GUIA PRÁTICO SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

ÍNDICE

abecs

1 INTRODUÇÃO

A Lei nº 13.709/18, conhecida como Lei Geral de Proteção de Dados ("LGPD"), trará um avanço importante para o Brasil ao criar um sistema de proteção de dados pessoais e tutelar questões relacionadas à privacidade e sua compatibilização com outros direitos fundamentais.

Antes da LGPD, questões relacionadas a sigilo e a dados pessoais existiam apenas em leis esparsas e setoriais (como a Constituição Federal, o Código Civil, o Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei Complementar nº 105, a Lei de Acesso à Informação, a Lei do Cadastro Positivo, entre outras). A LGPD regula a matéria de forma abrangente, aplicando-se a todas as atividades de tratamento, independentemente do meio, e estabelece diversos direitos para as pessoas físicas (chamadas de "titulares") sobre o uso de seus dados pessoais, bem como deveres para os setores público e privado que realizam o tratamento de dados pessoais.

O uso de dados pessoais é comum e indissociável de diversas atividades empresariais e sociais. Tanto o poder público como o setor privado – incluindo o mercado de meios de pagamento – devem observar os princípios e as regras estabelecidos pela LGPD.

São fundamentos da proteção a dados pessoais, além do respeito à privacidade e da intimidade, o desenvolvimento econômico e tecnológico, a inovação, a livre concorrência e a livre iniciativa. A LGPD reconhece a relevância desses direitos essenciais para o exercício de atividades econômicas e para o desenvolvimento do bem-estar da própria sociedade. A LGPD não almeja impedir atividades de tratamento, mas sim regular como elas podem ser realizadas de forma equilibrada.

A LGPD se aplica quando: (i) os dados pessoais são coletados no Brasil; (ii) o tratamento de dados pessoais é realizado no Brasil; e (iii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional.

Por outro lado, a LGPD não se aplica: (i) em casos em que dados pessoais, provenientes e destinados a um mesmo país e que apenas transitem pelo Brasil, não sejam tratados e/ou compartilhados em território nacional; (ii) quando o tratamento dos dados pessoais for realizado por pessoas naturais para uso pessoal e não econômico; (iii) para fins jornalísticos e artísticos; (iv) para fins acadêmicos; e (v) para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais.

Além disso, a LGPD criou a Autoridade Nacional de Proteção de Dados Pessoais ("ANPD"), órgão federal que tem a missão de regulamentar, fiscalizar, aplicar sanções, interpretar a lei e definir critérios sobre a proteção de dados pessoais.

O objetivo deste Guia é abordar, de forma sucinta e prática, a aplicação das bases legais de tratamento de dados pessoais previstas na LGPD no contexto das atividades mais recorrentes do mercado de meios eletrônicos de pagamento. Entretanto, o material não é vinculante para os associados da ABECS e busca apenas contribuir para a avaliação e a aplicação da LGPD para situações específicas desse mercado.

2 CONCEITOS IMPORTANTES

Em primeiro lugar, para entender a aplicação da LGPD no contexto das atividades do setor de meios de pagamento, é importante conhecer alguns **termos definidos** pela lei:

- **Dado pessoal:** é a informação relacionada a uma pessoa física identificada ou identificável, ou seja, qualquer informação que identifique ou possa identificar uma pessoa natural, tal como nome números e códigos de identificação, endereços, perfil de consumo, histórico de transação, etc. O conceito de dado pessoal é amplo, mas nem toda informação é dado pessoal, sendo necessário avaliar o dado tratado e o contexto do tratamento.

- **Dado pessoal sensível:** é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa física. Por serem dados ligados à intimidade da pessoa, com potencial discriminatório, a lei traz um maior grau de proteção e exigências específicas para o tratamento de dados pessoais sensíveis.

- **Dado anonimizado:** é o dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. O dado anonimizado está excluído do escopo de aplicação da LGPD.

- **Titular:** é a pessoa física a quem se referem os dados pessoais que são objeto de tratamento.

- **Controlador:** é a pessoa natural ou jurídica, de direito público ou privado, que toma as decisões referentes ao tratamento de dados pessoais. Dentro desse conceito, em determinadas situações os mesmos dados pessoais poderão ter mais de um controlador.

- **Operador:** é a pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, devendo seguir rigorosamente as suas instruções.

- **Agentes de tratamento:** o controlador e o operador são considerados agentes de tratamento.

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

- **Uso compartilhado de dados:** refere-se à comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

- **Encarregado:** é a pessoa indicada pelo controlador e/ou pelo operador para atuar como canal de comunicação entre o controlador, os titulares de dados pessoais e a ANPD. A identidade e as informações de contato do encarregado deverão estar disponíveis de forma simples e facilmente acessíveis.

3 PRINCÍPIOS

Além dos conceitos e termos indicados acima, a LGPD estabelece **princípios**, tais como os da **finalidade, transparência segurança e necessidade, adequação, livre acesso, qualidade, prevenção, não discriminação, responsabilização e prestação de contas**, que devem ser sempre respeitados em todas as atividades de tratamento de dados.

Em resumo, os dados pessoais devem ser tratados para **propósitos legítimos** e **específicos**, com **informações claras** e **facilmente acessíveis** aos titulares. O titular deve ter **livre acesso** aos seus dados pessoais e às **informações** sobre o seu tratamento.

O tratamento de dados pessoais deve ser **adequado** e limitado ao **mínimo necessário** para o cumprimento da **finalidade** estipulada pelo controlador. Cabe aos agentes de tratamento adotar **medidas de segurança** para proteger os dados pessoais (de acessos não autorizados e situações ilícitas ou acidentais de destruição, perda, alteração, comunicação ou difusão, entre outras), e **prevenir** a ocorrência de danos em decorrência do tratamento de dados pessoais. Também cabe aos agentes de tratamento demonstrar que as **medidas adotadas são eficazes** e capazes de proteger os dados pessoais.

4 BASES LEGAIS PREVISTAS NA LGPD PARA TRATAMENTO DE DADOS PESSOAIS

Todo tratamento de dados pessoais deve ser realizado de acordo com ao menos uma das bases legais previstas na LGPD. Ao todo são **10 (dez) bases legais para o tratamento de dados pessoais comuns e 8 (oito) bases legais específicas para o tratamento de dados pessoais sensíveis.**

Um ponto extremamente importante: **o consentimento do titular é apenas uma das bases legais previstas.**

Não há diferença hierárquica entre as bases legais. Isso significa que há outras bases legais extremamente importantes, especialmente para o setor de meios de pagamento, e que fundamentam grande parte dos tratamentos realizados. Por exemplo, o cumprimento de obrigação legal e regulatória, a execução de contrato ou de procedimentos preliminares relacionados a contrato com o titular, proteção do crédito,

o legítimo interesse e o exercício regular de direito em processo judicial, administrativo ou arbitral.

