PROTEÇÃO DE DADOS PESSOAIS NO SETOR DE FINTECHS

MOLINA ADVOGADOS

ÍNDICE

1 O QUE SÃO FINTECHS?

2 FINTECHS E PROTEÇÃO DE DADOS PESSOAIS

3 DADOS PESSOAIS TRATADOS PELAS FINTECHS

4 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS ("LGPD")

5 NORMAS SETORIAIS APLICÁVEIS ÀS FINTECHS

6 BASES LEGAIS PARA TRATAMENTO

7 DIREITOS DOS TITULARES

8 DA SEGURANÇA E BOAS PRÁTICAS

9 CONSIDERAÇÕES FINAIS

MOLINA ADVOGADOS

1

O QUE SÃO FINTECHS?

A palavra **Fintech** é formada pela união dos termos em língua inglesa *finance* e *technology* (finanças e tecnologia) para identificar as empresas que utilizam tecnologia para prestação de serviços financeiros.

As Fintechs surgiram para tentar solucionar os desafios oriundos da concentração bancária, incluindo a burocracia, falta de acessibilidade, altas taxas cobradas pelo mercado e o spread bancário.

Com o uso de tecnologia, as Fintechs conseguem oferecer serviços de maneira menos burocrática e mais célere que as empresas convencionais, apostando também na acessibilidade desses serviços, por exemplo, oferecendo serviços por meio de aplicativos.

As Fintechs geralmente se especializam em poucos serviços financeiros, diferente dos grandes bancos, para focar na experiência do cliente. Assim, oferecendo um serviço em um nicho mais específico, conseguem competir com os serviços oferecidos pelos bancos convencionais.

MOLINA ADVOGADOS

2

FINTECHS E PROTEÇÃO DE

DADOS PESSOAIS

Tratamento é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

- O tratamento de dados pessoais tem extrema importância nos mais diversos setores da economia, sendo certo que atualmente os dados são considerados como uma nova modalidade de **ativo**.
- A obtenção e tratamento escalonados de dados permitem a elaboração de perfis (*profiling*), segmentação de pessoas pelo seu comportamento (*behavioral targeting*) e a segmentação de público, podendo influenciar e manipular resultados de mercado, hábitos, controle de segurança, ideologias, dentre outros. Por isto, o tratamento de dados pessoais é cada vez mais importante para as operações e negócios de iniciativa privada e de gestão governamental.
- No setor das Fintechs, esse cenário não é diferente. Para exercer suas atividades de maneira eficiente, a maioria das Fintechs trata dados de forma massiva, por exemplo, para análise de perfil de crédito ou para verificar a segurança das transações (mecanismos antifraude).
- Diante do aumento da coleta de dados pessoais e os riscos de abusos e violação ao direito à privacidade, a tendência mundial é de que os países adotem uma política de proteção de dados, garantindo maior segurança para os indivíduos.
- No setor de atuação das Fintechs, considerando a natureza dos dados tratados, se faz necessária a proteção e privacidade dos dados, bem como a segurança da informação, o que é disciplinado de maneira específica pelos órgãos reguladores. Assim, nestes casos, além das normas gerais de proteção de dados pessoais também devem ser observadas as normas específicas do setor.

MOLINA ADVOGADOS

3

DADOS PESSOAIS TRATADOS PELAS FINTECHS

Os dados tratados pelas Fintechs podem incluir dados pessoais e, em particular, podem integrar uma categoria especial de dados pessoais, os quais são designados como dados sensíveis, o que deixa clara a necessidade de adoção de medidas de proteção dos dados tratados e cumprimento das legislações e regramentos aplicáveis à privacidade e segurança de dados.

Dados pessoais: qualquer informação relacionada a pessoa natural identificada ou identificável.

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, genético ou biométrico.

