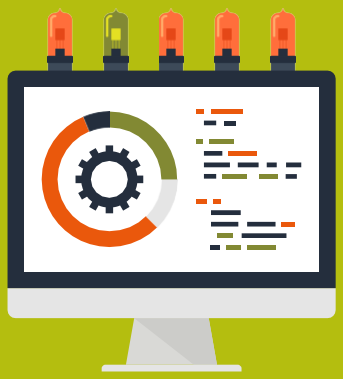
- **1.1** Princípio orientador: estabelecer acordos de governança e consulta
- **1.2** Princípio orientador: avaliar o atual framework jurídico e regulamentar dos SFDs e o mercado
- **1.3** Princípio orientador: estabelecer políticas abrangentes e princípios regulatórios
- **1.4** Princípio orientador: desenvolver o framework jurídico da PDSFD

PILAR 2: OBRIGAÇÕES DO RESPONSÁVEL PELO TRATAMENTO DE DADOS E DO PROCESSADOR DE DADOS

- **2.1** Princípio orientador: exigir arranjos eficazes de governança interna da PDSFD
- **2.2** Princípio orientador: estabelecer princípios abrangentes de processamento de dados
- **2.3** Princípio orientador: criar modelo para consentimento informado e eficaz
- **2.4** Princípio orientador: exigir um responsável pela proteção de dados quando apropriado

SEIS PILARES DE PRINCÍPIOS ORIENTADORES PARA UM FRAMEWORK DA PDSFD

PILAR 1: FRAMEWORK POLÍTICO E REGULATÓRIO DO DP4DFS



PILAR 2: OBRIGAÇÕES DO RESPONSÁVEL PELO TRATAMENTO DE DADOS E PROCESSADOR DE DADOS DE DADOS

PILAR 3: DIREITOS DO TITULAR DOS DADOS

PILAR 4: CONSCIENCIALIZAÇÃO E RECURSOS DO CONSUMIDOR

PILAR 5: SUPERVISÃO E APLICAÇÃO EFETIVA

PILAR 6: PDSFD EM EMERGÊNCIAS GLOBAIS E NACIONAIS

Uma "Abordagem Minimalista da PDSFD para Reguladores do Setor Financeiro" de uma página também foi incluída nesta Nota Orientadora. Esta proposta contém sugestões sobre as ações mínimas que os reguladores do setor financeiro poderão tomar no período intermédio antes de existir uma lei abrangente de proteção de dados em vigor.

Em resumo, o organismo principal desta Nota Orientadora está organizado da seguinte forma:

ESCOPO, CONCEITOS CHAVE E DEFINIÇÕES

Os Princípios Orientadores abrangem questões de "privacidade de dados" que afetam informações pessoais, mas não questões específicas de "proteção de dados".

Estes termos são definidos da seguinte forma para efeitos desta Nota Orientadora: 'privacidade de dados' é considerada como a utilização e gestão adequadas de dados pessoais tendo em conta os direitos à privacidade e 'proteção de dados', como proteção dos dados contra utilização não autorizada. Estas são as definições utilizadas no Modelo de Política da AFI sobre Proteção ao Consumidor para Serviços Financeiros Digitais (2020). Nesta base, questões como a fraude cibernética, os sistemas de segurança e as regras de localização de dados são consideradas no domínio da «proteção de dados». Algumas questões relevantes para a área "cinzenta" que se sobrepõe à privacidade e à proteção de dados foram, no entanto, abordadas (como a fraude e a utilização indevida de identidade).

Para completar, note-se também que o direito à privacidade é geralmente considerado como "o direito de ser deixado em paz", embora sujeito a algumas limitações. [1] No entanto, considera-se que está fora do âmbito desta Nota Orientadora discutir a natureza do direito à "privacidade" ou se qualquer direito ou outro direito à privacidade pode existir em qualquer jurisdição. [2]

Os Princípios Orientadores são relevantes para produtos de SFD de varejo e modelos de negócios relacionados, comuns em economias emergentes de tempos em tempos (agora e no futuro). Isto poderia incluir, por exemplo, poupança, crédito digital, empréstimos P2P, dinheiro eletrónico, remessas, microsseguros, financiamento coletivo e produtos de investimento, bem como produtos e serviços mais inovadores, como agregação de contas e outros serviços de open banking.

Outras questões importantes refletidas nos Princípios Orientadores são:

> **Inclusão financeira:** os Princípios Orientadores baseiam-se no pressuposto de que devem ser relevantes para os consumidores em economias com objetivos ambiciosos de inclusão financeira.

1 Sameul D Warren e Louis D. Brandeis. O direito à privacidade. Revisão de Direito de Harvard, vol. 4, nº 5 (15 de dezembro de 1890), pp. 193-220

2 Para uma discussão destas questões no contexto da Índia, ver a importante decisão do Supremo Tribunal da Índia no caso da justice KS Puttaswamy vs. União da Índia (2017) 10 SCC 1 que, em resumo, considerou a privacidade um direito protegido pelo Constituição da Índia.

- **FinTech:** os Princípios Orientadores foram desenvolvidos considerando os desenvolvimentos da FinTech que são relevantes para os SFDs, incluindo prestadores novos e inovadores, modelos de negócios, sistemas de processamento e aplicações. Os Princípios Orientadores também pretendem ser "neutros em termos de tecnologia", no sentido de que devem ser relevantes independentemente da tecnologia utilizada para conceber, comercializar ou fornecer SFD.
- **Grupos vulneráveis:** as questões de privacidade de dados relevantes para grupos vulneráveis estão refletidas nos Princípios Orientadores. Esses grupos incluem, por exemplo, mulheres, jovens, idosos, pessoas com deficiência e pessoas deslocadas.
- **Emergências e PDSFD:** existem benefícios indubitáveis na utilização generalizada de SFD para responder a emergências globais e nacionais (como a COVID-19, a crise do Ébola, a crise da Síria e desastres naturais). No entanto, também existem desafios de privacidade de dados. Neste contexto, foi incluído um Pilar específico sobre PDSFD em Emergências Globais e Nacionais.

Os principais termos utilizados nesta Nota Orientadora (incluindo os Princípios Orientadores) devem ter os significados constantes do Anexo 3. Estes significados foram desenvolvidos tendo em conta os termos mais utilizados e as definições relacionadas em frameworks regulamentares, pesquisas e comentários. Para facilitar a referência, as definições mais significativas são apresentadas na Tabela 1 abaixo.

É, no entanto, sublinhado que podem ser adotadas diferentes abordagens para os termos e definições relevantes, e as propostas não se destinam a ser obrigatórias.

CAIXA 1: DEFINIÇÕES DE 'DADOS PESSOAIS' OU SEMELHANTES NAS LEIS DE PRIVACIDADE E PROTEÇÃO DE DADOS

Regulamento Geral de Proteção de Dados da UE: 'dados pessoais' significa qualquer informação relativa a uma pessoa singular identificada ou identificável ('titular dos dados');
uma pessoa singular identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;' (secção 4).

Para outros exemplos de definições de 'dados pessoais' ou de um termo equivalente, consulte:

- Lei de Proteção de Dados do Quénia de 2019 (secção 2),
- Lei de Proteção de Dados da Malásia de 2010 (secção 4),
- Lei de Privacidade de Dados das Filipinas de 2012 (secção 3).

Ver também o projeto de lei de proteção de dados pessoais de 2019 da Índia (secção 3(28)), que inclui especificamente qualquer inferência extraída de dados pessoais para fins de perfilização.

TABELA 1: PRINCIPAIS CONCEITOS E

CONCEIT	DEFINIÇÕES
TITULAR DOS DADOS	Um indivíduo cujos dados pessoais são ou podem ser processados.
DADOS PESSOAIS	Qualquer informação ou opinião relativa a uma pessoa física identificada ou identificável, verdadeira ou não, mantida de forma material ou não, e automatizada ou não.
CONTROLADOR	Pessoa singular ou coletiva ou autoridade pública que, isoladamente ou em conjunto com outras, determina a finalidade ou o método de tratamento de dados pessoais.
PROCESSADOR	Pessoa física ou jurídica ou autoridade pública, que trata dados pessoais em nome do controlador.
EM PROCESSAMENTO	Qualquer operação realizada em relação a dados pessoais, seja manual ou automaticamente, incluindo recolha, utilização, divulgação, armazenamento, registo, apagamento ou de outra forma, e 'processos', 'processados' e palavras semelhantes que tenham um significado semelhante, mas que excluem qualquer processamento: - exigido para fins de atividades específicas (como função judicial, aplicação efetiva de uma reivindicação, segurança nacional ou finalidade puramente doméstica); ou - realizado para um propósito exigido ou permitido por lei

ANTECEDENTE S E CONTEXTO

NOVAS FORMAS DE PROCESSAMENTO DE DADOS, FINTECHS E PDSFD

O fenómeno do "Big Data" e as tecnologias relacionadas estão a alimentar inovações e oportunidades de SFD, inclusive nos países em desenvolvimento.

'Big Data' para efeitos desta Nota Orientadora podem ser considerados conjuntos de dados massivos e complexos que são caracterizados por enormes volumes de formas tradicionais e alternativas de dados pessoais estruturados ou não estruturados, com enorme variedade que podem ser processados em grande velocidade para fins de SFD.

As categorias de dados que podem ser tratadas incluem: tanto as formas tradicionais de dados de clientes, contas e transações, como formas alternativas de dados, como dados de redes sociais, dados derivados de telemóveis e dados disponíveis publicamente. O aumento da conectividade com a Internet e a adoção de smartphones também podem fornecer uma rica fonte de dados para processamento e aumentar a disponibilidade dos SFDs. [3] As tecnologias relevantes incluem algoritmos, que facilitam a aprendizagem automática, a computação em nuvem, a tecnologia blockchain, ferramentas de identificação biométrica e sistemas de identificação digital. [4] Finalmente, estas novas formas de processamento de dados podem ser utilizadas:

- Para reidentificar uma pessoa comparando dados anónimos (dados anonimizados) com dados publicamente disponíveis, informações já conhecidas ou outros dados; e
- Para inferir dados confidenciais a partir de dados não confidenciais (como utilizar o nome de uma pessoa para inferir sua raça, religião ou gênero). [5]

As entidades FinTech que dependem destes desenvolvimentos são diferentes dos prestadores de serviços financeiros tradicionais. Já não é o caso de os dados serem processados para fins de SFD por entidades altamente regulamentadas, como bancos tradicionais, seguradoras ou entidades de valores mobiliários, que estão sujeitas à conduta de mercado, bem como a regras prudenciais. Uma gama cada vez maior de entidades e modelos de negócios FinTech novos, inovadores, ágeis e muitas vezes sem fronteiras estão agora a tratar os dados, seja como o próprio prestador de serviços financeiros ou como um prestador de serviços subcontratado (como para fins de análise de dados).

BENEFÍCIOS DE NOVAS FORMAS DE TRATAMENTO DE DADOS

Os desenvolvimentos de processamento de dados descritos acima podem criar benefícios significativos para os titulares dos dados de SFD. Breves exemplos incluem:

- **Escolha de produtos:** É provável que os consumidores tenham maior acesso a uma ampla gama de serviços financeiros, incluindo produtos de nanocrédito para aqueles sem históricos formais de crédito; produtos de empréstimo ponto a ponto; produtos de pagamento, como dinheiro eletrónico; produtos de microsseguros; contas de poupança de baixo custo; e financiamento coletivo.
  Além disso, os serviços de open banking, como a agregação de contas, podem proporcionar aos titulares dos dados um maior controlo sobre os seus dados e benefícios relacionados na escolha e preços dos produtos, bem como na gestão dos seus assuntos financeiros.
- **Produtos personalizados:** as grandes quantidades de dados pessoais disponíveis aos prestadores de SFDs podem ser utilizadas para conceber e oferecer produtos específicos às necessidades e ao perfil de risco dos titulares dos dados e que podem ser precificados em conformidade.
- **Identificação mais fácil:** os sistemas de identificação digital desenvolvidos com base em novas fontes de dados, como dados biométricos e tecnologias de processamento melhoradas, podem facilitar o acesso seguro aos SFDs.
- **Ajuda de emergência:** a identificação dos beneficiários com direito a ajuda de emergência (tais como transferências de dinheiro do governo para pessoa (G2P) e crédito subsidiado) pode ser facilitada.

Os prestadores de SFDs provavelmente serão beneficiados por esses desenvolvimentos no processamento de dados. Eles podem melhorar a sua capacidade de conceber, comercializar e fixar preços de produtos e serviços financeiros específicos e de gerir riscos comerciais relacionados com dados (tais como riscos de crédito, riscos de avaliação de seguros e queixas e reclamações). Alguns prestadores também podem tentar vender direitos de acesso a terceiros. A realização destas vantagens potenciais estaria, obviamente, sujeita às leis aplicáveis.

Os desenvolvimentos no processamento de dados também apresentam uma série de benefícios potenciais a nível nacional. Em resumo, no contexto dos SFDs, isto poderia incluir assistência no alcance das metas de inclusão financeira; no desenvolvimento e gestão de sistemas nacionais de identificação; em encorajar concorrência e inovação no setor financeiro; e na gestão de riscos no setor financeiro.

3 GSMA: Relatório sobre o estado da conectividade à Internet móvel (2020)

4 Banco Mundial: Proteção do Consumidor Financeiro e Novas Formas de Processamento de Dados Além dos Relatórios de Crédito (2018)

5 UIT: Iniciativa Global de Inclusão Financeira (FIGI) Grupo de Trabalho de Infraestrutura e Confiança de Segurança, Big data, aprendizagem de máquina, proteção ao consumidor e privacidade (2018)

RISCOS COM NOVAS FORMAS DE TRATAMENTO DE DADOS

CAIXA 2: MODELO DE POLÍTICA AFI SOBRE PROTEÇÃO DO CONSUMIDOR PARA SERVIÇOS FINANCEIROS DIGITAIS (2020)

"Na era financeira digital, os dados estão no centro dos SFDs.

…

Neste contexto, a utilização, gestão e armazenamento inadequados dos dados dos clientes, juntamente com uma fraca divulgação e transparência, têm o potencial de excluir segmentos vulneráveis dos serviços financeiros, gerar falta de confiança nos SFDs e minar os ganhos na inclusão financeira" (Princípio Orientador 2.1: Salvaguarda da Privacidade e Proteção de Dados Pessoais).

Há uma vasta gama de riscos para os titulares dos dados de SFDs com estes desenvolvimentos, especialmente quando não existe um framework regulamentar de privacidade de dados em vigor.
A um nível elevado, estes riscos podem resultar em consequências prejudiciais, como a recusa de um SFD ou de um benefício governamental, perdas financeiras, danos à reputação social ou profissional ou tratamento injusto, como discriminação.
Mais especificamente, incluem os seguintes riscos significativos:

- **Os titulares dos dados podem ter nenhum controlo ou ter controlo limitado sobre seus dados pessoais**: nenhuma ou limitada informação pode ser fornecida ou disponível sobre quais tipos de dados estão a ser processados, por quem, como ou onde. Mesmo quando a informação está disponível, o consentimento não pode ser dado livremente ou informado.
- **Os dados sensíveis podem ser comprometidos através da recolha, utilização ou divulgação não autorizada:** Existem preocupações acrescidas com a privacidade dos dados que podem ser considerados especialmente sensíveis. Por exemplo, informações sobre dados biométricos, identificador oficial, crenças ou afiliações religiosas ou políticas de uma pessoa, raça, etnia, casta, saúde ou identidade sexual. Além disso, como observado acima, dados não sensíveis podem ser utilizados para inferir dados sensíveis. [6]
- **Dados pessoais incorretos, enganosos, incompletos ou desatualizados podem ser processados:** Isto pode levar a tratamento injusto, como a recusa injustificada de uma linha de crédito, o assédio ao devedor, a recusa injusta de um pedido de seguro ou a negação de benefícios governamentais, bem como a perdas financeiras e danos à reputação.
- **A tomada de decisão automatizada, incluindo a perfilização, pode levar a decisões injustas:** Decisões sobreum titular de dados, que são feitos com base no processamento automatizado e na perfilização sem qualquer intervenção humana, podem resultar em discriminação e preconceitos injustos. [7] Além disso, os titulares dos dados provavelmente não compreender algoritmos complexos e em constante evolução e outras tecnologias utilizados em tais processos. Uma complexidade adicional é que estas tecnologias podem ser consideradas comercialmente confidenciais e podem ser protegidas por direitos e obrigações de propriedade intelectual.
- **Pode ocorrer fraude na identificação e utilização indevido de IDs digitais:** Esses eventos podem resultar em perdas financeiras e danos à reputação dos titulares dos dados. Há também a complexidade adicional que comprometeu os dados de identidade biométrica não podem ser corrigidos, ao contrário de outras credenciais de segurança comprometidas (como uma senha ou número de identificação pessoal). Veja mais detalhes na secção intitulada 'IDs digitais e riscos de fraude de identidade, utilização indevido e acesso inadequado'.
- **Os direitos de recurso podem ser limitados:** Sem um framework regulamentar de privacidade de dados em vigor, o titular dos dados pode não ter recurso para qualquer utilização indevida dos seus dados. Isto pode incluir, por exemplo, um recurso que exija que o responsável pelo tratamento de dados interrompa ou altere o tratamento dos dados pessoais ou corrija ou apague quaisquer registos que possua ou pague uma compensação.
- **Os sistemas e procedimentos do responsável pelo tratamento de dados não garantem a privacidade:** Também pode haver o risco de os responsáveis pelo tratamento de dados não terem em vigor sistemas e procedimentos globais que reflitam proativamente as considerações de privacidade na conceção e comercialização dos SFDs.
  Dito de outra forma, as questões de privacidade não estão na "vanguarda". Isto pode ser mais provável com entidades FinTech novas e inovadoras, em comparação com prestadores de SFDs mais tradicionais.
- **Os riscos de privacidade com intermediários, como corretores de dados que comercializam Big Data e as análises relacionadas, estão a ser alvo de um escrutínio cada vez maior:** por exemplo, o Gabinete do Comissário de Informação do Reino Unido investigou recentemente três agências de referência de crédito que também operavam como corretores de dados. [8]

Os prestadores de SFDs também podem ser desafiados por novos desenvolvimentos no processamento de dados, mesmo sem obrigações de cumprir um framework regulamentar de privacidade de dados.