O mais importante é avaliar, no caso concreto, o tratamento realizado para verificar qual é o embasamento legal mais adequado. Devem ser levados em consideração: (i) o contexto; (ii) o tipo de dado pessoal tratado; e (iii) quem realiza o tratamento. Logo, para cada finalidade distinta é necessário indicar a base legal mais apropriada.

A LGPD traz, ainda, regras sobre o tratamento de **dados pessoais de acesso público e/ou tornados manifestamente públicos pelo titular.** Como regra, o tratamento de dados pessoais cujo acesso seja público ou que tenham sido tornados manifestamente públicos pelo titular dispensa o consentimento para o seu tratamento. Tais dados devem observar a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização. Ainda, a LGPD expressamente prevê a possiblidade de tratamento posterior de dados pessoais de acesso público e/ou manifestamente tornados públicos pelo titular para novas finalidades, desde que: (i) o propósito seja legítimo e específico para o novo tratamento e (ii) os direitos do titular, os fundamentos e os princípios da LGPD sejam respeitados. Note-se que o tratamento de dados pessoais de acesso público ou tornados manifestamente públicos pelo titular não dispensa o enquadramento em uma base legal apropriada. Desse modo, ainda que o consentimento não seja necessário no caso do tratamento desses dados, mesmo assim é imprescindível basear o tratamento em uma das outras bases legais previstas na LGPD.

Por fim, o tratamento de **dados pessoais de crianças** (menores de 12 anos) também deve seguir regras específicas e merecem maior atenção e cuidado, pois a LGPD prevê que o tratamento desses dados só pode ocorrer mediante consentimento específico fornecido por pelo menos um dos pais ou responsáveis, ou, caso aplicado, mediante o enquadramento em uma das bases legais apresentadas (por exemplo, cumprimento de obrigação legal ou regulatória).

Abaixo, segue uma breve explicação das principais bases legais previstas na LGPD para o tratamento de dados pessoais no mercado de meios de pagamento.

Cumprimento de obrigação legal ou regulatória pelo controlador

Tratamentos de dados pessoais podem decorrer de obrigação legal ou regulatória, mesmo que a norma não indique especificamente os dados pessoais a serem tratados ou a atividade de tratamento em si - como é o caso de diversas normas do Conselho Monetário Nacional ("CMN") e do Banco Central do Brasil - ("Banco Central") - sobre gerenciamento de riscos e política de segurança cibernética). Deve ser sempre observada, de toda forma, a finalidade do tratamento. Também há atividades que, se realizadas por instituições financeiras e/ou instituições de pagamento, estão sujeitas a normas específicas (como no caso da cessão de crédito, do cadastro de clientes, da portabilidade etc.).
Como o mercado eletrônico de meios de pagamento é altamente regulado, diversos são os tratamentos de dados pessoais baseados em cumprimento de obrigações legais ou regulatórias pelo controlador, como o cumprimento de: (i) divulgação de dados

pessoais aos órgãos reguladores; (ii) normas sobre cadastro de clientes; (iii) normas sobre atendimento a clientes; (iv) normas específicas de cada arranjo de pagamento (as atividades necessárias para que seja implantada a interoperabilidade entre os arranjos, por exemplo), entre outras. Ou seja, tais tratamentos não dependem do consentimento do titular dos dados.

Com relação às normas relativas aos arranjos de pagamento, a Lei nº 12.865 de 9 de outubro de 2013 ("Lei 12.865/13"), em seu art. 9º, dá a competência ao Banco Central, nos termos das diretrizes do Conselho Monetário Nacional para disciplinar e fiscalizar os arranjos de pagamento, bem como seus instituidores e participantes. Neste sentido, o CMN, na Resolução nº 4.282, de 4 de novembro de 2013 ("Resolução 4.282/13"), estabelece as diretrizes que devem ser observadas na supervisão e na fiscalização dos arranjos de pagamento, os quais são disciplinados pelas bandeiras (instituidoras do arranjo).

Por sua vez, o Banco Central definiu as principais obrigações de instituidores de arranjos de pagamento, conforme o Regulamento anexo à Circular do Banco Central nº 3.862 de 4 de novembro de 2013 ("Circular 3.682/13"), o qual rege a prestação dos serviços de pagamento no âmbito dos arranjos de pagamento integrantes do Sistema de Pagamentos Brasileiro ("SPB"). Portanto, em razão da normatização vigente, os participantes dos arranjos de pagamento integrantes do SPB estão sujeitos às regras previstas nos regulamentos dos arranjos, os quais são submetidos à análise e aprovação do Banco Central e suas disposições são mandatórias para todos os participantes.

Destaca-se que um dos objetivos determinados pelo Banco Central e pelo CMN na regulamentação e na supervisão dos arranjos é a implantação da interoperabilidade entre os arranjos de pagamento (art. 3º da Resolução 4.282/13), tendo como foco a promoção da eficiência e do acesso não discriminatório aos serviços e infraestruturas necessários ao funcionamento dos arranjos de pagamento

O Banco Central determina, no art. 4º da Circular 3.682/13, que os instituidores dos arranjos devem, entre outras obrigações, estabelecer os procedimentos para viabilizar a interoperabilidade com outros arranjos de pagamento, incluindo a previsão de transferência de recursos de um arranjo de pagamento para outro. Por essa perspectiva, deve ser possível aos usuários finais utilizarem uma única conta de depósitos à vista ou de pagamento para realizar pagamentos para usuários de outros arranjos. Portanto, o tratamento dos dados pessoais dos usuários finais se faz necessário para que seja possível viabilizar o fluxo de recursos entre os diferentes arranjos de pagamento.

As principais normas aplicáveis ao setor são as seguintes:

Lei 12.865/13: marco legal dos arranjos de pagamento e das instituições de pagamento.

Resolução 4.282/13: estabelece as diretrizes que devem ser observadas na regulamentação, na vigilância e na supervisão das instituições de pagamento e dos arranjos de pagamento integrantes do SPB, de que trata a Lei 12.865/13[1].
Circular do Banco Central nº 3.680, de 4 de novembro de 2013 ("Circular 3.680/13"): dispõe sobre a conta de pagamento utilizada pelas instituições de pagamento para registro de transações de pagamento de usuários finais e para cadastro.

1 Note-se que esta norma sujeita as instituições de pagamento e as instituições de pagamento aos termos da Lei Complementar 105/01.

Circular do Banco Central nº 3.681, **de 4 de novembro de 2013**: dispõe sobre o gerenciamento de riscos, os requerimentos mínimos de patrimônio, a governança de instituições de pagamento, e a preservação do valor e da liquidez dos saldos em contas de pagamento.

Circular 3.682/13: aprova o regulamento que disciplina a prestação de serviço de pagamento no âmbito dos arranjos de pagamentos integrantes do SPB, estabelece os critérios segundo os quais os arranjos de pagamento não integrarão o SPB e dá outras providências.