MOLINA ADVOGADOS

3

DADOS PESSOAIS TRATADOS PELAS FINTECHS

Nosso ordenamento jurídico prevê alguns tipos de dados sigilosos, dentre eles:

Informações protegidas pelo sigilo fiscal

aquelas que, nos termos do artigo 198 do Código Tributário Nacional, são produzidas ou obtidas para o cumprimento de finalidades relacionadas à atividade da Administração Tributária. Seria o caso, por exemplo, das declarações de Imposto Renda das Pessoas Físicas e Jurídicas.

Informações protegidas pelo sigilo bancário

aquelas que expõem o conteúdo individualizado das operações ativas e passivas e serviços prestados pelas instituições financeiras. O sigilo bancário é previsto na Lei Complementar nº 105/2001 ("Lei de Sigilo Bancário") e deve ser observado pelas instituições financeiras, bem como pelos órgãos regulamentadores. Este é o caso, por exemplo, de informações sobre valores remetidos para e do exterior por pessoas físicas e jurídicas e de extratos sobre a movimentação financeira de contas bancárias.

Para as Fintechs que não sejam constituídas como instituições financeiras, o dever de sigilo poderá não ser aplicável, o que dependerá da análise do caso concreto (ao verificar, por exemplo, as atividades e dados tratados pela Fintech). Isto não afasta o dever de observar quais as consequências de eventual tratamento inadequado ou compartilhamento de dados, já que as Fintechs responderão pelos danos eventualmente ocasionados aos titulares dos dados.

As Fintechs constituídas como instituições financeiras, a exemplo de Sociedade de Crédito Direto ("SCD") e Sociedade de Empréstimo entre Pessoas ("SEP"), registradas perante o Bacen, devem observar a Lei de Sigilo Bancário.

Não obstante a previsão legal de sigilo bancário e sigilo fiscal, é possível que o dever de sigilo sobre determinados dados seja imposto judicialmente, por exemplo.

É importante ressaltar, ainda, que convencionou-se denominar "dados financeiros" os dados referentes a operações ou serviços financeiros, por exemplo, data da transação, dados cadastrais, dentre outros, mas não há uma definição legal para o termo. Tais dados financeiros poderão ser considerados dados sigilosos ou dados pessoais, a depender do contexto e do tipo de dado tratado.

MOLINA ADVOGADOS

4

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Em observância à tendência mundial de proteção aos dados pessoais, foi publicada no Brasil, em 14 de agosto de 2018, a Lei nº 13.709, também conhecida como "Lei Geral de Proteção de Dados Pessoais" ou "LGPD".

Até o advento da LGPD, o ordenamento jurídico brasileiro regulava o tratamento de dados pessoais de forma vaga e esparsa, encontra-se a abordagem de forma superficial na Constituição Federal Brasileira, no Código Civil Brasileiro (Lei nº 10.406/2002), no Código de Defesa do Consumidor (Lei nº 8.078/1990), no Marco Civil da Internet (Lei nº 12.965/2014), na Lei de Sigilo Bancário, na Lei do Cadastro Positivo (Lei nº 12.414/2011), dentre outras.

Destacamos que os direitos à intimidade e à privacidade, fundamentos para a proteção dos dados pessoais, são amparados por nosso ordenamento jurídico e estão previstos na Constituição Federal Brasileira, a qual assegura o direito à indenização pelos danos decorrentes de sua violação.

Apesar destas leis terem como objetivo garantir o direito à intimidade e à privacidade, foram elaboradas em circunstâncias que não contemplavam o cenário dinâmico e tecnológico atual. Com o intuito de suprir a lacuna legislativa sobre a proteção de dados pessoais, foi sancionada a LGPD, que estabelece regras sobre como as empresas e os órgãos públicos devem tratar os dados pessoais das pessoas físicas, fixa limites e procedimentos para o tratamento desses dados.