6 Projeto de lei de proteção de dados da Índia (2019) (Secção 3(36))

7 G20: Princípios de Alto Nível para Inclusão Financeira Digital (2016) (Princípio 5 refere-se como uma ação chave para apoiar os SFDs: 'Exigir que os dados não sejam utilizados de forma injusta e discriminatória para serviços financeiros digitais (por exemplo, para discriminar mulheres em relação ao acesso ao crédito ou ao seguro)».

8 https://ico.org.uk/about-the-ico/news-and-events/news-and- blogs/2020/10/ico-takes-enforcement-action-against-experian-after- data-broking-investigation/

Eles incluem: as complexidades e os custos envolvidos em manter-se atualizado com essas inovações e ajustar sistemas e processos existentes; as implicações comerciais do processamento de dados imprecisos ou irrelevantes; a necessidade resultante de métodos mais complexos de recolha e verificação de dados; os riscos e custos associados ao aumento da dependência de prestadores externos de dados e de análise de dados, e a necessidade de sensibilizar os clientes para a necessidade de salvaguardar os seus dados pessoais, identificações oficiais e credenciais de segurança.

Existem também desafios para os reguladores e decisores políticos do sector financeiro no contexto da PDSFD. Em termos gerais, incluem a possibilidade de os consumidores não confiarem na utilização dos SFDs devido a preocupações com a privacidade dos dados, com implicações para a inclusão financeira. Desafios mais específicos podem ser necessários para reguladores e formuladores de políticas:

- Compreender os modelos de negócios, parcerias, atividades e técnicas de processamento de dados de prestadores FinTech novos, ágeis e inovadores;
- Adquirir capacidade e recursos organizacionais e tecnológicos adequados;
- Para compreender quaisquer lacunas e sobreposições nas regras da PDSFD específicas do setor (por exemplo, nos setores bancário, de pagamentos, dinheiro eletrónico ou leis gerais de proteção ao consumidor); e
- Estabelecer acordos de consulta e coordenação com outras agências governamentais, o setor privado (incluindo prestadores tradicionais e de SFDs de FinTech) e stakeholders da sociedade civil (tais como grupos de consumidores).

PDSFD E GRUPOS VULNERÁVEIS

Os grupos vulneráveis precisam de ser considerados no desenvolvimento de um framework regulamentar e político da PDSFD. Tal como mencionado acima, o termo "grupos vulneráveis" abrange titulares de dados que são suscetíveis de ter necessidades especiais, incluindo mulheres, jovens, idosos, pessoas com deficiência e pessoas deslocadas. Questões de especial preocupação incluem:

- **Mulheres:** As normas culturais em algumas sociedades podem significar que as mulheres estão especialmente preocupadas com a privacidade dos seus dados de SFDs, inclusive no que diz respeito a outros os membros do agregado familiar (tais como os seus parceiros) e as suas comunidades estão preocupados.
- **Juventude:** É provável que os jovens tenham crescido familiarizados com as tecnologias possibilitadas pelas FinTech e com os SFDs, embora não seja claro se compreendem todos os riscos de privacidade relacionados.
- **Idosos:** Este grupo é especialmente suscetível de sofrer de capacidades financeiras e tecnológicas limitadas, o que pode, por sua vez, afetar desproporcionalmente a sua capacidade de compreender e exercer quaisquer direitos de privacidade de dados.
- **Pessoas com deficiência:** Existe uma ampla gama de deficiências, que podem ser relevantes para a leitura ou compreensão das divulgações de privacidade de dados e formas de consentimento. Eles incluem deficiências visuais e intelectuais, bem como limitações de linguagem. Este último ponto é especialmente provável em países que possuem múltiplas línguas oficiais e dialetos locais.
- **Pessoas deslocadas:** As questões de privacidade de dados para este grupo especialmente vulnerável podem incluir preocupações sobre quem tem acesso aos seus dados pessoais, incluindo registos biométricos criados por organizações de ajuda humanitária como o ACNUR (por exemplo, para facilitar a entrega de assistência em dinheiro através dos SFDs). Esta questão é amplamente discutida, inclusive pelo ACNUR, que possui a sua própria Política de Proteção de Dados.

Os fatores acima sugerem a necessidade de olhar para a gama diversificada de utilizadores de SFDs ao desenvolver uma política e framework regulamentar a PDSFD, e para desenvolver programas de alfabetização direcionados.

CAIXA 3: DISCURSO DO DIRETOR EXECUTIVO DA AFI DR. ALFRED HANNIG (18 DE NOVEMBRO DE 2020)

"A literacia digital desempenha um papel importante para que os utilizadores aprendam a navegar nestes serviços. Deve haver foco e proporcionalidade ao que os reguladores podem fazer na educação dos clientes financeiros, especialmente aqueles que não estão familiarizados com os riscos. Por exemplo, os idosos não estão habituados aos SFDs e ao internet banking e, devido à sua falta de conhecimento, enfrentam riscos de cair fora do sistema. Portanto, os reguladores precisam de olhar para a diversidade de grupos e riscos que enfrentam."

Os clientes de serviços financeiros de baixa renda demonstraram que se preocupam com a privacidade dos dados. Existem vários inquéritos e estudos que apoiam esta opinião, embora alguns indiquem que os clientes podem estar preparados para partilhar dados com empresas financeiras para obter benefícios adicionais. [9] Mais especificamente, experiências recentes da CGAP no Quénia e na Índia concluíram (em resumo) que a maioria dos clientes pobres participantes:

- Valorizam a privacidade dos dados e estão preparados para pagar por isso através de uma taxa ou taxa de juros mais elevada;
- Estávamos preparados para gastar tempo na obtenção de um empréstimo que oferecesse privacidade; e/ou
- Não estávamos dispostos a partilhar dados pessoais com terceiros. [10]

PDSFD E INCLUSÃO FINANCEIRA

Existe um compromisso entre a inclusão financeira e as regras de privacidade de dados? Pode-se, por exemplo, considerar que as regras de privacidade de dados inibem as inovações dos SFDs, como crédito digital e produtos de microsseguros, ou impõem restrições aos serviços de open banking ou à utilização de certas tecnologias, como os serviços de computação em nuvem. [11] A opinião contrária é que a privacidade dos dados e a inclusão financeira são objetivos compatíveis, uma vez que os direitos à privacidade dos dados são provavelmente
para construir confiança na utilização dos SFDs. Além disso, um regime proporcional de privacidade de dados pode fornecer uma base para inovações como instalações de open banking e digitalização económica, em geral. [12] Práticas de dados não regulamentadas também podem funcionar contra os objetivos fundamentais

CAIXA 4: DR. KATHERINE KEMP, PROFESSORA SÊNIOR, UNIVERSIDADE DE NOVA GALES DO SUL: FÓRUM DE FINANÇAS RESPONSÁVEIS 'BIG DATA, INCLUSÃO FINANCEIRA E PRIVACIDADE PARA OS POBRES' (2017)

"Deveria ser dada baixa prioridade à proteção dos dados dos consumidores à luz da necessidade mais premente de inclusão financeira?

…

Aqui, é importante lembrar como começámos: a inclusão financeira não é um fim em si mesma, mas um meio para outros fins, como permitir que os pobres e aqueles que vivem em áreas remotas possam sustentar as suas famílias,
prosperar, ganhar controlo sobre os seus destinos financeiros e sentir um sentimento de orgulho e pertença nas suas comunidades mais amplas. Os danos causados por práticas não regulamentadas de dados vão contra cada um desses objetivos."

PDSFD, COVID-19 E OUTRAS EMERGÊNCIAS

A COVID-19 e outras emergências globais e nacionais destacaram a necessidade de considerar as questões da PDSFD. A importância fundamental dos SFDs na preservação do funcionamento do sistema financeiro, melhorando a segurança e aliviando a pobreza durante emergências globais como a COVID-19 foi bem reconhecida, inclusive no Framework de Políticas da AFI para Alavancagem de Serviços Financeiros Digitais para responder a Emergências Globais – Caso de COVID-19 (2020). As razões incluem a capacidade de
SFDs para facilitar a entrega de transferências de dinheiro G2P de baixo custo, crédito de emergência e remessas locais e internacionais. os SFDs também permite que contas sejam operadas e pagamentos de bens e serviços sejam feitos de forma remota e sem contato.

No entanto, a explosão na utilização de SFDs durante crises como a da COVID-19 levanta desafios de privacidade de dados.
A escala das preocupações existentes com a privacidade dos dados provavelmente será exacerbada em caso de emergência. Isto porque os controlos habituais sobre as informações de identificação ou a privacidade dos dados de pagamentos podem ser dispensados ou ignorados numa emergência em benefício do sector privado e/ou agências governamentais. [13] Isso pode acontecer porque
da necessidade urgente de identificar indivíduos com direito ao auxílio emergencial. Outra consideração é a procura de extrema de receção de fundos, o que pode tornar ainda menos provável que os titulares dos dados leiam as divulgações de privacidade ou sejam capazes de fornecer consentimento efetivo.
Estas preocupações coexistem com outras questões de privacidade e proteção de dados (por exemplo, relacionadas com o aumento do risco de fraude cibernética, a necessidade de garantir a privacidade das informações de saúde e dos dados pessoais carregados em aplicações de localização relacionadas com a COVID-19).

9 OCDE: Utilização de dados pessoais em serviços financeiros e o papel da educação financeira: uma análise centrada no consumidor (2020) (secção 1.6)

10 CGAP: Nota de foco – A privacidade de dados é boa para os negócios? (2019) e CGAP: Blog - Preocupações com privacidade de dados influenciam comportamentos financeiros na Índia, Quénia

11 Centro de Toronto: Computação em Nuvem: Questões para Supervisores (2020)

12 Comitê de Supervisão Bancária do BIS Basel: Relatório sobre Open Banking e Interfaces de Programação de Aplicativos (2019) (Resumo Executivo e secção 6)

13 FMI: Série Especial sobre COVID-19 - Serviços Financeiros Digitais e a Pandemia: Oportunidades e Riscos para Economias Emergentes e em Desenvolvimento (2020)

TENDÊNCIAS EMERGENTES NA POLÍTICA DA PDSFD E REGULATÓRIO

LEIS GERAIS DE PRIVACIDADE DE DADOS

Há uma tendência crescente para estabelecer frameworks regulamentares de privacidade de dados, que refletem a importância dos desenvolvimentos de processamento de dados acima mencionados.

A base de dados da UNCTAD sobre Legislação Mundial sobre Proteção de Dados e Privacidade indica que 66 por cento dos países possuem tal legislação, com outros 10 por cento tendo projetos de legislação. As Leis de Proteção de Dados do Mundo da DLA Piper também fornecem uma visão geral das leis de privacidade e proteção de dados em 116 jurisdições.

O exemplo mais conhecido de um framework regulamentar de proteção de dados de utilização geral é provavelmente o Regulamento Geral de Proteção de Dados (RGPD) da UE, [14] **mas existem outros exemplos importantes.** Muitos emergentes,
assim como as economias desenvolvidas, promulgaram leis abrangentes sobre privacidade e proteção de dados nos últimos anos. Exemplos de membros da AFI com tais leis incluem Gana, Malásia, Quénia, México, Peru, Filipinas e África do Sul. A Índia também tem um projeto avançado de tal lei e o Governo do Ruanda também aprovou recentemente um projeto de lei relativo à proteção de dados e privacidade. [15] Consulte o Anexo 2 para obter detalhes. Estas leis são de aplicação geral no sentido de que se aplicam a todas as formas de processamento de dados para qualquer finalidade, ou seja, não apenas a serviços financeiros. No entanto, refletem uma série de tendências emergentes relevantes para os SFDs, sendo as mais significativas discutidas abaixo.

UMA ABORDAGEM PROPORCIONAL BASEADA EM RISCO

É geralmente aceite que uma abordagem proporcional baseada no risco deve ser uma consideração fundamental na regulação de desenvolvimentos inovadores do mercado, incluindo aqueles relevantes para a PDSFD. Esta é a abordagem refletida nos Princípios Orientadores propostos. Conforme observado no Relatório Especial da AFI sobre a Criação de Ecossistemas Habilitadores: O Papel dos Reguladores (2020): 'para
regulamentar implementações inovadoras no mercado, muitos países membros da AFI, como o Quénia, a Tanzânia e as Filipinas, estão a implementar abordagens regulamentares proporcionais». [16] O conceito de "proporcionalidade" é definido no Modelo de Política da AFI sobre Proteção ao Consumidor para Serviços Financeiros Digitais (2020) como "garantir que as respostas regulamentares refletem o modelo de negócio, a dimensão, a importância sistémica, bem como a complexidade e a atividade transfronteiriça das entidades reguladas». [17]

Uma abordagem proporcional baseada no risco é especialmente importante no contexto da FinTech e da inclusão financeira, dado o desejo de não prejudicar a inovação ou a concorrência dos SFDs. Isto pode ocorrer com requisitos regulamentares excessivamente onerosos, especialmente para entidades FinTech de menor dimensão, com incentivos e recursos limitados para gerir os riscos de privacidade. Outra consideração importante é que os reguladores nos países em desenvolvimento podem não ter os recursos ou a capacidade técnica para supervisionar padrões de PDSFD complexos. O desafio
é garantir um equilíbrio entre estas considerações e os riscos da PDSFD, juntamente com a necessidade de incentivar a inclusão financeira e a confiança dos titulares dos dados.

Os reguladores precisariam de uma metodologia de avaliação de risco de privacidade de dados para uma abordagem da PDSFD baseada em risco.
Qualquer metodologia desse tipo precisaria levar em conta os fatores de risco comuns no processamento de dados pelos modelos de negócios dos SFDs, incluindo aqueles decorrentes de fontes de informação, sensibilidade da informação, casos de utilização e interconectividade de sistemas. AFI está a considerar a publicação um artigo sobre esta questão.

A fim de abordar a proporcionalidade, pode ser considerada a imposição de obrigações com base na importância das atividades de tratamento de dados. Fatores relevantes podem incluir, por exemplo:

- A natureza dos produtos ou modelo de negócios de SFDs;
- O volume e a sensibilidade dos dados processados;
- O número de titulares dos dados;
- Rotatividade do fiduciário de dados;
- O risco de danos decorrentes do processamento; e
- Novas tecnologias utilizadas.

14 https://gdpr.eu/

15 https://www.primature.gov.rw/index.php?id=131&tx_news_pi1%5Bnews%5D=933&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=7a012c144e6b2eb6d384a0bf1f153c26

16 https://www.afi-global.org/publications/3181/Creating-Enabling-FinTechFinTechFinTechFinTech-Ecosystems-The-Role-of-Regulators

17 https://www.afi-global.org/publications/3465/Policy-Model-on-Consumer-Protection-for-Digital-Financial-Services. Esta definição também aparece na Orientação Política do G20/OCDE: Abordagens de Proteção ao Consumidor Financeiro: Proteção ao Consumidor Financeiro na Era Digital (2018)

As obrigações precisas impostas a um 'controldor de dados significativo' dependerão provavelmente do contexto do país. Por exemplo, pode acontecer que apenas os responsáveis pelo tratamento de dados "significativos" tenham de ser registados; preparar uma avaliação do impacto na privacidade dos dados para atividades de processamento específicas; nomear um responsável pela proteção de dados ou preparar relatórios anuais de conformidade ou auditá-los. Exemplos estão na Lei de Proteção de Dados de 2019 do Quénia, bem como no projeto de Lei de Proteção de Dados Pessoais de 2019 da Índia.

Alternativamente, as obrigações podem ser formuladas em termos de medidas "razoáveis" ou de algum outro padrão moderador. A Lei de Proteção de Dados das Filipinas (2019), por exemplo, refere-se a direitos de acesso "razoáveis", pedidos de correção de dados "razoáveis" do titular dos dados e requisitos de segurança "razoáveis e apropriados". [18] Orientações adicionais quanto ao significado
O conceito de "razoável" é útil nesta abordagem, tal como através de regulamentos e orientações emitidas pela DPA.