Circular do Banco Central nº 3.885, **de 26 de março de 2018:** estabelece os requisitos e os procedimentos para autorização de funcionamento, alteração de controle e reorganização societária, cancelamento da autorização para funcionamento, condições para o exercício de cargos de administração nas instituições de pagamento e autorização para a prestação de serviços de pagamento por instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Lei 9.613, de 3 de março de 1998 e Circular do Banco Central nº 3.641, de 24 de julho de 2009: normas sobre prevenção da utilização do sistema financeiro para os ilícitos de lavagem de dinheiro.

Resolução CMN nº 3.694, de 26 de março de 2009[2]: dispõe sobre prevenção de riscos e a adequação dos produtos e serviços ofertados ou recomendados às necessidades, interesses e objetivos dos clientes e usuários.

Resolução CMN nº 2.554, de 29 de setembro de 1998: dispõe sobre a implantação de sistema de controles internos.

Resolução CMN nº 4.658, de 26 de abril de 2018 e Circular do Banco Central nº 3.909, de 16 de agosto de 2018: dispõem 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.

Execução de contrato ou de procedimentos preliminares ao contrato

Esta base legal é aplicável para os tratamentos de dados pessoais necessários para a execução de contrato ou para procedimentos preliminares relacionados a contrato do qual seja parte o titular, ou a pedido do titular dos dados. Essa base legal inclui os tratamentos que decorrem da relação jurídica contratual, como as atividades de cadastro após uma contratação, de avaliação de crédito, de processamento das transações de cartão de débito e crédito, e de cobrança, entre outros.

Lembramos que, para a avaliação de crédito ser adequadamente enquadrada nesta base legal, essa avaliação deverá ser necessária para a contratação, como é o caso dos cartões de crédito, em que é preciso estabelecer um limite de crédito. Com isso, esse tratamento pode ser enquadrado na definição de "procedimentos preliminares" ao contrato que será firmado com a instituição.

2 Revogada a partir de outubro de 2020, quando passará a vigorar a Circular do Banco Central nº 3.978, de 23 de janeiro de 2020.

Consentimento

O consentimento é definido como "*a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para finalidades determinadas*". O titular pode revogar o consentimento a qualquer momento.

Há diversos requisitos a serem observados no caso de consentimento:

- As finalidades devem ser determinadas e as informações sobre o tratamento devem ser apresentadas com transparência ao titular, pois o consentimento pode ser considerado nulo nos casos em que for baseado em: (a) autorizações genéricas para tratamento; (b) informações enganosas ou abusivas relativas ao tratamento; ou (c) informações não disponíveis ao titular.
- O consentimento deve ser fornecido por qualquer meio que demonstre, de modo inequívoco, a vontade do titular. Caso o consentimento seja fornecido por escrito, deverá ser obtido por meio de cláusula destacada das demais cláusulas contratuais.
- Não deve haver dúvidas de que o titular consentiu por livre e espontânea vontade.

É importante lembrar que, se houver alteração com relação ao tratamento de dados, por exemplo, sua finalidade, caberá ao controlador informar previamente ao titular dos dados as novas características do tratamento, pois o titular poderá a seu critério revogar o consentimento, caso não concorde com as alterações.

Proteção do crédito

Os tratamentos de dados pessoais que têm por finalidade a proteção do crédito e do sistema financeiro podem ser enquadrados nesta base legal.

Esta base legal é uma criação da lei brasileira e não tem equivalência na legislação de outros países, o que dificulta sua interpretação e principalmente a extensão de sua aplicabilidade. Em linhas gerais, parece defensável que a inclusão do titular em cadastros de devedores inadimplentes e consultas a informações do Cadastro Positivo são atividades de tratamento que podem ser realizadas com fundamento na base legal de proteção do crédito.

Outros exemplos que, eventualmente, poderão ser enquadrados são a definição e o gerenciamento de limites de crédito, a cobrança de operações de crédito, a cessão de crédito, a inclusão do titular em cadastros de devedores inadimplentes, o desenvolvimento ou consulta a scores e informações de bureaux de crédito, consultas a informações do Cadastro Positivo, a constituição e execução de garantias.

Legítimo interesse do controlador ou de terceiro

O tratamento de dados pessoais também poderá ser realizado quando identificado o legítimo interesse do controlador ou de terceiros (como outro controlador, parceiros de negócio, outro setor ou a própria sociedade), quando não prevalecerem os direitos e as liberdades fundamentais do titular.

A LGPD traz um rol não taxativo de hipóteses em que pode ser aplicável o legítimo interesse, como

- o apoio e a promoção de atividades do controlador (como no caso de oferta e melhoria de produtos e serviços);
- a proteção, em relação ao titular dos dados, do exercício regular dos direitos ou a prestação de serviços que o beneficiem, respeitadas as legítimas expectativas do titular dos dados.

De toda maneira, para verificar se essa base legal pode ser utilizada no caso concreto, é recomendável aplicar um teste de três partes para identificar a finalidade, a necessidade e a proporcionalidade (equilíbrio do interesse com os direitos e as liberdades fundamentais). Esse teste deve, preferencialmente, ser consolidado em uma avaliação da aplicabilidade do legítimo interesse (também conhecido como LIA – Legitimate Interest Assessment).

Essa avaliação poderá fazer parte do relatório de impacto sobre a proteção de dados pessoais que pode ser solicitado ao controlador pela ANPD no caso de tratamentos baseados em legítimo interesse.

Exercício regular de direitos em processos administrativos, judiciais e arbitrais

Essa base legal autoriza os tratamentos de dados pessoais realizados para o exercício regular de direitos em processo judicial, administrativo ou arbitral, existente ou futuro. Por exemplo, a retenção de dados pessoais pode ser realizada em muitos casos para possível utilização em demandas judiciais futuras.

Outras bases legais previstas na LGPD que autorizam o tratamento de dados pessoais são:

- **pela administração pública, para a execução de políticas públicas;**
- **para a realização de estudos por órgãos de pesquisa** (entidade pública ou privada, sem fins lucrativos, que inclua em sua missão ou objeto a pesquisa histórica, científica, tecnológica ou estatística e altamente recomendável, utilizando técnicas de anonimização dos dados);
- para **proteção da vida ou da incolumidade física** do titular ou de terceiros;
- para a **tutela da saúde**, exclusivamente em tratamentos por profissionais de saúde, serviços e saúde ou autoridades sanitárias.