MOLINA ADVOGADOS

4

LEI GERAL DE

PROTEÇÃO

DE DADOS PESSOAIS

Aplicação da lei

De acordo com o artigo 3º da LGPD, referida lei se aplica a qualquer operação de tratamento de dados realizada por pessoa física ou jurídica (de direito público ou privado), independentemente do meio, do país de sua sede ou do país em que estejam localizados os dados, desde que:

- Os dados pessoais tenham sido coletados no Brasil ou qualquer operação de tratamento seja realizada no território nacional; ou
- A atividade de tratamento, mesmo que realizada fora do território nacional, tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no Brasil.

Agentes de Tratamento

Importante mencionar que a LGPD criou algumas figuras para delimitar responsabilidades no processo de tratamento de dados.

- Controlador: pessoa (natural ou jurídica) a quem competem as decisões referentes ao tratamento de dados pessoais;
- Operador: pessoa (natural ou jurídica) que realiza o tratamento de dados pessoais em nome do controlador; e
- Encarregado: pessoa indicada pelo controlador, que atua como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados ("ANPD").

A LGPD estabelece a responsabilidade solidária entre o controlador das informações e seus operadores, garantido o direito de regresso entre eles.

MOLINA ADVOGADOS

4 LGPD

A LGPD prevê diversos princípios que devem ser observados no tratamento de dados e assim, em vista do caráter principiológico, é possível que referida Lei possa acompanhar os avanços tecnológicos sem que sejam necessárias alterações ou adaptações ao texto da Lei. O artigo 6º da LGPD elenca os princípios que devem ser observados em todo tratamento de dados pessoais, quais sejam:

Finalidade
O tratamento deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular.

Livre acesso
Deve ser garantida ao titular consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Transparência
Deve-se garantir informações claras, precisas, acessíveis aos titulares.

Prevenção
Os agentes de tratamento devem adotar medidas para prevenir a ocorrência de danos aos titulares.

Adequação
O tratamento deve ser compatível com as finalidades informadas ao titular.

Segurança
Os agentes de tratamento devem adotar medidas para proteção dos dados pessoais de acessos não autorizados ou situações acidentais ou ilícitas (perda, destruição, alteração, comunicação ou difusão).

Responsabilização e prestação de contas *(accountability)*
Demonstração e comprovação pelos agentes de tratamento que foram adotadas medidas de segurança adequadas e eficazes para assegurar o cumprimento da LGPD.

Qualidade
Os agentes de tratamento devem garantir aos titulares que os dados sejam exatos, claros, atualizados.

Necessidade
Uso apenas de dados necessários (não excessivos).

Não discriminação
Proibição do uso para fins discriminatórios, ilícitos ou abusivos.

MOLINA ADVOGADOS

5

NORMAS SETORIAIS APLICÁVEIS ÀS FINTECHS

O setor financeiro é extremamente regulado, em vista das atividades realizadas pelos participantes desse ecossistema. Antes do advento da LGPD, já existiam regramentos setoriais tratando sobre sigilo de dados e segurança cibernética no mercado financeiro.

A LGPD não revogou referidos diplomas, os quais permanecem vigentes e devem ser interpretados de forma harmônica com a LGPD. Sempre que houver norma mais específica, esta deverá ser observada, uma vez que a LGPD é ampla e deve ser vista como norte para a aplicação das demais leis.

- **Código Civil Brasileiro:** estabelece a responsabilização em caso de ameaça ou lesão a direito da personalidade, de forma que o infrator tem a obrigação de reparar os danos causados (artigos 12 e 927).
- **Código de Defesa do Consumidor:** estabelece normas de proteção ao consumidor nas relações de consumo. Destacamos que referida lei é aplicável na prestação de serviços financeiros.
- **Marco Civil da Internet ("Lei nº 12.965/2014") e Decreto Regulamentador ("Decreto nº 8.771/2016"):** estabelecem princípios, garantias, direitos e deveres para o uso da Internet no Brasil, com disposições sobre o tratamento de dados no ambiente *online* e medidas de segurança da informação.
- **Lei do Cadastro Positivo:** disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.
- **Lei de Sigilo Bancário:** estabelece o dever de sigilo bancário e as hipóteses de não violação deste sigilo.