Outra abordagem à proporcionalidade é isentar as "pequenas empresas" claramente definidas de qualquer obrigação de cumprir um framework regulamentar de privacidade de dados. A Austrália constitui atualmente um raro exemplo desta abordagem, com a sua isenção para a maioria das "pequenas empresas" (aquelas com um volume de negócios anual
de A$ 3 milhões ou menos).[19] No entanto, a isenção está sob revisão na Austrália.[20] A dificuldade desta abordagem é que ela não leva em consideração o impacto das atividades das pequenas empresas sobre a privacidade dos titulares dos dados. Uma "pequena" entidade FinTech, por exemplo, poderia ter muito poucos funcionários, mas utilizar ferramentas e técnicas avançadas e opacas de processamento de dados para processar enormes volumes de dados pessoais, incluindo dados sensíveis. Além disso, tal abordagem não cria condições de concorrência equitativas e aumenta o risco de arbitragem regulamentar.[21]

Para completar, quando os direitos de privacidade de dados são reconhecidos pela legislação local, qualquer limitação a esses direitos também deve ser proporcional aos riscos enfrentados pelo titular dos dados. Por exemplo, o tratamento de dados pessoais só deverá ser permitido na medida do necessário para os fins para os quais os dados foram recolhidos e tendo em conta qualquer consentimento fornecido.
Além disso, qualquer limitação aos direitos de privacidade de dados deve ser cuidadosamente justificada e devem ser exigidas salvaguardas proporcionais.[22]

CAIXA 5: REQUISITOS DE PROPORCIONALIDADE NA ÍNDIA

O Supremo Tribunal da Índia observou os seguintes 4 requisitos de 'proporcionalidade' ao considerar a Lei Aadhaar (Fornecimento Direcionado de Subsídios Financeiros e Outros Subsídios, Benefícios e Serviços) (2016) e as limitações ao direito constitucional da Índia à privacidade:

(a) Uma medida restritiva de um direito deve ter um objetivo legítimo (etapa do objetivo legítimo).
(b) Deve ser um meio adequado para promover este objetivo (fase de adequação ou ligação lógica).
(c) Não deve haver nenhuma alternativa menos restritiva, mas igualmente eficaz (fase de necessidade).
(d) A medida não deve ter um impacto desproporcional no titular do direito (fase de equilíbrio)

Fonte: Caso de justice KS Puttaswamy vs. União da Índia (Julgamento de 26 de setembro de 2018)

FATORES DE MITIGAÇÃO DE RISCO DE PDSFD

As leis de privacidade de dados analisadas para efeitos desta Nota Orientadora contêm fatores de mitigação para os riscos de privacidade de dados. A Tabela 2 abaixo resume os mais comuns
desses atenuantes por referência aos riscos de privacidade descritos acima. É provável que os fatores de mitigação variem entre países, sejam mais detalhados na prática e possam estar sujeitos a qualificações e exceções.

A seguir à tabela há explicações adicionais sobre os fatores de mitigação mais importantes e conceitos relacionados, incluindo uma discussão de questões específicas de proporcionalidade.

Está também a ser dada clareza quanto ao procedimento de exercício dos direitos dos titulares dos dados. Esta é uma questão importante, dadas as complexidades do ambiente FinTech e a necessidade de os titulares dos dados estarem cientes de como podem exercer os seus direitos. Por exemplo, os regulamentos elaborados ao abrigo da Lei do México sobre a Proteção de Dados Privados detidos por Partes Privadas (2012) contêm disposições extensas sobre os procedimentos para o exercício de direitos
de acesso, retificação, cancelamento e direitos de objeção (ACRO) (Capítulo VII).

18 Filipinas: Lei de Proteção de Dados (2019) (seções 16 e 20)
19 Office of the Australian Information Commissioner: Small Business (acessado em 14 de dezembro de 2020) e definições relacionadas na Austrália: Privacy Act 1988 (Divisão 1 da Parte 1)
20 Austrália: Procurador-Geral: Documento sobre questões de revisão da Lei de Privacidade (2020)
21 Ver Princípios de Alto Nível do G20 para Inclusão Financeira Digital (2016) (Princípio 3)
22 Autoridade Europeia para a Proteção de Dados: Guia rápido da EDPS sobre a necessidade e a proporcionalidade (2020).

TABELA 2: RISCOS E FATORES DE MITIGAÇÃO DA PDSFD

RISCOS DE PRIVACIDADE DE DADOS RESPONSÁVEL PELO TRATAMENTO DE DADOS DADOS	FATORES DE MITIGAÇÃO – OBRIGAÇÕES DO	FATORES DE MITIGAÇÃO – DIREITOS DO TITULAR DOS
SEM CONTROLO SOBRE O PROCESSAMENTO DE DADOS PESSOAIS	**Tratamento legal:** o tratamento deve ser 'lícito', o que normalmente significa que existe consentimento do titular dos dados ou que o tratamento é necessário para efeitos de um contrato, de um requisito legal ou para proteger os interesses vitais do titular dos dados ou os do responsável pelo tratamento de dados . **Informações transparentes:** devem ser fornecidas informações ao titular dos dados sobre a recolha de dados pessoais e abranger questões como: as finalidades e fontes de recolha; os tipos de informação a serem recolhidas; a quem podem ser divulgadas; dados de controlador de contato do responsável pelo tratamento de dados ; e os direitos do titular dos dados. Além disso, todas as informações devem ser expressas de forma clara e simples e numa linguagem que o titular dos dados possa compreender. **Pedidos de consentimento:** os pedidos de consentimento devem ser apresentados separadamente de outras informações, ser específicos e ser dados e informados livremente. **Requisito de justiça:** os processadores de dados são obrigados a tratar os titulares dos dados de forma justa. Este conceito normalmente não é definido e pode exigir orientação regulatória. **Limitação da finalidade:** os dados pessoais só podem ser processados para a finalidade principal/específica de recolha, a menos que se aplique uma exceção (como o consentimento). Esta atenuante pode ser uma variação da atenuante da "licitude". **Minimização de dados:** os dados tratados devem ser adequados e relevantes e limitados ao mínimo necessário para as finalidades do tratamento.	**Direito à informação:** o titular dos dados tem direito a informação clara e simples sobre as atividades de tratamento e as entidades envolvidas. **Direito ao apagamento/a ser esquecido:** o titular dos dados tem o direito de solicitar o apagamento dos seus dados pessoais depois de estes já não serem necessários para a finalidade para que foram tratados. **Direito de restringir o processamento:** o titular dos dados pode solicitar a restrição do processamento em determinadas circunstâncias, como quando a exatidão é contestada ou o tratamento é ilícito. **Direito à portabilidade:** o titular dos dados pode solicitar que os dados pessoais, que foram tratados automaticamente, lhe sejam fornecidos num formato estruturado, de utilização corrente e legível por máquina. **Direito de retirar o consentimento:** o titular dos dados pode retirar o consentimento a qualquer momento.
DADOS SENSÍVEIS PODEM ESTAR COMPROMETIDOS	**Consentimento expresso**: exigir que o consentimento prévio e expresso seja obtido para o processamento de informações "sensíveis". Consulte o Anexo 3 para uma definição sugerida deste conceito.	
DADOS PESSOAIS INCORRETOS, ENGANOSOS, INCOMPLETOS OU DESATUALIZADOS PODEM SER PROCESSADOS	**Qualidade dos dados:** o responsável pelo tratamento de dados é obrigado a tomar pelo menos medidas razoáveis para garantir que os dados processados sejam precisos e atualizados. **Prazo de conservação:** os dados pessoais só podem ser conservados pelo período necessário à satisfação da finalidade do processamento.	**Direito à correção:** o titular dos dados tem o direito de solicitar a correção dos seus dados. **Direito de acesso:** o titular dos dados tem direito a ter acesso às suas informações, mediante pedido, e aos detalhes de quaisquer atividades de processamento e de quem as realizou.
TOMADA DE DECISÃO AUTOMATIZADA, INCLUINDO A PERFILIZAÇÃO PODE LEVAR A DECISÕES INJUSTAS	**Informações sobre processamento automatizado:** Exigir que o titular dos dados receba informações significativas sobre qualquer processo de tomada de decisão automatizada (incluindo a perfilização) e suas possíveis consequências, no momento em que os dados pessoais são recolhidos.	**Direito de oposição:** o titular dos dados tem o direito de se opor à tomada de decisões baseadas exclusivamente no processamento automatizado de seus dados pessoais.

TABELA 2: *CONTINUAÇÃO*

RISCOS DE PRIVACIDADE DE DADOS RESPONSÁVEL PELO TRATAMENTO DE DADOS DADOS	FATORES DE MITIGAÇÃO – OBRIGAÇÕES DO	FATORES DE MITIGAÇÃO – DIREITOS DO TITULAR DOS
IDENTIFICAR FRAUDE E UTILIZAÇÃO INDEVIDA DE IDENTIFICAÇÕES OFICIAIS PODEM OCORRER	**Trate as informações de identidade como uma categoria de "informações confidenciais":** essas informações devem exigir consentimento expresso para processamento. É provável que existam outros fatores de mitigação nas leis que estabelecem sistemas nacionais de identificação e, de um modo mais geral, nos requisitos de segurança aplicáveis aos sistemas de tratamento de dados pessoais e nas leis penais.	**Consciencialização do consumidor:** exigir que os titulares dos dados sejam informados sobre a melhor forma de proteger suas informações de identidade, incluindo suas credenciais de segurança.
OS DIREITOS DE RECURSO PODEM SER LIMITADOS.	**Responsabilidade:** responsabilizar o responsável pelo tratamento de dados por suas próprias ações e pelas de qualquer processador que atue em seu nome. **Sistemas de reclamações:** exigir que os responsáveis pelo tratamento de dados tenham sistemas transparentes, eficazes e gratuitos para processar reclamações sobre utilização indevida de dados pessoais. **Recursos:** garantir que exista um esquema de Resolução de Disputas Externas (EDR) para mediar sobre disputas entre um titular de dados e um responsável pelo tratamento de dados e emitir ordens apropriadas (por exemplo, quanto a compensação ou correção de dados). O esquema EDR é normalmente fornecido pela DPA relevante. **Limites às transferências transfronteiriças de dados:** exigir que as transferências transfronteiriças de dados sejam feitas apenas para jurisdições que tenham proteções de privacidade equivalentes às da jurisdição do cessionário e/ou que existam salvaguardas contratuais adequadas. Também pode haver regras de localização de dados em vigor. **Registo de responsáveis pelo tratamento de dados :** também pode haver requisitos para que os responsáveis pelo tratamento de dados sejam registados pela DPA relevante. Esta obrigação só pode aplicar-se aos responsáveis pelo tratamento de dados significativos.	**Conhecimento dos sistemas de processamento de reclamações e do esquema EDR:** os titulares dos dados devem ser informados sobre os seus direitos e sobre as vias de reclamação e recurso relevantes pelo responsável pelo tratamento de dados quando os dados são fornecidos e ao apresentar uma reclamação.
PROCEDIMENTOS E SISTEMAS DE CONTROLADORES E PROCEDIMENTOS NÃO GARANTEM A PRIVACIDADE DOS DADOS.	**Arranjos de governança:** exigir que os responsáveis pelo tratamento de dados de dados tenham políticas e procedimentos detalhados concebidos para garantir a conformidade com os princípios e regras relevantes de privacidade de dados, juntamente com os recursos tecnológicos e organizacionais relacionados. **Avaliações de Impacto na Privacidade (AIPs):** Exigir que as operações de processamento de alto risco sejam objeto de AIPs proativas, que cubram questões como as atividades de processamento propostas e os riscos e fatores de mitigação de privacidade relacionados. **Publicidade:** exigir que as políticas de privacidade e AIPs sejam tornadas públicas (por exemplo, no site do processador de dados). **Responsáveis pela proteção de dados:** Exigem que os responsáveis pelo tratamento de dados nomeiem um DPD com funções, como supervisionar a conformidade com quaisquer regras de privacidade de dados e ser um ponto de contato para os titulares dos dados e qualquer DPA. Esta obrigação só pode aplicar-se aos responsáveis pelo tratamento de dados significativos.	

Alguns dos fatores de mitigação acima podem ser controversos. Existem opiniões divergentes quanto à eficácia ou adequação de alguns dos fatores de mitigação, bem como preocupações quanto à existência de um equilíbrio adequado entre os riscos relevantes e os fatores mitigação.

Exemplos destas controvérsias incluem a aparente tensão entre as regras de minimização de dados e a era dos grandes volumes de dados e da aprendizagem automática [23] e o debate sobre se o direito a ser esquecido é realista dada a tecnologia blockchain. [24]

TOMADA DE DECISÃO AUTOMATIZADA

Há um foco crescente nos riscos associados à tomada de decisão automatizada, incluindo preconceitos contra mulheres/outros segmentos vulneráveis e perfilização. Em resumo, a preocupação é que as decisões sobre um titular de dados tomadas com base no processamento automatizado e na perfilização, sem qualquer intervenção humana, possam resultar em discriminação e preconceitos injustos.

Outra preocupação é que os titulares dos dados provavelmente não compreenderão algoritmos complexos e em constante evolução utilizados em tais processos. [25] A caixa abaixo apresenta alguns exemplos de diferentes abordagens regulamentares a estes riscos.

CAIXA 6: TOMADA DE DECISÕES AUTOMATIZADA

Seguem-se exemplos de regras relativas à tomada de decisão automatizada, incluindo a perfilização (em resumo).

UE: Regulamento Geral de Proteção de Dados (2016) O titular dos dados tem o direito de não sujeitar-se a uma decisão baseada exclusivamente no processamento automatizado, incluindo a perfilização, que produza efeitos jurídicos ou que afete significativamente o titular dos dados (Artigo 22). Aplicam-se exceções quando o consentimento tiver sido dado ou a decisão for necessária para a celebração de um contrato ou a sua execução ou o tratamento tiver sido expressamente autorizado por lei com as devidas salvaguardas.

'Perfilização' significa, em resumo, o tratamento automatizado, que utiliza dados pessoais para avaliar aspetos pessoais de uma pessoa (por exemplo, para analisar ou prever o desempenho profissional ou a saúde, o desempenho económico, as preferências, os interesses, a fiabilidade, a localização ou os movimentos) (artigo 4).

Filipinas: Lei de Proteção de Dados Pessoais (2012)
O titular dos dados tem direito a informações sobre processos automatizados em que os dados possam ser a única base para uma decisão que afete o titular dos dados (secção 16)

CAIXA 6: *CONTINUAÇÃO*

Gana: Lei de Proteção de Dados (2012)
Um indivíduo pode exigir que um responsável pelo tratamento de dados garanta que as decisões que afetam significativamente o indivíduo não se baseiam apenas no processamento automatizado de dados. O responsável pelo tratamento de dados tem então 21 dias para informar sobre as medidas que tomará para cumprir. No entanto, existem exceções a estes requisitos, inclusive quando o tratamento diz respeito a uma decisão de celebrar um contrato (secção 41).

CONSENTIMENTO

Há uma ênfase crescente na necessidade de consentimentos justos e eficazes para o processamento de dados. Muitos dos produtos de conhecimento da AFI listados no Anexo 5 referem-se a esta questão. Por exemplo, o Modelo de Política AFI para Dinheiro Eletrónico 2019 defende a exigência de que os emitentes de dinheiro eletrónico obtenham consentimento informado para acesso a informações demográficas ou pessoais (Parte VI). Muitas leis também exigem o consentimento do titular dos dados para o processamento dos seus dados, a menos que se aplique uma exceção. As exceções comuns são o processamento exigido ou permitido por lei ou o processamento necessário para executar um contrato. Em termos gerais, há agora uma ênfase crescente na necessidade de:

- Consentimentos dados livremente, informados e inequívocos;
- Consentimento a ser dado para uma finalidade específica;
- Solicitações de consentimento separadas de outras informações;
- Consentimento que pode ser retirado; e
- Foi dado ao responsável pelo tratamento de dados ou processador de dados o ónus de provar o consentimento.

Veja os exemplos na Caixa 7 na próxima página.

No entanto, há um debate contínuo sobre se o modelo de consentimento está "quebrado". As preocupações surgiram porque o consentimento é a base por trás de muitos frameworks de privacidade de dados e existem preocupações fundamentais sobre se os titulares dos dados podem dar consentimento livre e informado.

23 UIT: Iniciativa Global de Inclusão Financeira (FIGI) Grupo de Trabalho de Infraestrutura e Confiança de Segurança, Big data, aprendizagem de máquina, proteção ao consumidor e privacidade (2018)

24 Finextra: Blog de Carlo RW de Meijer Economista e pesquisador da De Meijer Independent Financial Services Advisory (MIFSA): Blockchain versus RGPD e quem deve se ajustar mais (2018)

25 Blog de CIF: Dados para finanças inclusivas: cumprimento de promessa aos consumidores (2020)

CAIXA 7: EXEMPLOS DE REQUISITOS DE CONSENTIMENTO REFORÇADOS

UE: Regulamento Geral sobre a Proteção de Dados (2016) O processamento de dados pessoais só é lícito na medida em que o titular dos dados tenha dado o seu consentimento específico para a finalidade específica do processamento ou caso se aplique outra exceção (artigo 6).

O conceito de 'consentimento' é definido como: 'qualquer indicação dada livremente, específica, informada e inequívoca da vontade do titular dos dados, pela qual este, através de uma declaração ou de uma ação afirmativa clara, manifesta o seu acordo com o tratamento de dados pessoais que lhe diz respeito' (artigo 4(11).

Outras regras do RGPD no Artigo 7 exigem que a solicitação de consentimento seja:

- 'claramente distinguível' de outros assuntos;
- De forma inteligível e de fácil acesso; e
- Em linguagem clara e simples.

O titular dos dados também deve ter o direito de retirar o consentimento a qualquer momento e deve ser tão fácil retirar o consentimento como fornecê-lo.

Malásia: Lei de Proteção de Dados Pessoais e Código de Proteção de Dados Pessoais para o Setor Bancário e Financeiro (Código BFS)
A Lei estabelece como princípio geral que os titulares dos dados devem dar o seu consentimento para o tratamento de dados pessoais (com algumas exceções) (secção 6).
Embora o conceito de "consentimento" não esteja definido na Lei, o Código BFS obrigatório fornece exemplos de formas de consentimento para aceleração de um contrato (incluindo consentimento presumido, bem como assinaturas ou marcas indicando consentimento, consentimento opt-in e consentimento verbal). Também está previsto que os consentimentos sejam fornecidos por canais eletrónicos, incluindo SMS,
e-mail e sistemas de mensagens). Em todos os casos, o formulário de consentimento deve ser registado e mantido.