Bases legais para o tratamento de dados pessoais sensíveis

As bases legais para o tratamento de dados pessoais sensíveis são mais restritas e não incluem, por exemplo, a proteção do crédito e o legítimo interesse. Os dados pessoais sensíveis podem ser tratados com base em consentimento específico e destacado, ou também com fundamento em outras bases legais, quando o tratamento for considerado indispensável. As bases legais que permitem o tratamento de dados pessoais sensíveis são:

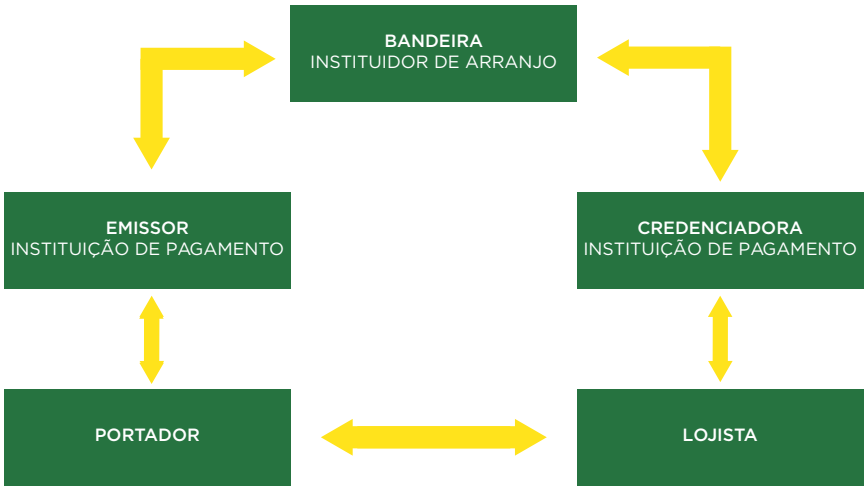
- **consentimento;**
- o cumprimento de **obrigação legal ou regulatória** pelo controlador;

- **pela administração pública, para a execução de políticas públicas;**
- **para a realização de estudos por órgãos de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- para **proteção da vida ou da incolumidade física** do titular ou de terceiros;
- para a **tutela da saúde**, exclusivamente em tratamentos por profissionais de saúde, serviços e saúde ou autoridades sanitárias;
- **exercício regular de direitos, inclusive em contratos**, e em processo judicial, administrativo e arbitral; e
- **para garantia da prevenção à fraude e da segurança do titular,** nos processos de **identificação e autenticação de cadastro em sistemas eletrônicos,** resguardados os direitos do titular.

5 MERCADO DE MEIOS ELETRÔNICOS DE PAGAMENTO

Destacamos abaixo os principais participantes do mercado de meios de pagamento para que possamos, em seguida, avaliar o enquadramento de situações corriqueiras no processamento de transações de pagamento nas bases legais previstas na LGPD.

ESTRUTURA DE SETOR



Portador: é o portador do instrumento de pagamento (crédito, débito ou pré-pago). No caso do cartão de crédito, o portador possui um limite de crédito pré-aprovado pelo emissor do cartão (banco ou outras instituições que emitem cartão). O portador pessoa física é um titular de dados pessoais para fins da LGPD.

Lojista: é o estabelecimento comercial ou pessoa física que aceita instrumentos de pagamento emitidos sob arranjos de pagamento para a oferta de produtos e serviços, podendo ser uma loja física ou online. O lojista é considerado um controlador de dados na sua relação direta com o portador do cartão.

Emissor: é uma instituição financeira ou instituição de pagamento responsável pela emissão dos instrumentos de pagamento e, quando aplicável, por oferecer crédito ao portador do cartão do crédito. O emissor é considerado um controlador de dados na sua relação direta com o portador do cartão.

Credenciadora: é uma instituição financeira ou instituição de pagamento que credencia o lojista para o aceite dos meios eletrônicos de pagamento, sendo

responsável por capturar, processar e liquidar a transação. A credenciadora não entra em contrato direto com o portador do cartão, mas sim com o lojista, que pode, também, ser uma pessoa física. Entretanto, o portador do cartão é beneficiado pelos serviços da credenciadora ao utilizar seu instrumento de pagamento para realizar a transação de compra.

Bandeira: é a instituidora do arranjo de pagamento, responsável pela organização, estruturação, fiscalização e normas operacionais e de segurança necessárias ao funcionamento do arranjo de pagamento. A bandeira, em regra, não tem relação direta com o portador ou com o lojista, mas estes se beneficiam do sistema da bandeira, que inclui também a participação dos outros players, como o emissor e a credenciadora.

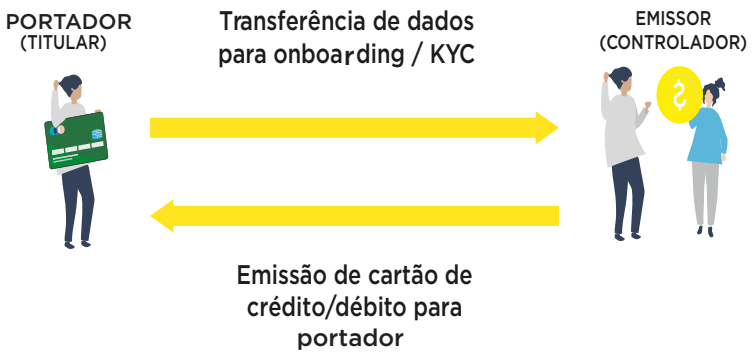
Subcredenciador: participante do arranjo de pagamento, que pode adotar diversos modelos de negócio, habilitando usuários finais recebedores para o aceite do instrumento de pagamento emitido por instituição de pagamento ou por instituição financeira participante de um mesmo arranjo de pagamento, mas que não participa do processo de liquidação das transações de pagamento como credor perante o emissor.

6 BASES LEGAIS SOBRE SITUAÇÕES ESPECÍFICAS DO MERCADO DE MEIOS ELETRÔNICOS DE PAGAMENTO

Abaixo indicamos alguns fluxos relativos a situações específicas do mercado de meios de pagamento eletrônico, com avaliação acerca das possíveis bases legais para fundamentar os respectivos tratamentos dos dados pessoais envolvidos.

É importante ressaltar que as bases legais podem ser distintas a depender de quem realiza o tratamento dos dados pessoais e em que condição (de controlador ou operador). Assim, ainda que haja indicação das possíveis bases legais para cada uma das situações abaixo, é necessário avaliar qual participante da cadeia de meios de pagamento realiza determinado tratamento, para o enquadramento da base legal em relação a tal participante.

A) Relação entre emissor e portador – *onboarding* e KYC



O emissor é o responsável pela emissão dos instrumentos de pagamento e por oferecer crédito ao portador, bem como é quem tem relação direta com o portador. Nesse contexto, há tratamento de dados pessoais do portador do cartão (titular e cartões adicionais) por parte do emissor.

Proposta do cartão: o tratamento de dados pessoais dos portadores no contexto da proposta do cartão é fundamentado em uma das bases legais abaixo mencionadas abaixo mencionadas, observando cada caso:

- **Execução de contrato ou de procedimentos preliminares relacionados ao contrato com o titular;** com relação aos tratamentos de dados pessoais relativos à elaboração do contrato, incluindo análise de crédito para estabelecer o limite do portador;
- **Proteção do crédito** com relação à avaliação; à definição dos limites de crédito, no caso de cartão de crédito;
- **Legítimo interesse** quando o tratamento é feito com o objetivo de prospectar clientes e, para isso, o emissor possuir ou gerar lista de valores de crédito pré-aprovado dos clientes em potencial ("prospects"); e
- **Cumprimento de obrigação legal e regulatória**, especialmente em relação às normas de cadastro (Circular 3.680/13) e processos de prevenção à lavagem de dinheiro (Circular 3.461/09) e fraudes (Resolução CMN 3.694, sobre prevenção de riscos e a adequação dos produtos e serviços ofertados ou recomendados às necessidades, interesses e objetivos de clientes e usuários).