MOLINA ADVOGADOS

5

NORMAS SETORIAIS APLICÁVEIS ÀS **FINTECHS**

O setor financeiro é extremamente regulado, em vista das atividades realizadas pelos participantes desse ecossistema. Antes do advento da LGPD, já existiam regramentos setoriais tratando sobre sigilo de dados e segurança cibernética no mercado financeiro.

A LGPD não revogou referidos diplomas, os quais permanecem vigentes e devem ser interpretados de forma harmônica com a LGPD. Sempre que houver norma mais específica, esta deverá ser observada, uma vez que a LGPD é ampla e deve ser vista como norte para a aplicação das demais leis.

- Código Penal Brasileiro: destacamos os crimes contra a inviolabilidade dos segredos, previstos nos artigos 153, 154 e 154-A.
- Lei de Crimes Contra o Sistema Financeiro Nacional (Lei nº 7.492/1986): o conceito de instituição financeira trazido pela lei é amplo e a responsabilidade pode atingir controladores e administradores da instituição.
- Lei de Lavagem de Dinheiro (Lei nº 9.613/1998): dispõe sobre como os dados e informações devem ser tratados e repassados para as autoridades, bem como sobre a manutenção e registro de dados cadastrais.
- Resolução do Conselho Monetário Nacional ("CMN") nº 4.658/2018 e Circular Bacen nº 3.909/2018: tratam sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Bacen.

6

BASES LEGAIS PARA TRATAMENTO

A LGPD prevê as bases legais para que o tratamento de dados possa ser realizado, ou seja, hipóteses em que o tratamento está fundamentado e, portanto, é permitido e regular. Tais bases legais estão previstas no artigo 7º (hipóteses de tratamento de dados pessoais de forma geral), artigo 11 (hipóteses de tratamento de dados pessoais sensíveis) e artigo 14 (hipóteses de tratamento de dados pessoais de crianças e adolescentes).
Diante da natureza dos dados e tratamentos realizados pelas Fintechs, destacamos as bases legais mais relevantes para o setor:

Consentimento do titular dos dados pessoais

Deve haver o aceite pelo titular, esse consentimento deve ser uma manifestação livre, informada e inequívoca.

Cumprimento de obrigação legal ou regulatória pelo controlador

Quando o tratamento é necessário e justificado por uma obrigação legal ou regulatória, por exemplo, determinação em ordem judicial, lei federal, estadual, municipal ou demais normas (decretos, resoluções, entre outros).

Execução de contrato ou de procedimentos preliminares relacionados a contrato

Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato, do qual seja parte o titular, a pedido do titular dos dados. Por exemplo, caso o controlador necessite compartilhar os dados do titular com algum fornecedor para que possa executar o contrato celebrado com o titular, irá se valer desta base legal.

Para o exercício regular de direitos em processo judicial, administrativo ou arbitral

Tratamento dos dados pessoais como elementos para o exercício de direitos em demandas em geral, no curso de processos judiciais, administrativos ou arbitrais.

6

BASES LEGAIS PARA TRATAMENTO

A LGPD prevê as bases legais para que o tratamento de dados possa ser realizado, ou seja, hipóteses em que o tratamento está fundamentado e, portanto, é permitido e regular. Tais bases legais estão previstas no artigo 7º (hipóteses de tratamento de dados pessoais de forma geral), artigo 11 (hipóteses de tratamento de dados pessoais sensíveis) e artigo 14 (hipóteses de tratamento de dados pessoais de crianças e adolescentes).
Diante da natureza dos dados e tratamentos realizados pelas Fintechs, destacamos as bases legais mais relevantes para o setor:

Para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais

deve ser observado com cautela o uso do interesse legítimo como base legal para o tratamento de dados a ser realizado por terceiros, que não somente o controlador. O tratamento de dados com base no interesse legítimo pode ser realizado apenas para finalidades legítimas do controlador, devendo estar dentro da expectativa do titular, ademais, só poderão ser tratados os dados estritamente necessários.