Peru: Lei de Proteção de Dados Pessoais (2011) e Regulamento da Lei (2013)
Um dos Princípios Orientadores da Lei é que o titular dos dados deve dar o seu consentimento para o tratamento dos seus dados pessoais (com exceções específicas).
O consentimento deve ser "prévio, informado, expresso e inequívoco" e pode ser revogado a qualquer momento (Artigos 5 e 13). O Regulamento de Proteção de Dados Pessoais do Peru contém regras detalhadas e exemplos sobre o significado deste conceito de consentimento e deixa claro que ele pode ser dado eletronicamente.

Filipinas: Lei de Privacidade de Dados de 2012 e Regras e Regulamentos de Implementação
É necessário consentimento para a recolha e processamento de informações pessoais (sujeito a exceções) (secção 12). O conceito de 'consentimento do titular dos dados' é definido como '... qualquer manifestação de vontade dada livremente, específica e informada, pela qual o titular dos dados concorda com a recolha e tratamento de informações pessoais sobre e/ou relacionadas com ele ou ela. O consentimento deve
ser comprovado por meios escritos, eletrónicos ou gravados. .....' (secção 3(b)). As regras e regulamentos de execução também preveem que os consentimentos sejam limitados no tempo e possam ser retirados (secção 19)

África do Sul: Lei de Proteção de Informações Pessoais de 2013
O processamento de informações pessoais requer consentimento (a menos que se aplique uma exceção) (secção 11). A parte responsável tem o ónus de provar o consentimento. O conceito de consentimento é definido como "qualquer expressão de vontade voluntária, específica e informada em termos da qual é dada permissão para o processamento de informações pessoais" (secção 1). Além disso, existe um requisito de que os consentimentos para marketing direto por comunicação eletrónica sejam num formato prescrito (secção 69, regulamento 6 e formulário 4).

Este é especialmente o caso num contexto de inclusão financeira, onde os titulares dos dados têm provavelmente baixos níveis de capacidade financeira. [26] As principais preocupações incluem:

- Formas de consentimento longas e complexas;
- Consentimentos que ficam "enterrados" em termos e condições extensos;
- Falta de escolha – o titular dos dados pode sentir que tem de consentir se quiser os SFDs;
- Consentimentos agrupados, que abrangem o processamento de dados para os SFDs e, por exemplo, marketing direto;
- Incapacidade de retirar um consentimento;
- Os consentimentos são endereçados a múltiplas entidades, por exemplo, o prestador de SFDs e os prestadores de serviços;
- Não poder reter formulários de consentimento para referência futura; e
- Consente estar em um idioma que o titular dos dados não entende.[27]

26 Banco Mundial: Proteção do Consumidor Financeiro e Novas Formas de Processamento de Dados Além dos Relatórios de Crédito (2018)

27 McDonald AM and Cranor LF The Cost of Reading Privacy Policies A Journal of Law and Policy for the Information Society, vol. 4, no. 3 (2008), 543-568 (2008). Este estudo descobriu que uma pessoa média levaria 244 horas por ano para ler as políticas de privacidade online!

Estão agora a ser consideradas alternativas ao consentimento. Por exemplo, o CGAP defendeu tanto uma abordagem de fins legítimos como uma abordagem fiduciária de dados como alternativas ao modelo de consentimento na sua recente publicação CGAP Making Data Work for the Poor (2020). Contudo, não é provável que a necessidade de consentimento desapareça totalmente, dada a probabilidade de que o consentimento seja sempre necessário em alguns casos – por exemplo, consentimento expresso para processar informações sensíveis e consentimento expresso para fins de marketing direto ou venda cruzada. Além disso, o consentimento é a base de novas abordagens aos sistemas de open banking.

Existem abordagens que podem ajudar a aliviar os defeitos acima mencionados com o modelo de consentimento. Exemplos incluem:

- Exigência de um princípio geral imperativo para processar dados de forma justa (ou conceito semelhante) [28];
- Tratar os dados financeiros como uma categoria especial de dados que requer consentimento expresso para o processamento[29];
- Apoiar os requisitos legais de consentimento descritos acima com regras detalhadas sobre o que é necessário para cada elemento do requisito de consentimento (por exemplo, quanto ao significado de "dado gratuitamente", "prévio", "expresso" e "informado" e como os formulários de consentimento podem ser apresentados e dado em ambiente digital);[30] e
- A utilização de terceiros para gerir o processo de consentimento em sistemas de open banking (ver Caixa 8).

IDENTIFICAÇÕES DIGITAIS E RISCOS DE FRAUDE DE IDENTIDADE, UTILIZAÇÃO INADEQUADA E ACESSO INAPROPRIADO

Existe um reconhecimento global das vantagens dos sistemas de identificação digital para os objetivos de desenvolvimento. Conforme observado no Banco Mundial: ID Digital e Proteção de Dados Desafio: Nota do Praticante (2019), podem incluir (em resumo):

- Facilitar o acesso a "direitos, serviços e oportunidades económicas que exigem prova de identidade" (como serviços de SFDs, incluindo crédito, pagamentos, poupanças, seguros e pensões);
- Fortalecimento da governação e da prestação de serviços (por exemplo, mitigação da fraude do sector público nos pagamentos G2P e facilitação concomitante das transferências monetárias G2P);
- Apoiar o setor privado no cumprimento dos requisitos de identidade, como as regras eKYC; e
- Viabilizar a economia digital (por exemplo, facilitação de transações fiáveis e criação de oportunidades de inovação).

CAIXA 8: CGAP: A NOVA ABORDAGEM DA ÍNDIA PARA A PARTILHA DE DADOS PESSOAIS (2020)

Consentimento e modelo agregador de contas da Índia

"A partilha de dados entre prestadores de serviços financeiros (PSF) pode permitir que os prestadores ofereçam de forma mais eficiente uma gama mais ampla de produtos financeiros mais adaptados às necessidades dos clientes, incluindo clientes de baixos rendimentos. No entanto, é importante garantir que os clientes compreendam e concordem com a forma como os seus dados estão a ser utilizados.

A solução da Índia para este desafio são os agregadores de contas (ACs). O Reserve Bank of India (RBI) criou ACs em 2018 para simplificar o processo de consentimento dos clientes. Na maioria dos regimes de open banking, os fornecedores de informações financeiras (FIPs) e os utilizadores de informações financeiras (FIUs) trocam dados diretamente. Este modelo direto de troca de dados – como entre um banco e um bureau de crédito – oferece aos clientes controlo e visibilidade limitados sobre quais dados estão a ser partilhados e para que fim. Os ACs foram concebidos para serem colocados entre FIPs e FIUs para facilitar a troca de dados de forma mais transparente. Apesar do nome, os ACs estão proibidos de ver, armazenar, analisar ou utilizados dados do cliente. Como intermediários imparciais e fiáveis, eles simplesmente gerir o consentimento e servem como canais através dos quais os dados fluem entre os PSFs. Quando um cliente dá consentimento a um fornecedor através do AC, o AC obtém as informações relevantes das contas financeiras do cliente e envia por canais seguros para a instituição solicitante."

- **Veja também:** Reserve Bank of India: Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions (2016)

Por outro lado, há reconhecimento dos riscos relacionados com a privacidade associados às identificações digitais. A escala destes riscos tem potencial para ser enorme, dada a dimensão dos conjuntos de dados e a centralização dos dados. [31] Estes riscos podem ser resumidos da seguinte forma:

- A fraude de identidade é uma preocupação particular com os IDs digitais, que dependem da biometria, uma vez que não são secretos e os dados de identidade biométricos comprometidos não podem ser corrigidos;

28 Filipinas: Lei de Proteção de Dados Pessoais (2012) (secção 11(2)) e Regra IV secção 19(b) das Regras e Regulamentos de Implementação

29 México: Lei Federal sobre Proteção de Dados Pessoais detidos por Pessoas Privadas (2010) (Artigos 8,10 e 37) e Regulamentos (Artigo 15)

30 Ver, por exemplo, Peru: Lei de Proteção de Dados Pessoais (2011) e Regulamento para a Lei (2013) (ver especialmente o Artigo 7 do Regulamento e os Capítulos I e II do Título III).

31 Banco Mundial: ID Digital e o Desafio da Proteção de Dados: Nota do Profissional (2019)

- Identificação sem consentimento – isto pode ser feito através de:
  - Utilização não autorizada de dados biométricos, como impressões digitais ou leituras de íris ou informações de reconhecimento facial;
  - Identificar uma pessoa em vários domínios de serviço através da utilização de sua identificação digital;
- Vigilância ilegal de indivíduos através da utilização posterior de identificações digitais;
- Pedidos indevidos de identificação de um cliente através da disponibilização da sua identificação ID, com consequentes riscos de exploração comercial; e
- Utilização indevida de informações de identificação digital de domínio público por meio da utilização e partilha inadequadas entre agências governamentais. [32]

Os riscos acima são especialmente relevantes para os SFDs. Podem significar, por exemplo, que a identidade de um indivíduo é utilizada indevidamente para obter crédito, subsídios governamentais ou transferências monetárias; abrir conta poupança, que é utilizada para atividades ilegais; ou para obter acesso a fundos em contas de investimento ou de aposentadoria online. Estes riscos levaram a exigências de frameworks de proteção da privacidade.

Para uma discussão mais aprofundada sobre os benefícios e riscos dos sistemas de identificação digital, consulte: o Relatório Especial da AFI sobre FinTech para Inclusão Financeira: Um Framework para a Transformação Financeira Digital (2018) (Pilar 1) e também AFI: Inovações KYC, Inclusão Financeira e Integridade em Selecionados Países membros da AFI (2019).

PRIVACIDADE POR CONCEÇÃO

As regras proativas de privacidade desde a conceção são outra inovação importante, que pode minimizar os riscos da PDSFD para os titulares dos dados. Os princípios subjacentes a estas regras são bem conhecidos, [33] mas apenas agora começaram a ser introduzidos nos frameworks de privacidade de dados. Em resumo, a ideia é que os prestadores de SFDs devem ter disposições de governação, políticas, procedimentos e recursos documentados para garantir que cumprem sempre as regras de privacidade de dados. Além disso, a configuração padrão dos sistemas deve garantir a conformidade (por exemplo, com a regra de que apenas são processados os dados mínimos necessários para a finalidade de recolha permitida). Na prática, a conformidade com tais requisitos por parte dos prestadores de SFDs pode ser revista
pelos reguladores ao considerar pedidos de licença ou registo, pedidos de aprovação de novos produtos de SFDs ou em um contexto de sandbox regulatória.

Um exemplo está na nova Lei de Proteção de Dados do Quénia (2019), ao abrigo da secção 41, "Proteção de dados desde a conceção ou por defeito". Esses requisitos, que são semelhantes aos do Artigo 25 do RGPD, exigem (em resumo) que os controladores e processadores de dados implementem medidas técnicas e organizacionais adequadas:

- Implementar os princípios de proteção de dados do Quénia e as salvaguardas necessárias; e
- Garantir que, por defeito, apenas sejam tratados os dados pessoais necessários para cada finalidade específica, tendo em conta fatores específicos como a quantidade de dados pessoais recolhidos, a extensão do tratamento, o período de conservação e os custos de tratamento.

A Lei de Proteção de Dados do Quénia também contém requisitos para que os responsáveis pelo tratamento de dados e os processadores de dados considerem os riscos relevantes para os dados pessoais, as salvaguardas, a pseudonimização e a encriptação de dados pessoais e também a capacidade de restaurar dados.

Outro exemplo de requisitos de privacidade desde a conceção está no projeto de lei de proteção de dados pessoais da Índia (2019). O projeto de lei exige que todos os agentes fiduciários de dados preparem uma política detalhada de privacidade desde a conceção. A política pode ser submetida à DPA para certificação e qualquer política certificada deve ser publicada no site do fiduciário de dados e da Autoridade (secção 22). A publicação da política é um requisito importante, pois é provável que melhore a transparência para os titulares dos dados e investidores, bem como para a DPA e outros reguladores e agências governamentais.

AVALIAÇÕES DE IMPACTO NA PRIVACIDADE DE DADOS

Alguns países também têm requisitos para avaliar o impacto na privacidade de uma determinada operação de processamento de dados. Esses requisitos podem ser adicionais aos requisitos de Privacidade desde a conceção. Por exemplo, a Lei de Proteção de Dados do Quénia (2019) exige que seja preparada uma "avaliação de impacto da proteção de dados" em relação a uma operação de tratamento se esta for suscetível de resultar em "alto risco para os direitos e liberdades de um titular de dados, em virtude da sua natureza, âmbito, contexto e finalidades".[34] Em resumo, exige uma descrição sistemática dos requisitos de tratamento propostos e da sua necessidade e proporcionalidade, bem como dos riscos para os direitos e liberdades dos titulares dos dados e das medidas a tomar para os aliviar.

32 Para uma discussão destas questões, consulte a decisão do Supremo Tribunal da Índia no caso de justiça KS Puttaswamy vs. Union of India (2017) 10 SCC 1, que derrubou disposições legislativas que permitiam que empresas e indivíduos procurassem identificação através do identificador Aadhaar da Índia – ver https: //www.scobserver.in/court-case/constitutionality-of-aadhaar-act/ plain-englishsummary-of-judgment

33 Cavoukian, Ann 'Privacidade desde a conceção Os 7 Princípios Fundamentais Implementação e Mapeamento de Práticas Justas de Informação' (2011)

34 Lei de Proteção de Dados do Quénia (2019) (secção 31).

Está também prevista a consulta do Comissário para a Proteção de Dados e a publicação de diretrizes pelo Comissário para a Proteção de Dados.[35] O Gabinete do Comissário Australiano de Informação da Austrália publicou um Guia para Realizar Avaliações de Impacto na Privacidade e conselhos relacionados sobre a avaliação de riscos de privacidade e um curso de e-learning.[36] O projeto de lei de proteção de dados pessoais da Índia (2019) também é bastante específico ao exigir que um fiduciário de dados significativo conduza uma avaliação de impacto da proteção de dados nestes casos: onde o processamento envolve novas tecnologias ou processamento em grande escala ou a utilização de dados sensíveis (como dados genéticos ou biométricos) ou se o tratamento comportar um risco de "danos significativos".[37]

CADASTRO DE RESPONSÁVEL PELO TRATAMENTO DE DADOS E FORNECEDORES DE DADOS

Alguns países em desenvolvimento exigem agora que os responsáveis pelo tratamento de dados dos dados sejam registados. A Lei de Proteção de Dados do Gana (2012), conforme referido acima, exige o registo de todos os responsáveis pelo tratamento de dados .[38] A Lei de Proteção de Dados do Quénia (2019) estabelece que o Comissário de Dados pode prescrever limites para o registo obrigatório de controladores e processadores de dados.[39] As considerações relevantes para exigir o registo incluem:

- Se o registo ajudará a alcançar os objetivos de privacidade de dados e em que medida;
- Se a exigência de registo é uma resposta proporcional aos riscos de privacidade de dados; e
- Capacidade de supervisão e recursos para supervisionar o processo de registo.

OFICIAIS DE PRIVACIDADE DE DADOS

Está sendo cada vez mais prevista a nomeação de diretores pela privacidade (ou proteção) de dados (DPDs). Por exemplo, os regimes regulamentares de privacidade de dados de Gana, Quénia, México e Brasil têm tais disposições. A nomeação parece ser opcional em alguns casos. Noutros casos, depende de fatores como se a natureza, o âmbito, o contexto e as finalidades das atividades do processador são suficientemente grandes e/ou significativas e do tipo de dados que são processados. Por exemplo, o tratamento de dados sensíveis pode sugerir a nomeação de um DPD.

As funções dos DPDs variam mas, em termos gerais, podem incluir:

- Assessoria no cumprimento do framework;
- Ser um ponto de contacto para os titulares dos dados com dúvidas ou reclamações;
- Ser um ponto de contacto com a DPA relevante e outros reguladores e agências;
- Consultoria em Avaliações de Impacto na Privacidade; e
- Facilitar a capacitação de funcionários e agentes.

REPORTE DE VIOLAÇÕES DE PRIVACIDADE DE DADOS

Estão a ser introduzidos requisitos para comunicar o acesso não autorizado a dados pessoais. Por exemplo, a Lei de Proteção de Dados do Quénia (2019) prevê, com algumas exceções, que quando tenha havido acesso não autorizado a dados pessoais e "exista um risco real de danos" para o titular dos dados, o Comissário de Dados deve ser notificado no prazo de 72 horas. O titular dos dados deve ser notificado por escrito dentro de "um prazo razoavelmente praticável" e receber informações suficientes para tomar medidas de proteção.[40] Outros países com requisitos para notificar a DPA e/ou os titulares de dados relevantes incluem Gana, México, Peru e Austrália.