Atividades de PLD – prevenção à lavagem de dinheiro, KYC – *Know Your Customer*, fraude e segurança:

- **Cumprimento de obrigação legal e regulatória** (normas relacionadas a PLD e fraude, referidas acima); e
- **Garantia de prevenção à fraude e à segurança do titular em processos de autenticação e identificação e cadastro em sistemas eletrônicos** para os casos em que há o uso de dados biométricos do titular, no contexto da utilização de sistemas eletrônicos, informatizados, online e similares.

Cadastro e *onboarding*:

Os tratamentos de dados pessoais dos portadores no contexto do cadastro, onboarding e demais atividades relacionadas (como entrega do cartão, envio da fatura etc.), desde que observado cada caso, são necessários para:

- **Cumprimento de obrigação legal ou regulatória** pelo emissor (normas sobre cadastro, prevenção a fraudes, atendimento, disponibilização da fatura e cumprimento de outras obrigações legais);
- **Execução de contrato ou de procedimentos preliminares relacionados ao contrato com o titular**; para entrega do cartão, envio da fatura etc.; e
- **Garantia de prevenção à fraude e à segurança do titular em processos de autenticação e identificação e cadastro em sistemas eletrônicos** para os casos em que há o uso de dados biométricos do titular, no contexto da utilização de sistemas eletrônicos, informatizados, online e similares.

Limite de crédito:

A definição de limite de crédito, no caso de cartão de crédito, é baseada em:

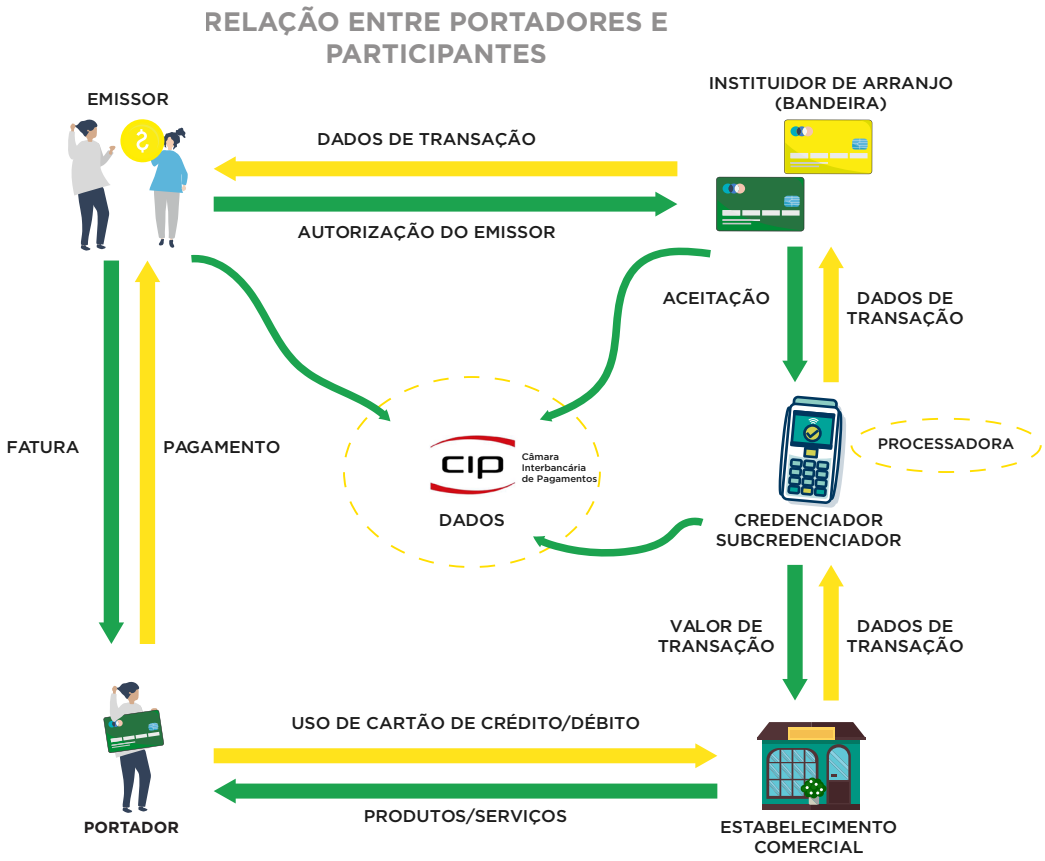
- **Cumprimento de obrigação legal e regulatória** (normas relacionadas à definição de limites e ao gerenciamento do risco de crédito);
- **Execução de contrato ou de procedimentos preliminares relacionados ao contrato com o titular**, com relação à análise de crédito para estabelecer o limite do portador no curso do contrato;
- **Legítimo interesse** com relação à avaliação e definição dos limites de crédito quando o tratamento é feito com o objetivo de prospectar clientes e, para isso, o emissor possuir ou gerar lista de valores de crédito pré-aprovado dos clientes em potencial ("*prospects*"); e
- **Proteção do crédito.**

Contratação de seguros atrelados ao cartão, ofertados pelo emissor:

- **Execução de contrato** com relação à contratação do seguro.
- **Legítimo interesse** com relação às atividades de prospecção para contratação de seguros.