Proteção do crédito, inclusive quanto ao disposto na legislação pertinente

os dados pessoais podem ser tratados para avaliação de crédito (sobre adimplência ou inadimplência), a fim de se tomar decisão acerca da concessão ou não do crédito. Importante neste ponto também observar a Lei do Cadastro Positivo e o Código de Defesa do Consumidor. Deverão ser fornecidos ao titular esclarecimentos sobre a fonte dos dados considerados na avaliação, bem como sobre as informações pessoais valoradas.

MOLINA ADVOGADOS

7

DIREITOS DOS TITULARES DOS DADOS PESSOAIS

A LGPD e leis setoriais estabelecem diversos direitos aos titulares de dados, que devem ser garantidos pelas Fintechs ao tratarem dados pessoais.

- Confirmar a existência de tratamento.
- Acesso aos dados.
- Correção dos dados.
- Anonimização, bloqueio ou eliminação dos dados desnecessários ou excessivos.
- Portabilidade dos dados a outro fornecedor.
- Revogação do consentimento.
- Informação sobre entidades com as quais o controlador realizou o uso compartilhado dos dados.
- Informação sobre a possibilidade de não fornecer o consentimento e consequências (consentimento granular).
- Eliminação dos dados pessoais tratados.
- Revisão de decisão automatizada.

MOLINA ADVOGADOS

8 DA SEGURANÇA E BOAS PRÁTICAS

Elencamos alguns pontos que devem ser observados pelos agentes de tratamento:

- Estudo da LGPD e demais leis que regulamentam a privacidade.
- Perceber o impacto da LGPD, é importante conscientizar a gerência da entidade para o envolvimento dos demais colaboradores.
- Implementar medidas de segurança, proteção e privacidade.
- Gerenciar incidentes de segurança e reclamações/solicitações feitas pelos titulares e pela ANPD.
- Preparar workflows de resposta aos direitos dos titulares.
- Listar os processos impactados pela LGPD (mapeamento dos dados e tratamentos realizados).
- Salvaguardar conformidade das entidades colaboradoras.
- Promover treinamentos internos para conscientização dos colaboradores, com o objetivo de otimizar a adaptação às novas políticas de proteção de dados e criar uma cultura interna de proteção de dados.
- Revisão de contratos, elaboração de minutas, políticas e protocolos adequados à LGPD.
- Monitoramento dos processos.
- Adaptar processos de coleta e tratamento de dados: implementar os conceitos de *"Privacy by design"* e *"Privacy by default"*.

MOLINA ADVOGADOS

O setor das Fintechs deve observar as normas de proteção de dados pessoais, tendo em vista que tratam dados pessoais, sigilosos, dados financeiros, dentre outros dados, de forma intensiva. Destacamos que, além da LGPD, que já está em vigor, as demais leis setoriais mencionadas neste Manual são aplicáveis e devem ser cumpridas pelas Fintechs.

Assim, as Fintechs devem implementar programas de *compliance* com as normas de proteção de dados, adotando medidas de segurança, técnicas e administrativas aptas a proteger esses dados, sempre que possível adotando os mecanismos de *privacy by design* (adotar medidas protetivas desde a fase de concepção do produto ou do serviço até a sua execução) e *privacy by default* (para os produtos e serviços disponibilizados ao público, deverão ser aplicadas por padrão as configurações mais seguras de privacidade).

9 CONSIDERAÇÕES FINAIS

MOLINA ADVOGADOS

MOLINA
ADVOGADOS

molina.adv.br

55 11 3151-3606

/molina.advogados

/molinaadvogados

/molina-&-advogados-associados

AUTORIA: EQUIPE DE PROTEÇÃO DE DADOS (AMANDA DE OLIVEIRA GOMIDE ALBIERI & CAMILA MARIA DE MOURA VILELA)