OPEN BANKING

Regimes open banking estão a ser introduzidos em vários países e regiões, incluindo economias em desenvolvimento e emergentes, levantando importantes questões de privacidade de dados.[41] Em resumo, o conceito de "open banking" refere-se geralmente a sistemas de partilha de dados de clientes por instituições financeiras com terceiros (tais como outras instituições financeiras, prestadores de serviços de pagamentos, agregadores de dados e parceiros comerciais). As questões preocupantes em matéria de privacidade de dados incluem a necessidade de consentimento expresso e a necessidade de garantir que os titulares dos dados compreendem o que estão a concordar. É claro que existem também questões de proteção de dados (tais como questões de segurança), que estão fora do âmbito desta Nota Orientadora. Exemplos de tais esquemas em diferentes formas encontram-se nas regras de partilha de dados da Lei das Instituições de Tecnologia Financeira do México (2018);[42] nas disposições relativas à capacidade dos sistemas de pagamentos e prestadores de serviços para aceder, processar e reter dados pessoais na Diretiva da UE 2015/2366 sobre

35 a nova Comissária para a Proteção de Dados do Quénia (Sra. Immaculate Kassait) que tomou posse em 6 de Novembro de 2020. Consulte https://www.capitalfm.co.ke/ news/2020/11/immaculate-kassait-sworn-in-as-inaugural-data- commissioner/

36 https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/

37 Lei de Proteção de Dados Pessoais da Índia (2019) (secção 27 e consulte a definição de 'dano significativo' na secção 3

38 Secção 27

39 Secção 18

40 Secção 43

41 Comitê de Supervisão Bancária do BIS Basel: Relatório sobre Open Banking e Interfaces de Programação de Aplicações (2019)

42 Artigo 76

Serviços de Pagamentos (PSD2);[43] e nas regras de open banking da Austrália e no direito de dados do cliente relacionado.[44]

RECURSO DO CONSUMIDOR

Estão sendo previstas reclamações por parte dos utilizadores de dados sobre violações de seus direitos em relação aos dados. Por exemplo, como observado acima, os regulamentos elaborados ao abrigo da Lei do México sobre a Proteção de Dados Privados detidos por Partes Privadas (2012) contêm disposições extensas sobre os procedimentos para o exercício dos direitos da ACRO. Outro exemplo é fornecido pelo Capítulo III do Título IV 'Procedimento de Proteção' no regulamento elaborado para fins da Lei de Privacidade de Dados das Filipinas (2012).

É comum permitir que reclamações sejam feitas à DPA relevante. Estes direitos geralmente só podem ser exercidos se a reclamação tiver sido apresentada primeiro ao responsável pelo tratamento de dados ou processador de dados e este tiver proferido uma decisão adversa ou não tiver tratado a reclamação num prazo razoável. Por exemplo, ao abrigo da Lei de Proteção de Informações Pessoais da África do Sul (2013), as reclamações podem ser apresentadas ao Regulador de Informação. Além disso, a compensação pode ser concedida com base em uma ação civil instaurada pelo titular dos dados ou pelo Regulador da Informação, a pedido do titular dos dados. Há também disposições para que os códigos de conduta emitidos pelo Regulador incluam disposições para o tratamento de reclamações, que devem cumprir as normas prescritas e quaisquer diretrizes emitidas pelo Regulador. Outros países também contemplam algumas ou todas estas questões. Exemplos estão nas leis de proteção de dados de Gana, Malásia, México e Filipinas.

As disposições que permitem à DPA iniciar ações em nome dos titulares dos dados são raras. A África do Sul é um exemplo. O OIAC da Austrália também pode investigar uma interferência na privacidade por sua própria iniciativa e determinar uma compensação ou exigir outras medidas corretivas. É importante que as DPA tenham esses poderes num contexto de inclusão financeira, dada a probabilidade de os titulares dos dados não terem os recursos ou a capacidade para intentar tais ações, ou não terem uma consciência clara dos seus direitos.

PRIVACIDADE DE DADOS EM EMERGÊNCIAS

Alguns países proporcionam alívio das regras estritas nos frameworks de privacidade de dados para permitir fluxos de dados para ajudar nas respostas a emergências (como a COVID-19). Um exemplo raro vem da Austrália. Em resumo, a Parte VIA da Lei de Privacidade da Austrália (1988) prevê a realização de declarações de emergência que permitem a recolha, utilização e divulgação de informações para uma finalidade permitida. Esses propósitos incluem, de forma relevante, ajudar indivíduos na obtenção de assistência financeira ou outra assistência humanitária. As declarações podem ser aplicadas por um período limitado de até 12 meses. Quando uma entidade confiar validamente em tal declaração, ela não será responsável pela violação de leis ou códigos específicos, incluindo os Princípios de Privacidade Australianos ou um código registado.

Orientações sobre questões de privacidade de dados no contexto da COVID-19 também foram fornecidas por agências internacionais. O Framework de Políticas da AFI para Alavancagem de Serviços Financeiros Digitais para responder a Emergências Globais – Caso de COVID-19 (2020), por exemplo, sugere que "os prestadores de SFDs devem garantir que os dados dos consumidores são protegidos e não partilhados com terceiros. Em circunstâncias extraordinárias, se for necessário extrair dados de clientes (para rastreamento de contactos e contenção de transmissão), isso deverá ser feito de forma voluntária. Além disso, tais medidas deveriam ser de natureza temporária.' (Regulamentos de Habilitação do Pilar III).

A OCDE também fez uma série de recomendações sobre privacidade de dados nas suas orientações sobre a COVID-19. As principais recomendações principais são (em resumo):

- Os governos precisam de promover a utilização responsável dos dados pessoais;
- Os governos devem consultar as Autoridades de Aplicação Efetiva da Privacidade (PEAs) antes de introduzir medidas que possam infringir os princípios estabelecidos de privacidade e proteção de dados;
- As PEAs devem abordar as incertezas regulamentares;
- Sujeitos às salvaguardas necessárias e proporcionais, os governos devem apoiar a cooperação nacional e internacional na recolha, processamento e partilha de dados pessoais de saúde; e
- Os governos e os responsáveis pelo tratamento de dados devem ser transparentes e responsáveis. [45]

CAIXA 9: OCDE: GARANTINDO A PRIVACIDADE DE DADOS ENQUANTO LUTAMOS CONTRA A COVID-19 (2020)

Os decisores políticos, em consulta com as autoridades responsáveis pela aplicação efetiva da privacidade, devem avaliar os possíveis compromissos na utilização de dados durante esta crise (conciliando os riscos e benefícios), mas devem garantir que quaisquer medidas extraordinárias sejam proporcionais aos riscos e sejam implementadas com total transparência, responsabilização e compromisso de

43 Artigo 94
44 Consulte https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0
45 OCDE Garantindo a privacidade dos dados enquanto lutamos contra a COVID-19 (2020)

A GSMA também lançou as Diretrizes de Privacidade sobre a COVID-19 para operadoras de redes móveis. [46]Podem ser relevantes para SFDs baseados em telemóveis e questões de privacidade relacionadas. O foco está nas divulgações para governos e agências. As Diretrizes cobrem questões como a necessidade de cumprir considerações éticas, bem como a lei; transparência sobre divulgações; e divulgações de metadados e dados agregados não identificáveis.

PENALIDADES

Penalidades significativas também estão sendo impostas em frameworks regulatórios de privacidade de dados mais recentes. Penalidades em grande escala podem constituir um incentivo ao cumprimento, bem como um incentivo ao investimento em Tecnologias de Melhoria da Privacidade (PETS) (que estão fora do âmbito desta Nota Orientadora).

Existem diversas abordagens sobre como as penalidades podem ser determinadas. Em alguns casos, baseiam-se numa percentagem do volume de negócios anual. Por exemplo, o RGPD da UE prevê uma penalidade máxima de até 4% do volume de negócios anual global da entidade.
A nova Lei de Proteção de Dados do Quénia (2019) adota uma abordagem menos rigorosa ao prever que a pena máxima seja a menor de uma pena máxima de cinco milhões de xelins (aproximadamente USD 45.700) [48] ou 1% do volume de negócios anual do exercício financeiro anterior. Outros países, como a Malásia, preveem uma multa de montante máximo e/ou uma pena de prisão.
A Lei Federal do México sobre a Proteção de Dados Pessoais detidos por Entidades Privadas adota uma abordagem interessante
na medida em que as potenciais multas são um múltiplo do salário mínimo da Cidade do México, com o montante variando a depender da violação. Um último exemplo vem do Peru, onde as violações são classificadas como leves, graves ou muito graves, com o nível da multa a variar de acordo.

SANDBOXES REGULATÓRIAS

Não parece ser comum que as sandboxes estabelecidas pelos reguladores do setor financeiro considerem especificamente as inovações da PDSFD. Em resumo, uma sandbox regulatória é um mecanismo cada vez mais popular para testar inovações FinTech num ambiente supervisionado. No entanto, não parece ser comum testar inovações relacionadas com a privacidade de dados em sandboxes ou em fóruns de inovação semelhantes estabelecidos pelos reguladores do setor financeiro. Em vez disso, países como
Em vez disso, países como a Austrália deixam claro que as entidades que recorrem a isenções regulamentares de sandbox ainda devem cumprir as leis de privacidade de dados.[49]

No entanto, existem alguns exemplos do conceito de sandbox que é utilizado em circunstâncias relevantes para a PDSFD.[50] Por exemplo:

- O Gabinete do Comissário de Informação (ICO) do Reino Unido criou uma sandbox e as suas principais áreas de enfoque para 2020-2021 incluem inovações relacionadas com a partilha de dados, nomeadamente na área das finanças. [51] É importante ressaltar que a ICO e a Autoridade de Conduta Financeira do Reino Unido também
têm um Memorando de Entendimento de 2019 que estabelece um framework de cooperação, coordenação e partilha de informações entre os reguladores.[52]
- Existem também sandboxes temáticas que abrangem objetivos específicos da política de privacidade de dados. Exemplos de sandboxes regulatórias temáticas existentes, incluindo alguns relevantes para a inclusão financeira e tecnologias 'NextGen', são destacados no CGAP: Blog - Uma Tendência Crescente na Regulamentação Financeira: Sandboxes Temáticas (2019).

Sandboxes regulatórias para inovações em privacidade de dados também podem ser previstas pela legislação. Um exemplo raro está no projeto de Lei de Proteção de Dados Pessoais da Índia (2019), que exige que a DPA crie uma 'Sandbox'. Isto deve ser feito "para efeitos de incentivo à inovação em inteligência artificial, aprendizagem automática ou qualquer outra tecnologia emergente de interesse público" (secção 40). Os fiduciários de dados que tiveram suas políticas de privacidade desde a conceção certificadas pela DPA são elegíveis para solicitar inclusão na Sandbox (sujeitos a regulamentações que ainda serão desenvolvidas).

REGRAS E ORIENTAÇÕES ESPECÍFICAS DO SETOR SOBRE PDSFD

Além das leis de aplicação geral acima referidas, existem exemplos limitados de frameworks regulamentares, códigos de prática, estratégias nacionais e intervenções políticas, que se aplicam especificamente a aspetos da PDSFD. Exemplos são fornecidos abaixo.

CAIXA 10: FRAMEWORK POLÍTICO DA AFI PARA CRÉDITO DIGITAL RESPONSÁVEL (2020)

'A proteção dos dados dos consumidores é crucial para garantir que o crédito digital, bem como outros serviços financeiros, dão aos consumidores a confiança de que os seus dados são privados e estão a ser utilizados de forma adequada.' (Princípio 6: Proteção de Dados e Privacidade)

46 Diretrizes de privacidade da GSMA sobre a COVID-19 (2020)
47 Para uma discussão sobre PETS e questões relacionadas, consulte ITU: Infraestrutura de Segurança de Iniciativa Global de Inclusão Financeira (FIGI) e Grupo de Trabalho de Confiança de Segurança, Big data, machine learning, proteção ao consumidor e privacidade (2018)
48 Em 15 de novembro de 2020 https://www.xe.com/
49 ASIC: INFO 248 Sandbox regulatória aprimorada (2020)
50 Centro de Liderança em Políticas de Informação: Sandboxes Regulatórias em Proteção de Dados: Engajamento Construtivo e Regulamentação Inovadora na Prática (2019)
51 https://ico.org.uk/sandbox
52 https://ico.org.uk/media/about-the-ico/documents/2614342/financial-conduct-authority-ico-mou.pdf

REGRAS DO SETOR FINANCEIRO PARA PDSFD

Também podem ser emitidas regras setoriais específicas cobrindo questões de especial preocupação da PDSFD. Um exemplo recente vem das Filipinas (ver Caixa 11).

CAIXA 11: CIRCULAR DA COMISSÃO NACIONAL DE PRIVACIDADE DAS FILIPINAS Nº 20-10 DIRETRIZES SOBRE O PROCESSAMENTO DE DADOS PESSOAIS PARA TRANSAÇÕES RELACIONADAS COM CRÉDITO (2020)

A Comissão Nacional de Privacidade das Filipinas emitiu recentemente a circular acima referida, na sequência de milhares de reclamações sobre a utilização de dados de telemóveis e de redes sociais por credores online, inclusive para fins de cobrança de dívidas. Aplica-se a empresas de empréstimo e financiamento e contém regras que proíbem a utilização de dados de contato para fins de cobrança de dívidas, restringindo a utilização de fotos e outras regras que limitam a recolha, utilização, divulgação e retenção de informações pessoais. A NPC ordenou separadamente a cessação das atividades de processamento por vários credores online [53] e a Comissão de Valores Mobiliários também tomou medidas para revogar a autorização de operação de alguns desses credores.[54]

Os frameworks regulamentares bancários, de pagamentos e de moeda eletrónica também podem conter regras de privacidade de dados. Exemplos incluem:

- O dever de confidencialidade/sigilo do banqueiro-cliente; [55]
- Regras sobre a privacidade e proteção das informações pessoais dos clientes nas regras de proteção do consumidor financeiro;[56]
- Uma obrigação para os requerentes de licenças de moeda eletrónica de cumprirem as normas aplicáveis relativas à segurança e confidencialidade dos dados;[57]
- Obrigações de garantir a confidencialidade da informação dos clientes relativa a instrumentos de pagamento, incluindo informação na posse de agentes;[58]
- A capacidade dos sistemas de pagamentos e dos prestadores de serviços de pagamento para aceder, processar e conservar dados pessoais (no caso da PSD2 da UE, isto requer consentimento explícito, sujeito a exceções como a deteção de fraudes[59]); e
- O direito dos utilizadores pagantes de utilizarem serviços de informação de contas (a PSD2 também requer consentimento explícito neste caso, bem como o cumprimento de outras condições). [60]

CÓDIGOS DA INDÚSTRIA

Códigos de privacidade de dados podem ser desenvolvidos para serviços financeiros, incluindo os SFDs. Nos frameworks regulatórios gerais de DP, é comum prever códigos específicos do setor a serem elaborados por grupos industriais e/ou o regulador de proteção de dados. Exemplos estão nos frameworks de DP para a UE, Austrália, Brasil, Gana, Quénia, Malásia, México e Filipinas e África do Sul. No entanto, tendo em conta que tais leis relevantes em matéria de DP são provavelmente bastante novas, são raros os exemplos de códigos específicos para serviços financeiros. A Malásia fornece um exemplo (ver Caixa 12).

Os códigos de práticas gerais do setor financeiro também podem conter disposições sobre privacidade. Por exemplo, o Código Bancário para a Proteção do Consumidor das Filipinas, que foi desenvolvido por várias associações bancárias, trata de questões de privacidade relativas a divulgações a terceiros não relacionados para fins de marketing e atividades de telemarketing através de e-mail, chamadas telefónicas e mensagens de texto (secção 2(e)).
Outro exemplo é o Código de Práticas Bancárias da indústria da África do Sul, que contém disposições que tratam da privacidade e confidencialidade das informações pessoais (secção 6.1).

CAIXA 12: MALÁSIA: O CÓDIGO DE PRÁTICAS DE PROTEÇÃO DE DADOS PESSOAIS PARA O SETOR BANCÁRIO E FINANCEIRO (2017)

A Lei de Proteção de Dados Pessoais da Malásia prevê o registo de "fóruns de utilizadores de dados" que podem então preparar um código de prática obrigatório por sua própria iniciativa ou a pedido do Comissário para a Proteção de Dados Pessoais (Parte II, Divisão 3). O código será registado se o Comissário estiver convencido de que é consistente com a Lei e se tiver sido dada a devida consideração às finalidades do processamento de dados pelos utilizadores de dados relevantes, às opiniões dos titulares dos dados e à autoridade reguladora relevante (como o Bank Negara Malaysia (BNM)), e o código em geral oferece um nível adequado de proteção. A pena por violação do Código é uma multa não superior a 100.000 ringgit (aproximadamente 2.425 dólares [61]) e/ou prisão até 1 ano.

53 https://www.privacy.gov.ph/2019/10/npc-shuts-down-26-online-lending-companies/

54 Por exemplo https://www.sec.gov.ph/pr-2020/sec-revokes-fcash-global-lendings-license/

55 Por exemplo: Afeganistão: Lei Bancária (1974) e Filipinas: Lei do Sigilo de Depósitos Bancários (1955)

56 Por exemplo: Filipinas: Circular BSP 857 – Regulamento sobre Proteção do Consumidor Financeiro (Capítulo II, secção (b) Proteção de Informações do Cliente)

57 Por exemplo: Regulamento de Dinheiro Eletrónico do Banco Indonésia (2018)

8 Por exemplo: Índia: Reserve Bank of India – Master Direction on Issuance and Operation of Prepaid Payment Instruments (2017) e Gana: Payments Systems and Services Act (2019)

59 Artigo 94

60 Artigo 67

61 Em 15 de novembro de 2020 - https://www.xe.com/currencyconverter/convert/?Amount=10%2C000&From=MYR&To=USD

CAIXA 12: *CONTINUAÇÃO*

O Código de Conduta de Proteção de Dados Pessoais para o Setor Bancário e Financeiro (2017) (Código BFS) está registado sob as disposições acima. O código aplica-se a todos os bancos e instituições financeiras licenciadas e foi desenvolvido pela Associação de Bancos da Malásia. O Código resume as disposições relevantes da Lei, os regulamentos relacionados e as Diretrizes de Transparência e Divulgação de Produtos do BNM e fornece exemplos específicos do setor de como eles podem ser interpretados na prática. A ênfase é colocada na explicação das definições de dados pessoais, sensíveis e pré-existentes e nas regras relativas ao marketing direto e à venda cruzada, ao contacto com o titular dos dados e à transferência de dados para o estrangeiro. Também
Também são fornecidos modelos para um Aviso de Privacidade, um Formulário de Pedido de Acesso a Dados e um Formulário de Solicitação de Correção de Dados.