B) Relação entre portador e participantes

FLUXO DE TRANSAÇÃO



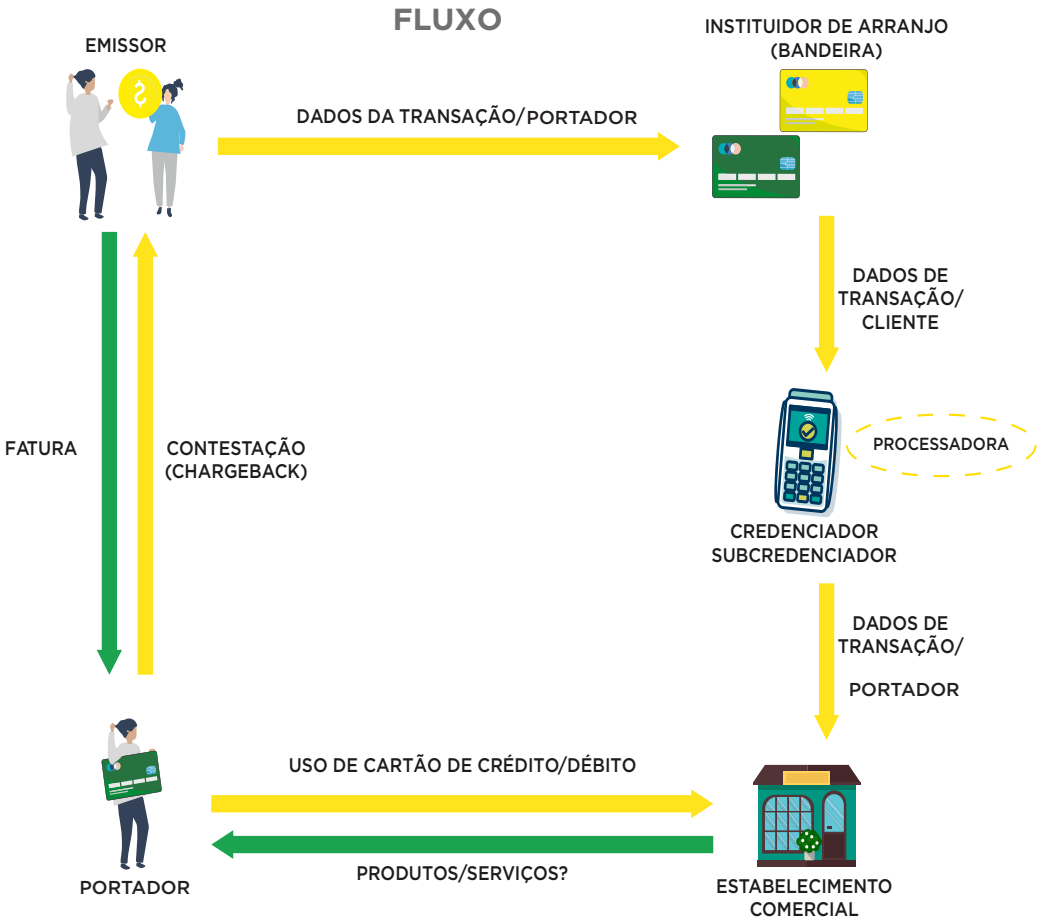
Há diversas etapas envolvidas no fluxo de uma transação com instrumento de pagamento. Avaliamos a possibilidade de enquadramento em bases legais das principais atividades envolvidas nesse fluxo.

Aprovação da transação pelo emissor: o emissor /instituição de pagamento, ao receber as informações da transação capturada pela credenciadora no lojista, avalia: (a) se há limite de crédito disponível (no caso de cartão de crédito); e (b) se há saldo na conta-corrente (no caso de cartão de débito) ou fundos na conta de pagamento (no caso de cartão pré-pago), além de realizar a verificação de fraude, para, então, aprovar a transação. Esses tratamentos são necessários para:

- **Execução de contrato**, visto se tratar de uma das atividades centrais do contrato existentes entre emissor e portador;
- **Cumprimento de obrigação legal** com relação à verificação de fraude e também ao gerenciamento dos riscos operacionais e de crédito (no caso de cartão de crédito);
- **No caso de serviço emergencial de crédito (overlimit)** ofertado por instituições financeiras, a execução de contrato seria igualmente aplicável.

Em geral, a credenciadora e a bandeira possuem acesso à informações sobre o cartão e a transação, mas não possuem informações que possam identificar o portador. Apenas no caso de transações realizadas por meio de e-commerce, a credenciadora poderia visualizar dados pessoais relativos ao portador e à sua compra, pois são dados pessoais necessários para a implementação do pagamento por meio da internet. Assim, quando houver tratamento de dados pessoais as orientações desse guia podem ser observadas.

C) *Chargeback*:



O processo de *chargeback* decorre de uma contestação referente a uma compra com cartão. Via de regra, é o portador quem solicita o chargeback diretamente ao emissor do cartão, sendo que somente o emissor pode, após a análise do fato ocorrido, proceder com o estorno.

Essa contestação poderá resultar no não pagamento do valor pertinente ao produto ou serviço pelo portador do cartão ao emissor ou ainda no estorno do valor do produto ou serviço na fatura do portador.

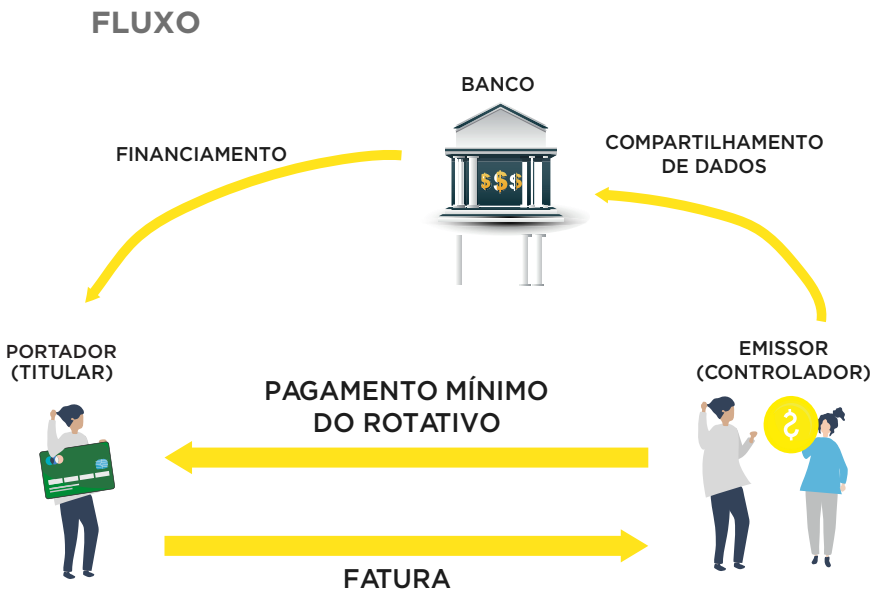
Tal contestação também poderá resultar no não pagamento do valor do produto ou serviço pela credenciadora ao lojista ou ainda no estorno do valor do produto ou serviço, se tal pagamento já tiver sido realizado pela credenciadora.

Em linhas gerais, o chargeback pode ocorrer em determinadas situações, tais como (i) não recebimento de mercadoria; (ii) não realização da transação pelo portador; (iii) erros de processamento, (iv) fraudes, entre outras.

Para que o processo de chargeback seja realizado, é necessário que haja o compartilhamento de informações sobre o portador e a transação entre o emissor, a credenciadora, a subcredenciadora, o lojista e a bandeira e o processo de avaliação do estorno da transação seja concretizado. Nesse contexto, o compartilhamento e a avaliação das informações são necessários e, desde que o dado identifique ou possa identificar o titular, pode ser enquadrado em:

- **Execução de contrato**, visto se tratar de uma das atividades que decorrem do contrato que o portador possui com o emissor;
- **Cumprimento de obrigação legal ou regulatória**, no caso de prevenção a fraudes, quando aplicável; ou quando houver regras obrigatórias ao *chargeback* e reversão de transações.