ORIENTAÇÃO DE POLÍTICAS NACIONAIS E INTERNACIONAIS

As DPAs nacionais fornecem orientações políticas relevantes para a PDSFD. Por exemplo, os sites da Comissão Nacional de Privacidade das Filipinas[62] e da Comissão de Proteção de Dados de Gana[63] fornecem orientações sobre direitos e responsabilidades de acordo com as leis relevantes, relatórios de violação, como fazer uma reclamação e atualizações sobre o exercício de suas atribuições.

O Gana constitui um raro exemplo de um framework político nacional específico para os SFDs. A Caixa 13 descreve as seções relevantes para PDSFD.

As agências internacionais também fornecem orientação sobre questões regulatórias e políticas relevantes para a PDSFD. Por exemplo, as Boas Práticas para a Proteção do Consumidor Financeiro do Banco Mundial (2017) fornecem orientações sobre questões de proteção de dados e privacidade aplicáveis aos pagamentos de retalho. Foram desenvolvidos tendo em conta o ambiente de "Big Data" e outros desenvolvimentos relacionados com FinTech. (ver Anexo A, secção D). Em resumo, sugere-se a existência de frameworks regulamentares aplicáveis aos prestadores de serviços de pagamento (PSP), que:

- Permitam que os PSPs recolham dados dos clientes dentro dos limites estabelecidos por lei ou consentimento;
- Estabeleçam regras de recolha e conservação de dados pessoais;
- Limitem a utilização dos dados pessoais às finalidades especificadas no momento da recolha, permitidas por lei ou especificamente acordadas pelo cliente;
- Exigem que os PSPs mantenham a confidencialidade e segurança dos dados pessoais;

CAIXA 13: POLÍTICA DE SERVIÇOS FINANCEIROS DIGITAIS DO GOVERNO DO MINISTÉRIO DAS FINANÇAS DE GANA (2020)

Em maio de 2020, Gana lançou uma Política de DFS de quatro anos (2020-2023), considerada pela CGAP como a primeira do mundo. Foi concebido para servir de modelo sobre como o Gana pode alavancar o financiamento digital para atingir os seus objetivos de inclusão financeira, complementando a Estratégia Nacional de Inclusão Financeira e Desenvolvimento do Gana. A privacidade e a segurança dos dados foram consideradas "particularmente importantes" no contexto dos SFDs, juntamente com o comentário: "Existem claramente riscos específicos dos SFDs que terão de ser abordados pelo framework de proteção de dados. Propostas específicas sobre este ponto foram (em resumo):

- A Comissão de Proteção de Dados (DPC) necessita de recursos adicionais para concluir o processo de registo do responsável pelo tratamento de dados ao abrigo da Lei de Proteção de Dados de Gana (2012).
- A capacidade técnica da DPC deve ser aumentada com formação sobre especificidades de dados no ecossistema de SFDs.
- A cooperação entre a DPC, os reguladores do sector financeiro e a Autoridade Nacional de Comunicações deve ser facilitada através de um MOU.
- A utilização de dados alternativos no sector financeiro deve ser avaliada para determinar se são necessárias regulamentações adicionais.

- Responsabilizar legalmente os PSP pela utilização indevida de dados pessoais e por quaisquer violações de segurança de dados;
- Proibir que os PSPs partilhem dados com terceiros para qualquer finalidade (incluindo telemarketing ou marketing direto) sem consentimento prévio por escrito, a menos que o terceiro atue em nome do PSP e as informações sejam utilizadas para fins consistentes com a finalidade original da recolha (a menos que se aplique uma exceção, tal como um requisito legal);
- Permitir que os consumidores optem por não partilhar dados anteriormente autorizados a serem partilhados; e
- Desenvolver regras específicas para terceiros, como autoridades governamentais, registos de crédito e agências de cobrança.

Outras organizações internacionais também desenvolveram orientações sobre boas práticas relevantes para a PDSFD. Exemplos estão no Anexo 4.

62 https://www.privacy.gov.ph/
63 https://www.dataprotection.org.gh/

PRINCÍPIOS ORIENTADORES PARA UMA INTRODUÇÃO GERAL DO FRAMEWORK DE PDSFD

Os Princípios Orientadores pretendem ser uma orientação não vinculativa para um framework para uma estrutura regulatória da PDSFD proporcional e baseada em risco geral.

O framework foi desenvolvido no pressuposto de que não existe uma lei geral de proteção de dados em vigor. Os Princípios refletem tendências emergentes de alto nível em direitos e responsabilidades em matéria de privacidade de dados. No entanto, não devem ser consideradas como melhores práticas. Em particular, a depender do contexto do país, as disposições regulamentares poderão necessitar de ser mais ou menos detalhadas do que as propostas e estar sujeitas a reservas e exceções. Finalmente, embora os Princípios Orientadores tenham sido elaborados tendo em conta especificamente o processamento de dados no contexto dos SFDs, eles podem ser mais relevantes em geral, inclusive em relação aos serviços financeiros tradicionais.

Existem várias maneiras pelas quais os Princípios Orientadores podem ser implementados. Elas incluem:

- Uma nova lei;
- Regulamentações elaboradas ou orientações fornecidas para efeitos de uma lei existente do setor financeiro; ou
- Um código de prática obrigatório a ser desenvolvido por associações industriais e/ou reguladores relevantes.

A medida em que os Princípios Orientadores são relevantes para um país dependerá de vários fatores. Podem incluir os riscos identificados para a privacidade dos dados, o framework jurídico e regulamentar existente, as prioridades políticas, o mandato e os poderes dos reguladores, a capacidade de supervisão e os recursos e se existem associações industriais que possam apoiar eficazmente o desenvolvimento, a implementação e a aplicação efetiva de um código de prática.

Deve haver consulta sobre a opção preferida com os stakeholders dos setores público e privado, e com o público em geral. Isto poderiincluindo consultas com ministérios e reguladores que cobrem o sector financeiro, telecomunicações, concorrência, proteção do consumidor e inovação em geral. Deverá também haver consulta com o setor privado (incluindo prestadores de SFDs tradicionais e FinTech) e com os stakeholders da sociedade civil (tais como grupos de consumidores).

Também poderiam ser consideradas iniciativas regionais de privacidade de dados. Conforme observado no Framework de Políticas da AFI para Crédito Digital Responsável (2020) 'Quando for prático, as iniciativas regionais transfronteiriças podem criar confiança entre os países, facilitar a partilha de melhores práticas entre os legisladores e permitir que os reguladores de privacidade de dados detetem e resolvam a não conformidade com mais facilidade ' (Princípio 6).

Uma proposta foi incluída no final das Diretrizes para um regime 'minimalista' baseado em risco e proporcional da PDSFD a ser supervisionado pelo principal regulador do setor financeiro (como o Banco Central). Esta proposta contém sugestões de prioridades provisórias, no pressuposto de que a capacidade de supervisão e
os recursos que podem ser aplicados à PDSFD são limitados e também assumindo que não existe uma lei geral de proteção de dados em vigor.

OS PRINCÍPIOS ORIENTADORES DESCRITOS ABAIXO ESTÃO ORGANIZADOS EM SEIS PILARES.

Incluem recomendações chave para cada pilar. Quando relevante, as principais recomendações são organizadas com base em que aquelas que

PILAR 1: POLÍTICA DA PDSFDE FRAMEWORK REGULAMENTAR

PILAR 2: OBRIGAÇÕES DO RESPONSÁVEL PELO TRATAMENTO DE DADOS E PROCESSADOR DE DADOS DE DADOS

PILAR 3: DIREITOS DO TITULAR DOS

PILAR 4: CONSCIENCIALIZAÇÃO E RECURSOS DO CONSUMIDOR

PILAR 5: SUPERVISÃO E APLICAÇÃO

PILAR 6: PDSFD EM EMERGÊNCIAS GLOBAIS E NACIONAIS

PILAR 1: POLÍTICA E FRAMEWORK REGULATÓRIO DA PDSFD

Este Pilar destina-se a cobrir o processo de estabelecimento da política e do framework regulamentar da PDSFD e dos princípios relacionados.

1.1. PRINCÍPIO ORIENTADOR: ESTABELECER ACORDOS DE GOVERNANÇA E CONSULTA

PRINCIPAIS RECOMENDAÇÕES:

- Estabelecer um Comitê Diretor com o principal regulador da PDSFD e representantes de outros reguladores do setor financeiro e outros ministérios e agências governamentais relevantes (por exemplo, para finanças/telecomunicações/concorrência/proteção ao consumidor/inovação), bem como representantes da indústria (incluindo o setor financeiro tradicional e FinTech entidades) e consumidores (por exemplo, associações de consumidores).
- Garantir que os representantes do Comité Diretor tenham ou tenham acesso a conhecimentos especializados que abrangem SFDs, questões de privacidade de dados e inovações FinTech no processamento de dados para SFDs.
- Envolver especialistas externos conforme necessário, por exemplo, cientistas de dados ou especialistas em privacidade de dados.
- Consultar amplamente sobre o novo framework com os stakeholders do sector público/privado e o público em geral.

1.2. PRINCÍPIO ORIENTADOR: AVALIAR O FRAMEWORK JURÍDICO E REGULATÓRIO E O MERCADO ATUAL DOS SFDs

PRINCIPAIS RECOMENDAÇÕES:

- Realizar uma análise diagnóstica do framework jurídico e regulamentar existente aplicável à PDSFD, incluindo:
  - leis gerais de privacidade de dados e proteção ao consumidor
  - leis financeiras de proteção ao consumidor
  - disposições específicas do setor, por exemplo, leis sobre dinheiro eletrónico e pagamentos
  - códigos de prática da indústria
  - estratégias nacionais (por exemplo, para SFDs ou desenvolvimento do sector financeiro ou inclusão financeira)
  - diretrizes políticas e regulatórias
- Avaliar lacunas/sobreposições no framework regulamentar e no mandato e poderes de supervisão relacionados com referência aos Princípios Orientadores.
- Considere o mercado de SFDs e os riscos de privacidade de dados relacionados, incluindo tipos de fornecedores, controladores e processadores de dados pessoais, produtos de SFDs, formas de consentimento, políticas de privacidade, tipos de dados e técnicas de análise de dados utilizadas e quaisquer questões específicas da FinTech.
- Considerar as necessidades dos grupos vulneráveis, por exemplo, mulheres, jovens, idosos, pessoas com deficiência e pessoas deslocadas.
- Avalie quaisquer problemas de reclamações sistêmicas relacionadas à PDSFD.
- Documente os principais benefícios e riscos do ambiente atual para os stakeholders (especialmente titulares de dados e controladores e processadores de dados).

1.3. PRINCÍPIO ORIENTADOR: ESTABELECER POLÍTICAS ABRANGENTES E PRINCÍPIOS REGULATÓRIOS

PRINCIPAIS RECOMENDAÇÕES:

- Esclarecer os princípios regulamentares para orientar a conceção do framework da PDSFD.
- Considere especialmente regras proporcionais e baseadas no risco, que proporcionem um equilíbrio entre privacidade, proteção de dados, inovação e concorrência e que sejam:
  - claros e acessíveis
  - baseados em princípios
  - com tecnologia neutra
  - focados em resultados
- Exigir que o novo framework seja baseado em atividades, de modo a criar condições de concorrência equitativas e minimizar o risco de arbitragem regulamentar (sujeito aos pontos seguintes).
- Considere se algumas obrigações só devem ser aplicadas a responsáveis pelo tratamento de dados 'significativos', tais como obrigações relativas a:
  - Registo
  - Nomeação de um responsável pela privacidade de dados
  - Preparação de uma avaliação de impacto na privacidade para operações de processamento de alto risco
  - Relatórios de violação aos reguladores e aos titulares dos dados
  - Avaliações independentes de conformidade
- Se algumas regras se aplicarem apenas a responsáveis pelo tratamento de dados 'significativos', estabeleça critérios para a sua definição, tais como:
  - Natureza dos produtos ou modelo de negócios de SFDs.
  - Volume e sensibilidade dos dados processados.

- Número de titulares dos dados.
- Rotatividade.
- Risco de danos aos titulares dos dados, por exemplo, com base em discriminação ou preconceito.
- Utilização de novas tecnologias para processamento de dados, como processamento automatizado e perfilização.

1.4. PRINCÍPIO ORIENTADOR: DESENVOLVER O FRAMEWORK JURÍDICO DA PDSFD

PRINCIPAIS RECOMENDAÇÕES:

> Considerar boas práticas regionais/internacionais relevantes para PDSFD.

> Aplicar o framework a entidades públicas e privadas.

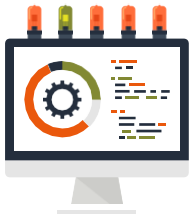
> Estabelecer definições e conceitos-chave (ver sugestões no Anexo 3).

> Considere quaisquer exceções que possam ser aplicadas, por exemplo, para dados abrangidos por outras leis, tais como relatórios de crédito ou cobrança de dívidas, para processamento de dados permitido ou exigido por outra lei ou quando existem considerações imperiosas, como a segurança nacional.

> Proporcionar um período de transição para que a indústria altere processos e procedimentos e sistemas de TI e para sensibilizar o público.

> Desenvolver campanha de sensibilização pública para o novo framework de PDSFD e direitos e responsabilidades relacionados.

PILAR 2: OBRIGAÇÕES DO RESPONSÁVEL PELO TRATAMENTO DE DADOS E DO PROCESSADOR DE DADOS



Este Pilar apresenta sugestões sobre as principais obrigações a impor aos responsáveis pelo tratamento de dados e aos processadores de dados, incluindo princípios fundamentais de processamento de dados.

2.1 PRINCÍPIO ORIENTADOR: EXIGIR ARRANJOS DE GOVERNANÇA INTERNA EFICAZES DA PDSFD

PRINCIPAIS RECOMENDAÇÕES:

- Exigir que os responsáveis pelo tratamento de dados :
  - Garantir que os funcionários e agentes sejam formados e estejam cientes das regras da PDSFD
  - Desenvolver e manter políticas e procedimentos documentados consistentes com as regras da PDSFD
  - Garantir a supervisão da alta gestão/Conselho sobre a conformidade com as regras da PDSFD
  - Ter sistemas e recursos tecnológicos e organizacionais adequados

> Exigir que a função de auditoria interna analise a conformidade com todas as regras da PDSFD.

> Exigir uma avaliação anual independente da conformidade com as regras da PDSFD.

2.2 PRINCÍPIO ORIENTADOR: ESTABELECER PRINCÍPIOS ABRANGENTES DE PROCESSAMENTO DE DADOS

PRINCIPAIS RECOMENDAÇÕES:

> Fazer a implementação básica dos princípios proativos de Privacidade desde a conceção estabelecidos numa política, que é aprovada e monitorizada pelo organismo de governo da entidade relevante e publicada no seu website e possivelmente no da DPA.[64]

> Estabelecer uma obrigação abrangente para garantir que o processamento seja sempre (independentemente do consentimento) justo, legal e transparente.

> Estabelecer outros princípios de processamento de dados, incluindo:

- Limitação de processamento: exigir que o processamento seja feito com consentimento, a menos que seja estritamente para fins da DFS

64 Veja também World Bank Group. A identificação digital e o desafio da proteção de dados: nota do profissional. 2019

contrato ou conforme exigido ou permitido por lei
- Minimização de dados: exigir que os dados sejam limitados às finalidades de processamento
- Precisão: exigir que os dados sejam precisos e atualizados e que sejam corrigidos ou apagados se não for o caso
- Limitação de armazenamento: exigir que as informações sejam retidas apenas por um período consistente com a finalidade do processamento
- Registos: exigir que registos de todas as atividades de processamento sejam mantidos
- Segurança: exigir processamento para minimizar o risco de processamento não autorizado ou ilegal e perda ou dano acidental

> Exigir que avaliações documentadas de impacto na privacidade baseadas em riscos sejam realizadas em atividades de processamento que possam representar alto risco para a privacidade dos titulares dos dados, especialmente considerando:
- Utilização de novas tecnologias
- Natureza, escala e finalidades do processamento
- Capacidades e necessidades dos titulares dos dados e especialmente dos grupos vulneráveis

> Incluir a obrigação específica de garantir que os processos e tecnologias relacionadas não resultem em decisões discriminatórias ou tendenciosas e atribuir o ónus da prova ao responsável pelo tratamento de dados /processador de dados para provar que não houve violação desta obrigação.