D) Financiamento da fatura



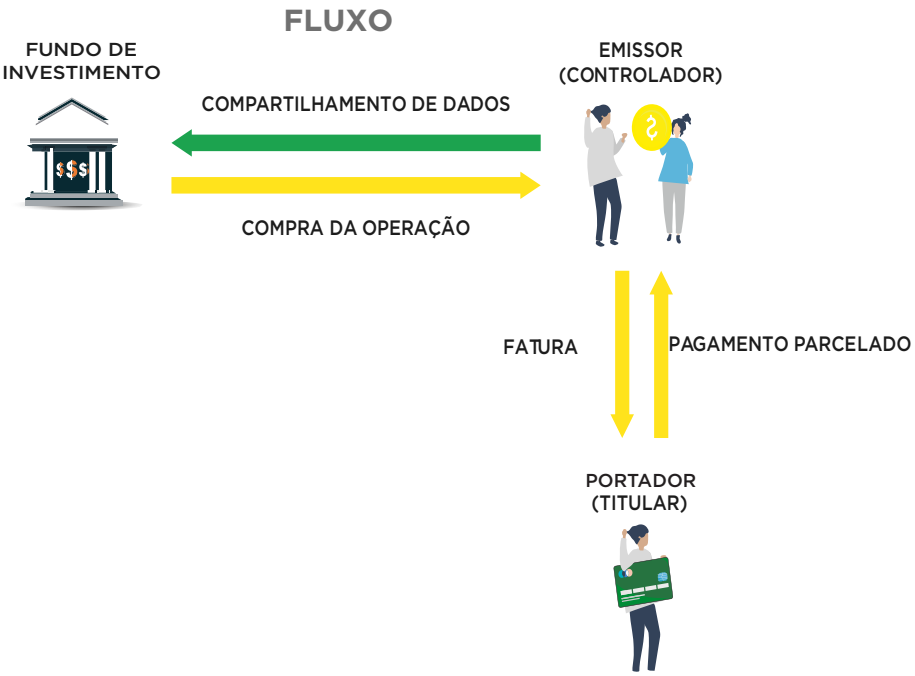
O financiamento do pagamento da fatura de cartão de crédito, quando o emissor é instituição financeira, poderá ser fundamentado nas seguintes bases legais, desde que observado cada caso:

- **Execução de contrato; proteção do crédito;**
- **Obrigação legal**, com relação ao gerenciamento do risco de crédito e observância das regras específicas de financiamento e parcelamento da fatura de cartão de crédito; e com relação ao cadastro de clientes para fins de PLD e prevenção à fraude.

Quando o emissor do cartão depender de uma instituição financeira para realizar o financiamento da fatura do cartão de crédito, as bases legais a serem utilizadas podem ser:

- **Execução de contrato** (tanto o contrato de cartão de crédito como o contrato de crédito firmado entre o portador do cartão e a instituição financeira que realizar o financiamento da fatura);
- **Proteção do crédito**; e
- Cumprimento de **obrigação legal ou regulatória**, no caso da instituição financeira, com relação ao gerenciamento do risco de crédito e observância das regras específicas de financiamento e parcelamento da fatura de cartão de crédito.

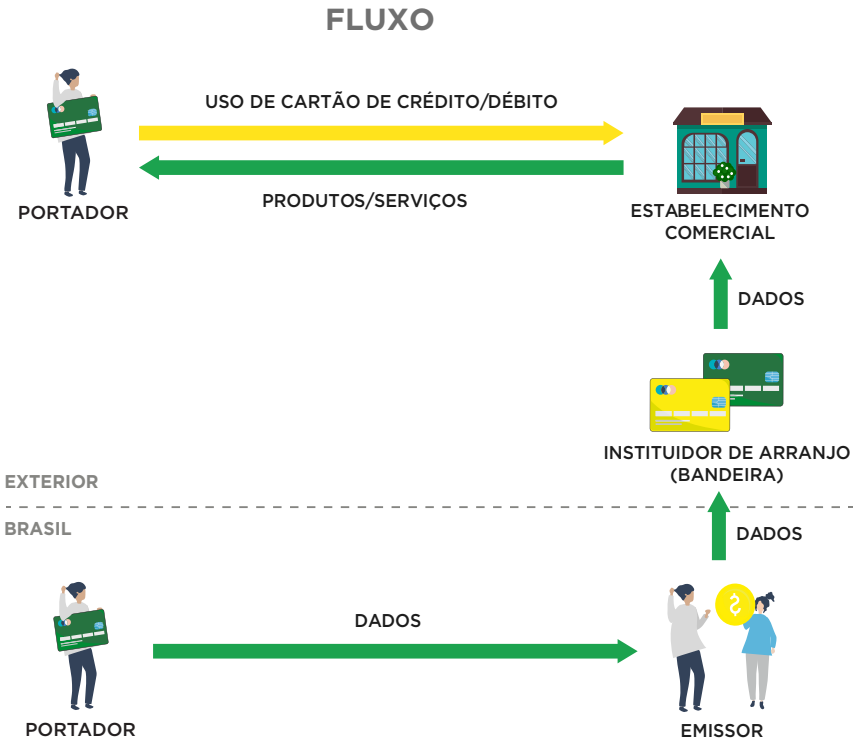
E) Securitização



É muito comum que a instituição financeira ou a instituição de pagamento, credora das operações oriundas do relacionamento com o portador do cartão, realize a cessão dos referidos créditos. A possibilidade de cessão do crédito não exige que haja consentimento do devedor para a sua realização. De qualquer forma, do ponto de vista da LGPD, é possível fundamentar a cessão de crédito nas seguintes bases legais:

- **Proteção de crédito**
- **Legítimo interesse**, por se tratar de atividade ligada ao interesse comercial da instituição financeira ou instituição de pagamento, proteção do crédito; e
- **Cumprimento de obrigação legal ou regulatória**, no que tange ao gerenciamento do risco de crédito e aos procedimentos legais e regulatórios aplicáveis às instituições financeiras e de pagamento que realizam a cessão de crédito.