2.3 PRINCÍPIO ORIENTADOR: CRIAR MODELO PARA CONSENTIMENTO INFORMADO E EFICAZ

PRINCIPAIS RECOMENDAÇÕES:

> Avaliar os impedimentos locais para alcançar o consentimento efetivo, especialmente considerando as necessidades dos grupos vulneráveis (por exemplo, para consentimentos verbais, utilização de idiomas locais, acesso a formas digitais de consentimento e também níveis de literacia financeira)

> Exigir que todos os consentimentos:
- Sejam dados livremente, informados e inequívocos
- Sejam em termos simples e claros e o mais breve possível
- Sejam dados para fins específicos
- Não sejam agrupados (em particular, o consentimento para processamento do serviço de DFS deve ser separado do consentimento para outros fins)
- Sejam opt-in em vez de opt-out (o padrão deve ser opt-out)
- Estejam separados de outras informações, por exemplo, termos e condições
- Sejam limitados no tempo
- Possam ser retirados, sendo a retirada tão fácil quanto dar consentimento
- Possam ser guardados para referência futura

> Aplicar as mesmas regras de consentimento a todos os tipos de dados (sensíveis ou não).

> Elaborar regulamentos/fornecer diretrizes quanto ao significado prático de cada elemento das regras de consentimento para DFS, com exemplos.

> Fornecer que o responsável pelo tratamento de dados ou processador de dados tenha o ónus de provar o consentimento.

2.4 PRINCÍPIO ORIENTADOR: EXIGIR OFICIAL DE PROTEÇÃO DE DADOS QUANDO APROPRIADO

PRINCIPAIS RECOMENDAÇÕES:

> Exigir a nomeação de um responsável pela proteção de dados independente e com recursos adequados, sempre que a natureza, o âmbito, o contexto e as finalidades das atividades de tratamento sejam suficientemente grandes e/ou significativos.

> Especifique as funções do responsável pela proteção de dados para incluir, por exemplo:
- Conselhos sobre regras da PDSFD
- Monitorizar o cumprimento das regras
- Ponto de contacto para titulares de dados com dúvidas/reclamações
- Ponto de contato para DPA e outros reguladores
- Facilitar a capacitação de funcionários/agentes
- Avaliações de impacto na privacidade

PILAR 3: DIREITOS DO TITULAR DOS DADOS

Este Pilar define os principais direitos que podem ser concedidos aos titulares dos dados.

3.1 PRINCÍPIO ORIENTADOR: ESTABELECER OS DIREITOS FUNDAMENTAIS DOS TITULARES DOS DADOS

PRINCIPAIS RECOMENDAÇÕES:

- Direito à informação sobre o processamento e processadores/controladores relevantes
- Direito ao anonimato
- Direito de acesso
- Direito à retificação/correção
- Direito ao apagamento/direito ao esquecimento
- Direito de restringir/opor-se ao processamento
- Direito à portabilidade dos dados
- Direito de não ficar sujeito a uma decisão baseada exclusivamente em processamento automatizado (por exemplo, utilização de algoritmos e/ou aprendizagem de máquina), incluindo a perfilização sem consentimento expresso ou se permitido por lei

3.2 PRINCÍPIO ORIENTADOR: ESPECIFICAR COMO OS DIREITOS PODEM SER EXERCIDOS PELOS TITULARES DOS DADOS

PRINCIPAIS RECOMENDAÇÕES:

- Incluir disposições que expliquem como os direitos podem ser exercidos pelos titulares dos dados, por exemplo, processos aplicáveis, prazos de resposta, modelos, direitos de recurso.

PILAR 4: CONSCIENCIALIZAÇÃO E RECURSOS DO CONSUMIDOR

Este Pilar abrange propostas para mecanismos internos e externos de resolução de reclamações e litígios, direitos de recurso para titulares de dados e programas de sensibilização pública.

4.1 PRINCÍPIO ORIENTADOR: EXIGIR PROCEDIMENTOS EFICAZES DE TRATAMENTO DE RECLAMAÇÕES INTERNAS

PRINCIPAIS RECOMENDAÇÕES:

- Exigir que os controladores e processadores de dados tenham procedimentos documentados, transparentes, gratuitos e eficazes para a resolução de reclamações, abrangendo, por exemplo, a resolução rápida de reclamações; canais diversos para fazer reclamações; e publicidade dos processos de reclamações.

4.2 PRINCÍPIO ORIENTADOR: FORNECER UM ESQUEMA EXTERNO DE RESOLUÇÃO DE DISPUTAS PARA TITULARES DE DADOS

PRINCIPAIS RECOMENDAÇÕES:

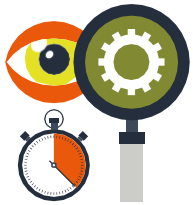
- Fornecer a um organismo externo (como DPA, supervisor do setor financeiro ou organismo de ombudsman) (EDR) poder para lidar com disputas relativas à PDSFD
- Permitir que a EDR inicie investigação ou ação judicial em nome dos titulares dos dados (incluindo uma classe) por sua própria iniciativa ou a pedido dos titulares dos dados.
- Certificar-se de que o EDR tenha poder para:
  - tomar decisões vinculativas
  - compensação de prémio
  - solicitar correção de dados
- Exigir que a EDR divulgue decisões em relação a disputas.

4.4 PRINCÍPIO ORIENTADOR: CONSIDERAR A NECESSIDADE DE PROGRAMAS DE CONSCIENCIALIZAÇÃO PÚBLICA

PRINCIPAIS RECOMENDAÇÕES:

- Incentivar os prestadores de DFS a promoverem a sensibilização para as questões de privacidade de dados, incluindo os direitos dos titulares dos dados e os principais riscos (por exemplo, para identificar roubo e fraude).
- Considerar o desenvolvimento de uma campanha específica de sensibilização pública para cobrir os direitos e responsabilidades no âmbito do novo framework da PDSFD.
- Ter em conta as questões de privacidade de dados e as necessidades específicas dos grupos vulneráveis nos programas de literacia financeira.

PILAR 5: SUPERVISÃO E APLICAÇÃO EFETIVA



Este Pilar abrange uma série de questões importantes relevantes para a supervisão e aplicação efetiva, incluindo a supervisão baseada no risco; mandato, poderes, capacidade e recursos de supervisão; a necessidade de consulta e coordenação contínuas; estabelecer uma ameaça credível de aplicação efetiva e considerar a privacidade dos dados num ambiente de sandbox regulatória.

5.1 PRINCÍPIO ORIENTADOR: ADOTAR UMA ABORDAGEM PROPORCIONAL E BASEADA NO RISCO PARA A SUPERVISÃO

PRINCIPAIS RECOMENDAÇÕES:

- Supervisionar as regras da PDSFD com base no risco firme e de mercado.
- Desenvolver uma metodologia para avaliar riscos de privacidade em modelos de negócios de DFS, por exemplo, fontes de informação, sensibilidade da informação, casos de utilização e interconectividade de sistemas.

5.2 PRINCÍPIO ORIENTADOR: GARANTIR QUE OS SUPERVISORES TENHAM MANDATO, PODERES, CAPACIDADE E RECURSOS EFICAZES

PRINCIPAIS RECOMENDAÇÕES:

- Fornecer aos supervisores um mandato claro da PDSFD.
- Garantir poderes apropriados para o supervisor, por exemplo, para supervisionar, avaliar a utilização de tecnologias relacionadas com FinTech ou exigir provas de como elas são utilizadas; emitir multas, conceder isenções, emitir ordens para proibir/suspender as práticas de processamento dos SFDs, registar ou cancelar o registo dos responsáveis pelo tratamento de dados e lidar com reclamações.
- Garantir que o supervisor tenha capacidade organizacional e tecnológica e recursos para conceber, implementar e supervisionar a PDSFD agora e no futuro, tendo em conta os prováveis desenvolvimentos da FinTech.
- Considerar o ambiente atual e os prováveis desenvolvimentos futuros, por exemplo, open banking.

5.3 PRINCÍPIO ORIENTADOR: ESTABELECER UM FRAMEWORK CLARO DE CONSULTA E COORDENAÇÃO

PRINCIPAIS RECOMENDAÇÕES:

- Fornecer consulta e coordenação contínuas com os stakeholders do sector público sobre questões políticas e regulamentares, inovações FinTech e questões sistémicas da PDSFD.
- Implementar mecanismo de consulta com grupos da indústria e da sociedade civil dos SFDs (por exemplo, defensores da privacidade e associações de consumidores).
- Considerar se o Grupo Consultivo da Indústria é desejável.[65]
- Estabelecer MOUs com os principais reguladores e agências governamentais.
- Considerar iniciativas regionais de privacidade de dados.

5.4 PRINCÍPIO ORIENTADOR: CONSIDERE OS PROBLEMAS DA PDSFD EM AMBIENTES DE SANDBOX REGULATÓRIA

PRINCIPAIS RECOMENDAÇÕES:

- Considerar questões de privacidade de dados ao testar inovações de DFS em sandboxes regulatórias.
- Considerar sandboxes regulatórias temáticas especificamente para inovações da PDSFD.

5.5 PRINCÍPIO ORIENTADOR: GARANTIR CREDIBILIDADE AMEAÇA DE APLICAÇÃO DA LEI

PRINCIPAIS RECOMENDAÇÕES:

- Garantir que as sanções sejam significativas o suficiente para serem eficazes.
- Divulgar todas as ações de aplicação efetiva.
- Exigir notificação de violações significativas aos reguladores/e titulares dos dados.
- Considerar prever que as multas sejam uma percentagem dos lucros ou do volume de negócios e/ou um montante fixo especificado.
- Considerar basear as multas na gravidade das violações.

65 Veja, por exemplo, Comitê Consultivo de Proteção de Dados Pessoais na Malásia

PILAR 6: PDSFD EM EMERGÊNCIAS GLOBAIS E NACIONAIS

Este Pilar contém recomendações para lidar com questões da PDSFD numa emergência, como a COVID-19, mas também se aplica de forma mais geral.

6.1 PRINCÍPIO ORIENTADOR: FORNECER ORIENTAÇÃO POLÍTICA SOBRE A APLICAÇÃO DA PDSFD EM EMERGÊNCIAS

PRINCIPAIS RECOMENDAÇÕES:

- Considerar orientações regulamentares para controladores/processadores de dados sobre desafios e expectativas específicas de privacidade de dados.
- Garantir a consulta entre a privacidade de dados e as autoridades reguladoras do setor financeiro.
- Considere os desafios da PDSFD em qualquer organismo de coordenação nacional.

6.2 PRINCÍPIO ORIENTADOR: GARANTIR QUE O FRAMEWORK JURÍDICO DA PDSFD PREVEJA SITUAÇÕES DE EMERGÊNCIA

PRINCIPAIS RECOMENDAÇÕES:

- Considere poderes para fornecer alívio das regras da PDSFD em caso de emergência.
- Se o poder não existir atualmente, considere a possibilidade de alterar a lei.

6.3 PRINCÍPIO ORIENTADOR: EXERCER A FLEXIBILIDADE ADEQUADA QUANTO À APLICAÇÃO EFETIVA NOS CASOS ADEQUADOS

PRINCIPAIS RECOMENDAÇÕES:

- Considerar fornecer alívio regulatório das leis existentes de privacidade de dados e identidade para fins de emergência para entidades do setor público e privado.
- Certifique-se de que qualquer alívio fornecido seja:
  - Proporcional aos riscos
  - Claro
  - Transparente para o público
  - Específico quanto aos propósitos
  - Tempo – limitado ao período de crise
- Tornar clara a responsabilização das autoridades reguladoras que prestam assistência.
- Proibir a partilha de dados com terceiros, exceto na medida especificamente permitida.
- Incentivar a indústria a colaborar com o governo, com as autoridades de privacidade de dados e com as autoridades de supervisão do setor financeiro nas questões da PDSFD.

ABORDAGEM MINIMALISTA DE PDSFD PARA REGULADORES DO SETOR FINANCEIRO

Esta proposta contém sugestões sobre as ações mínimas que os reguladores do setor financeiro poderão tomar no período intermédio antes de existir uma lei abrangente de proteção de dados em vigor.

1. REALIZAR AVALIAÇÃO DE ALTO NÍVEL DO MERCADO DE DFS E RISCOS DE PRIVACIDADE DE DADOS RELACIONADOS

- Abranger os setores público e privado, incluindo produtos, fornecedores (tradicionais e baseados em FinTech), canais de entrega, segmentos de clientes, tipos de dados utilizados e ferramentas analíticas.
- Desenvolver metodologia para avaliar riscos de privacidade em modelos de negócios de DFS, por exemplo, fontes de informação, sensibilidade da informação, casos de utilização e interconectividade de sistemas.
- Considerar especialmente as necessidades dos grupos vulneráveis.
- Considerar os objetivos de inclusão financeira.

2. ESTABELECER MECANISMO DE CONSULTA PARA NOVAS REGRAS DA PDSFD

Incluir representantes públicos, privados e da sociedade civil e garantir que tanto as entidades tradicionais como as FinTech sejam consultadas.

3. ESTABELECER CRITÉRIOS BASEADOS EM RISCO PARA DEFINIR OS RESPONSÁVEIS PELO TRATAMENTO DE DADOS de SFD 'SIGNIFICATIVOS'

Esses critérios poderão abranger, por exemplo:

- Volume e sensibilidade dos dados processados
- Número de titulares de dados
- Volume de negócios
- Risco de danos aos titulares dos dados, por exemplo, com base em discriminação ou preconceito
- Utilização de novas tecnologias para processamento de dados, como processamento automatizado e perfilização

4. DESENVOLVE NOVAS REGRAS DE PDSFD

As regras de prioridade baseadas no risco poderão abranger:

- Privacidade desde a conceção e governança padrão e arranjos de recursos
- Informações transparentes para os titulares dos dados sobre o processamento de dados
- Consentimentos efetivos e informados
- Direitos de acesso e correção e de oposição ao processamento
- Recurso para titulares de dados com reclamações (ex. quanto a indemnização ou correção de dados)

5. CONSIDERAR TAMBÉM REGRAS PARA CONTROLADORES E PROCESSADORES DE DADOS "SIGNIFICATIVOS"

As regras poderiam abranger, por exemplo, necessidades de registo; Diretor de Privacidade de Dados; Avaliações de impacto na privacidade; relatórios de violação aos reguladores e aos titulares dos dados; e avaliações independentes de conformidade.

6. CONSCIENCIALIZAR O CONSUMIDOR SOBRE PDSFD

Ter foco específico nas diversas necessidades dos grupos vulneráveis, na educação sobre os riscos de privacidade de dados com os SFDs e nos direitos e responsabilidades relacionados.

7. MANTER ARRANJOS DE CONSULTA CONTÍNUOS COM OS PRINCIPAIS STAKEHOLDERS

Por exemplo: principais ministérios e reguladores, FinTech e responsáveis pelo tratamento de dados de SFDs tradicionais e associações de consumidores.

ABREVIATURAS E ACRÔNIMOS

ACRO rights	Access, recertification, cancellation, and objection rights
AFI	Alliance for Financial Inclusion
CLD/CFT	Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo
BTCA	Better Than Cash Alliance
PCGTCM	Proteção do Consumidor e Grupo de Trabalho de Conduta de Mercado
CIF	Centro de Inclusão Financeira
GCAP	Grupo Consultivo de Assistência aos Pobres
PD	Privacidade de Dados
APD	Autoridade de Privacidade de Dados
PDSFD	Privacidade de dados para serviços financeiros digitais
SFDs	Serviços Financeiros Digitais
GTSFD	Grupo de Trabalho de Serviços Financeiros Digitais
DPD	Diretor de Privacidade de dados
G2P	Governo para Pessoa
RGPD/ Regulamento Geral de Proteção de Dados	Regulamento UE 2016/79 sobre a proteção de pessoas físicas no que diz respeito ao processamento de dados pessoais e à livre circulação desses dados
OCDE	Organização para a Cooperação e Desenvolvimento Económico
PSD2	Diretiva 2015/2366/UE relativa aos serviços de pagamentos no mercado interno
WB	World Bank Group

ANEXO 1.
LISTA DE ORGANIZAÇÕES ENTREVISTADAS PARA O PROJETO

PAÍS / REGIÃO	ORGANIZAÇÃO	NOME	POSIÇÃO
GLOBAL	CIF	Mayada El Zohghbi	Diretor-gerente
		Alexandra Rizzi	Diretor Sénior e Líder de Privacidade de Dados
GLOBAL	CRIF	Davide M. Meo	Diretor de Mercados Internacionais
		Valéria Racemoli	Especialista Regulatório Sénior
GLOBAL	GCAP	David Medine	Consultor
GLOBAL	GCAP	Ivo Jenik	Especialista do Setor Financeiro
GLOBAL	GSMA	Brian Muthiora	Diretor Regulatório, África
GLOBAL	Vodacom	Judith Obholzer	Gestão de Políticas Públicas Executivas
		Mpumi Simelane	Diretor de Privacidade do Grupo
GLOBAL	Crédito Habitação	Lucas Frohlich	Gerente Jurídico Sénior
		Vit Papousek	Gerente de Relações Exteriores
AUSTRÁLIA	Universidade de Nova Gales do Sul	Dra. Katherine Kemp	Professor Sénior Faculdade de Direito
GANA	Comissão de Proteção de Dados	Patrícia Adusei-Poku	Diretor Executivo/Comissário Comissão de Proteção de Dados
FILIPINAS	Comissão de Proteção de Dados	Ivy Grace Villasoto e outros	Diretor, Escritório de Política de Privacidade
	Bangko Sentral ng Pilipinas - Bangko Central das Filipinas	Ellen Joyce Suficiência e outros	Diretor, Centro de Inclusão e Estratégia de Aprendizagem