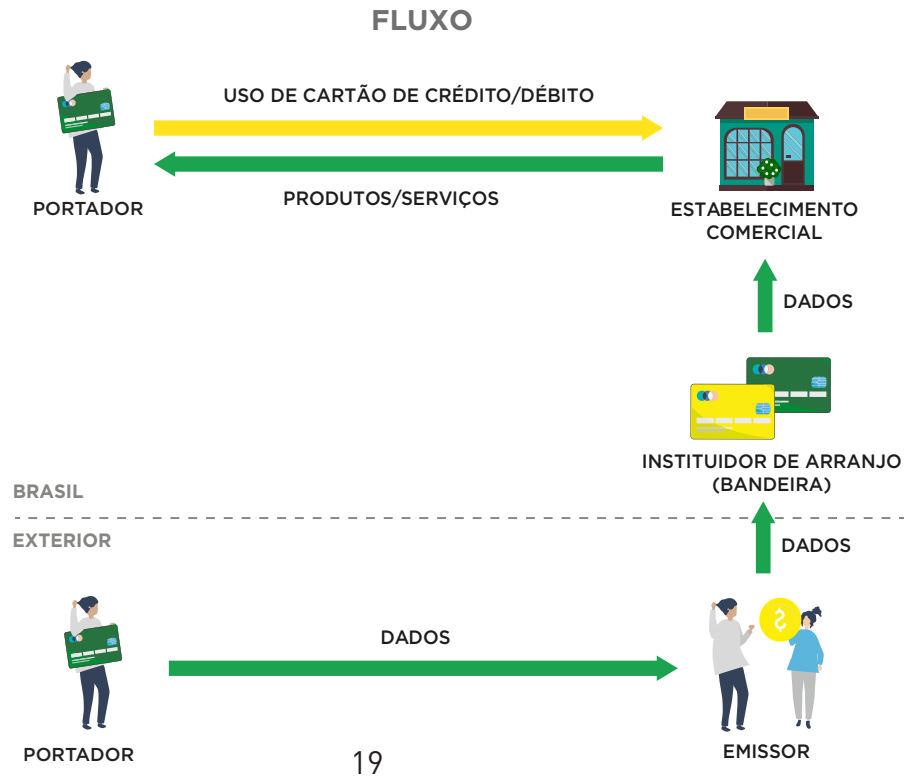
F) Uso do cartão no exterior



Quando o portador do cartão o utiliza no exterior, os tratamentos de dados pessoais necessários para que a referida transação seja liquidada e devidamente paga ao lojista no exterior podem ser justificados por meio da **execução de contrato** como base legal.

Como haverá **transferência internacional** de dados pessoais, um dos possíveis mecanismos de transferência a ser utilizado é a **execução do contrato** e o cumprimento de obrigação legal ou regulatória, ainda que seja possível utilizar, no futuro, cláusulas contratuais modelo estabelecidas pela ANPD.

G) Uso do cartão estrangeiro no Brasil



Quando o cartão de crédito é utilizado no Brasil, como ocorre a coleta de dados no Brasil e há a transferência internacional de dados pessoais para possibilitar a liquidação e o pagamento da transação aqui ocorrida, um dos possíveis mecanismos de transferência a ser utilizado é a execução do contrato e o cumprimento de obrigação legal ou regulatória, ainda que seja possível utilizar, no futuro, cláusulas contratuais modelo estabelecidas pela ANPD.

H) Outras situações

Além dos exemplos mencionados acima, há também outras situações recorrentes no mercado de meios de pagamento, como a oferta de produtos de crédito, atividades de embossing, back office, printers, Correios, o financiamento da fatura (por exemplo, o crédito pessoal para lançamento das prestações no cartão de crédito) e outros serviços e benefícios atrelados ao cartão, como o saque de valores e os programas de recompensas/fidelidade. Os tratamentos relativos a tais situações também devem ser considerados para o respectivo enquadramento nas bases legais respectivas.

7 OUTROS ASPECTOS IMPORTANTES DA LGPD

Destaca-se que a LGPD, ao dispor sobre o tema de transferência internacional de dados pessoais, detalha quais são os requisitos específicos que autorizam a transferência, tais como:

i. Ser para um país considerado adequado pela ANPD;

ii. O controlador oferecer e comprovar as garantias ao cumprimento dos princípios da lei, por meio de:

ii.1 Cláusulas contratuais específicas para determinada transferência;

ii.2 Cláusulas padrão definidas pela ANPD;

ii.3 Normas corporativas globais a serem aprovadas pela ANPD;

ii.4 Selos, certificados e códigos de conduta regularmente emitidos (a serem regulados e definidos pela ANPD);

iii. Quando for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, investigação, persecução, de acordo com os instrumentos do direito internacional;

iv. Quando for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

v. Quando devidamente autorizada pela ANPD;

vi. Quando resultar em compromisso assumido em acordo de cooperação internacional;

vii. Quando for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada a devida publicidade;

viii. Quando houver a obtenção do consentimento do titular;

ix. Para a execução de contrato;

x. Para o cumprimento de obrigação legal ou regulatória; e

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

Há, também, diversas obrigações para os agentes de tratamento. Dentre essas obrigações, destacam-se:

i. O registro das atividades de tratamento de dados pessoais;

ii. A implantação de medidas de segurança adequadas; e

iii. O aviso aos titulares e à ANPD, nos casos de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares.

Além disso, os dados pessoais devem ser mantidos **apenas se houver base legal que justifique o seu tratamento**, pois armazenamento é uma espécie de tratamento de dado pessoal.

A LGPD também estabelece diversos direitos aos titulares, entre os quais destacamos:

i. Confirmação da existência de tratamento;

ii. Acesso aos dados pessoais tratados;

iii. Correção dos dados pessoais;

iv. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;

v. Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa do titular e de acordo com a regulamentação da autoridade nacional; e

vi. Informações sobre o tratamento dos dados.

As penalidades pelo descumprimento da LGPD, a serem aplicadas pela ANPD incluem:

i. Multa, simples e diária, de até 2% (dois por cento) do faturamento da pessoa jurídica, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

ii. Advertência e publicização [divulgação pública] da infração;

iii. Bloqueio ou eliminação de dados pessoais;

iv. Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

v. Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; e

vi. Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Tais penalidades serão aplicadas após procedimento administrativo conduzido pela ANPD que observará o direito de defesa do suposto infrator, e ainda os seguintes critérios e parâmetros:

i. Gravidade e natureza das infrações e dos direitos pessoais afetados;
ii. Boa-fé do infrator;
iii. Vantagem auferida ou pretendida pelo infrator;
iv. Condição econômica do infrator;
v. Reincidência;
vi. Grau do dano;
vii. Cooperação do infrator;
viii. Adoção de mecanismos internos para minimizar o dano;
ix. Adoção de políticas e boas práticas de governança;
x. Pronta adoção de medidas corretivas; e
xi. Proporcionalidade entre a gravidade da falta e a intensidade da sanção.

A aplicação das penalidades previstas na LGPD não exclui outras penalidades (administrativas, civis ou penais) previstas em legislações específicas.

As empresas devem mapear os impactos da LGPD em suas atividades para realizar as adequações necessárias em suas rotinas de negócio em face das novas regras. Nesse sentido, os setores já regulados e acostumados com sigilo, segurança, proteção de dados, governança e compliance, como é o caso do setor financeiro e, especialmente, a indústria de meios de pagamentos, podem e devem aproveitar práticas já adotadas pelo setor para atender à LGPD.

8 BOAS PRÁTICAS DO MERCADO DE MEIOS ELETRÔNICOS DE PAGAMENTO

A LGPD estabelece a possibilidade de as empresas formularem regras de boas práticas e de governança para estabelecer condições para o cumprimento da lei com maior segurança. A vantagem de as empresas possuírem políticas de boas práticas é que a ANPD poderá levá-las em consideração ao avaliar alguma sanção.

O mercado de meios eletrônicos de pagamentos conta com diversas regras que auxiliam cada parte do arranjo de pagamento a seguir regras estritas que garantem boas práticas com relação ao tratamento de dados pessoais, como a Lei Complementar nº 105, entre outras.


abecs