ANEXO 2.
PRINCIPAIS FRAMEWORKS REGULATÓRIOS ANALISADOS

PAÍS	PRINCIPAIS FRAMEWORKS REGULATÓRIOS
AUSTRÁLIA	Lei de Privacidade (1988)
BRASIL	Lei de Proteção de Dados Pessoais (2018)
UE	Regulamento Geral de Proteção de Dados (2016)
GANA	Lei de Proteção de Dados (2012)
ÍNDIA	Projeto de Lei de Proteção de Dados Pessoais (2019) Direção mestre do agregador de contas de empresas financeiras não bancárias RBI (2016) (atualizado em 22 de novembro de 2019)
QUÉNIA	Lei de Proteção de Dados (2019)
MALÁSIA	Lei de Proteção de Dados Pessoais (2010) Código de Conduta de Proteção de Dados Pessoais para o Setor Bancário e Financeiro (2017)
MÉXICO	Lei Federal sobre Proteção de Dados Pessoais detidos por Pessoas Físicas (2010) e Regulamentos (2012)
PERU	Lei de Proteção de Dados Pessoais (2011) e Regulamentos (2013)
FILIPINAS	Lei de Privacidade de Dados (2012) e Regras e Regulamentos de Implementação Circular NPC nº 20-01 Diretrizes sobre o Processamento de Dados Pessoais para Empréstimos – Transações Relacionadas (2020)
ÁFRICA DO SUL	Lei de Proteção de Informações Pessoais (2013)

ANEXO 3.
PRINCIPAIS CONCEITOS E DEFINIÇÕES

CONCEITO	DEFINIÇÃO
CONTROLADOR	Pessoa singular ou colectiva ou autoridade pública que, isoladamente ou em conjunto com outras, determina a finalidade ou o método de tratamento de dados pessoais.
TITULAR DOS DADOS	Um indivíduo cujos dados pessoais são ou podem ser processados.
FINTECH	A aplicação da tecnologia em finanças (em resumo, 'Tecnologia Financeira'). [66]
ID	Um meio oficial de identificação de um indivíduo.
OPEN BANKING	Esquemas de partilha de dados baseados no consentimento do cliente, em que os dados são partilhados por instituições financeiras com terceiros (tais como outras instituições financeiras, prestadores de serviços de pagamentos, agregadores de dados e parceiros comerciais).
DADOS PESSOAIS	Qualquer informação ou opinião relativa a uma pessoa singular identificada ou identificável, verdadeira ou não, mantida de forma material ou não e automatizada ou não.
PROCESSADOR	Pessoa física ou jurídica ou autoridade pública, que trata dados pessoais em nome do controlador.
EM PROCESSAMENTO	Qualquer operação realizada em relação a dados pessoais, seja manual ou automaticamente, incluindo recolha, utilização, divulgação, armazenamento, gravação, eliminação ou de outra forma e 'processos', 'processado' e palavras semelhantes têm um significado semelhante, mas excluindo qualquer processamento: • exigido para fins de atividades específicas (como função judicial, aplicação efetiva de uma reivindicação, segurança nacional ou finalidade puramente doméstica); ou • realizado para uma finalidade exigida ou permitida por lei.
PERFILIZAÇÃO	Uma forma de processamento que analisa, avalia ou prevê aspetos pessoais relevantes para um indivíduo, incluindo (sem limitação) seu comportamento, atributos, preferências ou características.
INFORMAÇÃO SENSÍVEL	Informações ou opinião sobre os dados financeiros, dados biométricos, identificador oficial, crenças ou afiliação religiosa, política ou filosófica de uma pessoa, filiação sindical, raça, etnia, casta, saúde e identidade sexual.
GRUPOS VULNERÁVEIS	Indivíduos que podem ser especialmente vulneráveis no contexto da PDSFD, tais como mulheres, jovens, idosos, pessoas com deficiência e pessoas deslocadas.

66 Comité de Supervisão Bancária do Banco de Pagamentos Internacionais (BIS): Relatório sobre Open Banking e Interfaces de Programação de Aplicações (2019) (Notas de rodapé 1 e 2)

ANEXO 4. BOAS PRÁTICAS INTERNACIONAIS PARA PDSFD

As organizações internacionais desenvolveram orientações sobre boas práticas relevantes para a PDSFD.

Exemplos incluem:

- **O Banco Mundial:** Boas Práticas para a Proteção do Consumidor Financeiro (2017) (ver Anexo A, secção D)
- **Better Than Cash Alliance:** Diretrizes para Pagamentos Digitais Responsáveis (2016) (ver Diretriz 7)
- **G20:** Princípios de Alto Nível para Inclusão Financeira Digital (2016) (ver Princípios 2 e 5)
- **GSMA:** Diretrizes sobre proteção de dados de dinheiro móvel (2018). Consulte também GSMA: Proteção de Dados em Dinheiro Móvel (2019) e GSMA: Leis de Privacidade de Dados Inteligentes. Alcançando os resultados certos para a era digital (2019)
- **OCDE (2020):** Utilização de dados pessoais em serviços financeiros e o papel da educação financeira: uma análise centrada no consumidor (2020)

ANEXO 5. REFERÊNCIAS

PRODUTOS DE CONHECIMENTO AFI

AFI: Relatório especial sobre a criação de ecossistemas capacitadores de FinTech: o papel dos reguladores (2020) https:// www.afi-global.org/publications/3181/Creating- Enabling-FinTech-Ecosystems-The-Role-of-Regulators

AFI: Framework Político para Aproveitar Serviços Financeiros Digitais para Responder a Emergências Globais – Caso de COVID-19 (2020) https://www.afi-global.org/sites/ default/files/publications/2020-10/AFI_DFSWG_COVID_ PF_AW4_digital.pdf

AFI: Modelo de Política de Proteção ao Consumidor para Serviços Financeiros Digitais (2020) https://www.afi-global. org/publications/3465/Policy-Model-on-Consumer- Protection-for-Digital-Financial-Services

AFI: Estrutura Política para Crédito Digital Responsável (2020) https://www.afi-global.org/publications/3216/Policy-Framework-for-Responsible-Digital-Credit

AFI: Modelo de Política para Dinheiro Eletrónico (2019) https://www.afi- global.org/publications/3088/Policy-Model-for-E-Money

AFI: Inovações KYC, inclusão financeira e integridade em países membros selecionados da AFI (2019) https://www.afi-global.org/sites/default/files/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected- AFI-Member-Countries.pdf

AFI: Relatório Especial sobre FinTech para Inclusão Financeira: Um Framework para a Transformação Financeira Digital (2018) https://www.afi-global.org/publications/2844/FinTech-for-Financial-Inclusion-A-Framework-for-Digital-Financial-Transformation

Bases de dados globais de leis de proteção e privacidade de dados DLA Piper Leis de proteção de dados do mundo
https://www.dlapiperdataprotection.com/

Legislação Mundial de Proteção de Dados e Privacidade da UNCTAD
https://unctad.org/page/data-protection- and-privacy-legislation-worldwide

OUTRAS PUBLICAÇÕES

Arner DW, Buckley RP, Zetzsche, DA e Veidt, R: Sustentabilidade, FinTech e Inclusão Financeira Eur Bus Org Law Rev 21, 7–35 (2020) https://doi.org/10.1007/s40804-020-00183-y

Austrália: Procurador – Departamento Geral: Documento sobre questões de revisão da Lei de Privacidade (2020) https://www.ag.gov. au/integrity/publications/review-privacy-act-1988-cth- issues-paper

Comité de Supervisão Bancária do Banco de Pagamentos Internacionais (BIS): Relatório sobre Open Banking e Interfaces de Programação de Aplicações (2019) https://www.bis.org/bcbs/publ/d486.htm

Better Than Cash Alliance: Diretrizes para Pagamentos Digitais Responsáveis (2016) https://www. betterthancash.org/tools-research/case-studies/ responsible-digital-payments-guidelines

Carpenter v. Estados Unidos 585 EUA (2018) https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

Centro para Inclusão Financeira (CIF) e Instituto de Finanças Internacionais: Acelerando a Inclusão Financeira com Novos Dados (2018) https://www.centerforfinancialinclusion.org/accelerating-financial-inclusion-with-new-data-2

CIF: Blog - Proteção de Dados e Inclusão Financeira: Por que é Importante (Introdução) (2020)https://www.centerforfinancialinclusion.org/data-protection-and-financial-inclusion-why-it-matters-introduction

CIF: Blog - Consentimento de dados: vamos partilhar o fardo para uma proteção eficaz ao consumidor (2020)https://www. centerforfinancialinclusion.org/data-consent-lets-share-the-burden-for-efficient-consumer-protection

CIF: Blog - Dados para Finanças Inclusivas: Cumprindo a Promessa para os Consumidores (2020)https://www.centerforfinancialinclusion.org/data-for-inclusive-finance-delivering-on-the-promise-for-consumers

CGAP: Blog - Uma Tendência Crescente na Regulamentação Financeira: Sandboxes Temáticas (2019)https://www.cgap.org/blog/ growing-trend-financial-regulation-thematic-sandboxes

CGAP: Nota de foco – A privacidade de dados é boa para os negócios? (2019)https://www.cgap.org/sites/default/files/publications/2019_12_Focus_Note_Is_Data_Privacy_Good_for_Business.pdf

CGAP: Fazendo os dados funcionarem para os pobres: novas abordagens para proteção e privacidade de dados (2020)https://www.cgap.org/research/publication/making-data-work-poor

CGAP: Blog - Open Banking: 7 maneiras pelas quais a partilha de dados pode promover a inclusão financeira (2020)https://www.cgap. org/blog/open-banking-7-ways-data-sharing-can- advance-financial-inclusion

CGAP: Blog - Blog Preocupações com privacidade de dados influenciam comportamentos financeiros na Índia, Quénia (2020)https:// www.cgap.org/blog/data-privacy-concerns-influence- financial-behaviors-india-kenya

CGAP: Blog – Dados Abertos e o Futuro do Banco (2019)https://www.cgap.org/blog/open-data-and-future-banking

Centro de Liderança em Políticas de Informação: Sandboxes Regulatórias em Proteção de Dados: Engajamento Construtivo e Regulamentação Inovadora na Prática (2019) https:// www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/07/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf

Covington e Burlington LLP: Sobreposição entre o RGPD e o PSD2 Inside Privacy (2018) https://www.insideprivacy.com/financial-institutions/overlap-between-the-gdpr-and-psd2/

Deloitte: Depois que a poeira baixar. Como os serviços financeiros estão adotando uma abordagem sustentável para a conformidade com o RGPD em uma nova era de privacidade, um ano em https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-the-impact-of-gdpr-on-the-financial-services.pdf

Autoridade Europeia para a Proteção de Dados: Guia rápido da EDPS sobre a necessidade e a proporcionalidade (2020) https://edps.europa.eu/data-protection/our-work/ publications/factsheets/edps-quick-guide-necessity- and-proportionality_en

Parlamento Europeu: Perguntas Parlamentares: Referência da Pergunta: E-000054/2019 (10 de março de 2019) https://www.europarl.europa.eu/doceo/document/E- 8-2019-000054-ASW_EN.html

Kemp K, Universidade de Nova Gales do Sul: Big Data, Inclusão Financeira e Privacidade para os Pobres. Fórum de Finanças Responsáveis (2017) https://responsiblefinanceforum. org/big-data-financial-inclusion-privacy-poor/

Kemp K; Buckley RP, 'Protegendo dados de consumidores financeiros em países em desenvolvimento: uma alternativa para o modelo de consentimento falho, Georgetown Journal of International Affairs, vol. 18, pp 35 – 46 (2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3237856

Finextra: Blog de Carlo RW de Meijer Economista e pesquisador da De Meijer Independent Financial Services Advisory (MIFSA): Blockchain versus RGPD e quem deve se ajustar mais (2018) https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most

G20: Princípios de Alto Nível para Inclusão Financeira Digital (2016) https://www.gpfi.org/publications/g20-high- level-principles-digital-financial-inclusion

Orientação Política do G20/OCDE: Abordagens de Proteção ao Consumidor Financeiro: Proteção ao Consumidor Financeiro na Era Digital (2018) https://www.oecd.org/ finance/G20-OECD-Policy-Guidance-Financial-Consumer- Protection-Digital-Age-2018.pdf

GSMA: O impacto dos requisitos de localização de dados no crescimento do dinheiro móvel – remessas habilitadas (2018) https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Understanding- the-impact-of-data-localisation.pdf

GSMA: Diretrizes sobre proteção de dados de dinheiro móvel (2018) https://www.gsma.com/mobilefordevelopment/ wp-content/uploads/2018/09/GSMA-Guidelines-on- mobile-money-data-protection.pdf

GSMA: Proteção de dados em dinheiro móvel (2019) https://www.gsma.com/mobilefordevelopment/resources/data- protection-in-mobile-money/

GSMA: Leis de Privacidade de Dados Inteligentes. Obtenção dos resultados certos para a era digital (2019) https://www.gsma. com/publicpolicy/wp-content/uploads/2019/06/GSMA_ Smart-Data-Privacy-Laws_Report_June-2019.pdf

GSMA: Relatório sobre o estado da indústria sobre dinheiro móvel (2019) https://www.gsma.com/sotir/wp-content/uploads/2020/03/GSMA-State-of-the-Industry-Report- on-Mobile-Money-2019-Full-Report.pdf

GSMA: Relatório sobre o estado da conectividade da Internet móvel (2020) https://www.gsma.com/r/wp-content/ uploads/2020/09/GSMA-State-of-Mobile-Internet- Connectivity-Report-2020.pdf

GSMA: Diretrizes de privacidade da GSMA COVID-19 (2020) https://www.gsma.com/publicpolicy/resources/covid- 19-privacy-guidelines

Fundo Monetário Internacional (FMI): A promessa da inclusão financeira da FinTech na era pós-COVID-19. Nº 20/09 (2020) https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2020/06/29/The-Promise-of-Fintech-Financial-Inclusion-in-the-Post-COVID-19-Era-48623

FMI: Série Especial sobre COVID-19 - Serviços Financeiros Digitais e a Pandemia: Oportunidades e Riscos para Economias Emergentes e em Desenvolvimento (2020)

União Internacional de Telecomunicações (UIT): Grupo de Foco em Serviços Financeiros Digitais, Relatório do Grupo de Foco sobre Identificados Comummente Temas de proteção ao consumidor para serviços financeiros digitais 05/2016 (2016) https://www.itu.int/en/ITUT/focusgroups/dfs/Documents/09_2016/ConsumerProtectionThemesForBestPractices.pdf

ITU: Iniciativa Global de Inclusão Financeira (FIGI), Grupo de Trabalho de Infraestrutura de Segurança e Confiança, Big data, aprendizagem de máquina, proteção ao consumidor e privacidade (2018) https://www.itu.int/en/ITU-T/extcoop/figisymposium/2019/Documents/Presentations/Big%20data,%20Machine%20learning,%20Consumer%20protection%20and%20Privacy.pdf

McDonald AM e Cranor LF: O custo da leitura das políticas de privacidade. Um Jornal de Direito e Política para a Sociedade da Informação, vol. 4, nº 3 (2008), 543-568 (2008) https://kb.osu.edu/handle/1811/72839

OCDE: Diretrizes sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais (1980, atualizadas em 2013) http://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OCDE: Garantindo a privacidade dos dados enquanto lutamos contra a COVID-19 (2020) https://read.oecd-ilibrary.org/view/?ref=128_128758-vfx2g82fn3&title=Ensuring-data-privacy-as-we-battle-COVID-19

OCDE: Utilização de dados pessoais em serviços financeiros e o papel da educação financeira: uma análise centrada no consumidor (2020) http://www.oecd.org/financial/education/Personal-Data-Use-in-Financial-Services-and-the-Role-of-Financial-Education.pdf

Centro de Toronto: Computação em Nuvem: Questões para Supervisores (2020) https://res.torontocentre.org/guidedocs/Cloud%20Computing%20FINAL.pdf

Banco Mundial: Proteção do consumidor financeiro e novas formas de processamento de dados além dos relatórios de crédito (2018) https://openknowledge.worldbank.org/handle/10986/31009

Banco Mundial: Boas Práticas para Proteção do Consumidor Financeiro (2017) https://www.worldbank.org/en/topic/financialinclusion/brief/2017-good-practices-for-financial-consumer-protection

Banco Mundial: ID Digital e o Desafio da Proteção de Dados: Nota do Profissional (2019) https://openknowledge.worldbank.org/handle/10986/32629

Banco Mundial: Tecnologias Disruptivas na Indústria de Partilha de Informações de Crédito: Desenvolvimentos e Implicações (2019) http://documents1.worldbank.org/curated/en/587611557814694439/pdf/Disruptive-Technologies-in-the-Credit-Information-Sharing-Industry-Developments-and-Implications.pdf

Nações Unidas (ONU): Princípios de Proteção de Dados Pessoais e Privacidade (2018) https://unsceb.org/sites/default/files/UN-Principles-on-Personal-Data-Protection-Privacy-2018.pdf

Zetzsche, DA, Arner, DW. e Buckley, RP e Kaiser-Yücel, A: Kit de ferramentas FinTech: abordagens regulatórias e de mercado inteligentes para inovação em tecnologia financeira (maio de 2020). Artigo de pesquisa da Faculdade de Direito da Universidade de Hong Kong nº 2020/027 https://ssrn.com/ abstract=3598142

Alliance for Financial Inclusion
AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
t +60 3 2776 9000 **e** info@afi-global.org www.afi-global.org

Alliance for Financial Inclusion AFI.History @NewsAFI @afinetwork