

PINHEIRONETO
ADVOGADOS



Lei Geral de Proteção de Dados (“LGPD”) – Impactos e Desafios para a Indústria de Meios de Pagamento

São Paulo
20 de setembro de 2018

Relevância dos Dados



Regulating the internet giants

The world's most valuable resource is no longer oil, but data

'Data is the new oil': Your personal information is now the world's most valuable commodity

Huge amounts of data are controlled by just 5 global mega-corporations that are bigger than most governments

By Ramona Pringle, CBC News | Posted: Aug 26, 2017 5:00 AM ET | Last Updated: Aug 26, 2017 11:28 AM ET

Fuel of the future

Data is giving rise to a new economy

Relevância dos Dados

1

Disruption

dos serviços tradicionais e migração para solução tecnológicas



2

Internet of Things (IoT)

transmissão de informações entre equipamentos



3

Inteligência Artificial

Inteligência através de mecanismos e software



4

Big data e Data analytics



Relevância dos Dados

Big Data e Data Analytics

- Cerca de 2,5 exabytes (1 milhão de terabytes) de dados são produzidos por dia
- 2,3 milhões de buscas no Google em apenas 1 segundo (100 bilhões de pesquisas por mês)
- **Big Data:** Capacidade de extrair informações de conjunto de dados estruturados e não estruturados
 - E-commerce
 - Transações Bancárias
 - Redes Sociais
 - IoT
 - Mobile Tracking
- **Data Analytics:** Análise massiva de dados em busca de padrões

Relevância dos Dados

Equifax, empresa de crédito dos EUA, sofre ataque hacker e dados de 143 milhões de pessoas são expostos

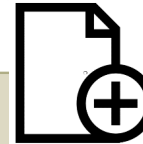
Empresa sofreu ataque no fim de julho e admitiu nesta quinta-feira vazamentos de informações dos usuários.

Uber revela vazamento de dados de 57 milhões de usuários

E-commerce terá de avisar 2 milhões de clientes de vazamento de dados

Falha na segurança da Netshoes libera informações pessoais de clientes a hackers. MP pede rápida ação da empresa

Relevância dos Dados



Resp. 1348532 - STJ

É abusiva cláusula que obriga cliente de cartão de crédito a fornecer dados a terceiros

No momento em que assina contrato de serviços de cartão de crédito, o cliente tem o direito de autorizar ou não o fornecimento de seus dados pessoais e de movimentação financeira a outras empresas, ainda que parceiras da administradora. Por esse motivo, a imposição da autorização em contrato de adesão é considerada abusiva e fere os princípios da transparência e da confiança nas relações de consumo.

Relevância dos Dados

MPF processa Microsoft para que Windows 10 deixe de coletar dados pessoais sem autorização dos usuários

👍 Curtir 176

🔗 Compartilhar

🐦 Tweetar



Opção padrão de instalação do software habilita a transferência de informações sem alertar consumidores; procedimento viola a legislação e representa riscos para a privacidade



O Ministério Público Federal (MPF) entrou com ação contra a Microsoft para impedir que o Windows 10 continue coletando dados pessoais sem o expresso consentimento dos usuários. Atualmente, a opção padrão de instalação e atualização do sistema operacional permite que a empresa obtenha diversas informações sobre os consumidores, como geolocalização, conteúdo de e-mails, hábitos de navegação e histórico de buscas realizadas na internet.

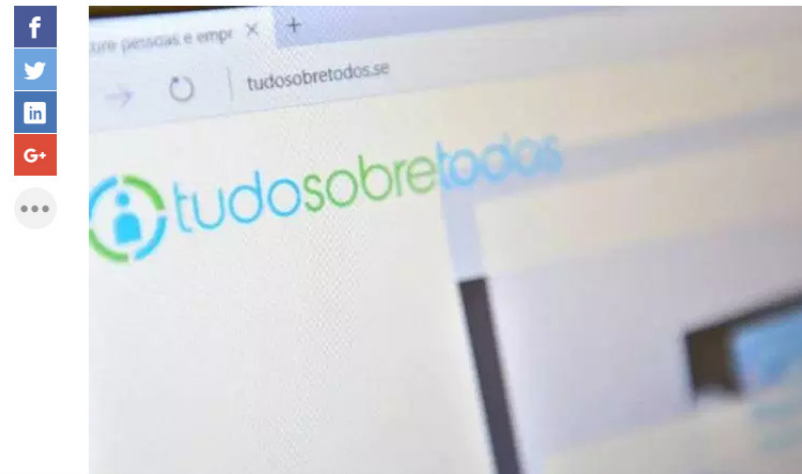
Relevância dos Dados

TECNOLOGIA

MP investiga site que vende seu nome, CPF e endereço

Site Tudo Sobre Todos segue na ativa vendendo ilegalmente dados de brasileiros

Por [Lucas Agreia](#)
© 11 jul 2018, 07h00



Privacidade e Proteção de Dados

O Brasil não tinha uma lei específica que regulamentasse privacidade e proteção de dados pessoais

A privacidade, até então, era protegida de maneira esparsa nas seguintes leis



Constituição
Federal



Código Civil



Código de Defesa
do Consumidor



Marco Civil da Internet
(Lei nº 12.965/2014)



Decreto 8.771/2016

Outras leis aplicáveis:

- Lei de Sigilo Bancário (Lei Complementar nº 105/2001)
- Lei 12.737/2012 (cyber crime)
- Lei 12.414/2011 (Lei do Cadastro Positivo)

Lei Geral de Proteção de Dados Pessoais (LGPD)



SENADO FEDERAL

PARECER Nº 129, DE 2018 – PLEN/SF ■

Redação final do Projeto de Lei da Câmara nº 53, de 2018 (nº 4.060, de 2012, na Casa de origem).

A Comissão Diretora, em Plenário, apresenta a redação final do Projeto de Lei da Câmara nº 53, de 2018 (nº 4.060, de 2012, na Casa de origem), que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014, consolidando as emendas de redação aprovadas pelo Plenário.

Senado Federal, em 10 de julho de 2018.

- Aprovada em julho/2018 no Congresso Federal
- Aguardando sanção presidencial
- **Início da vigência:** 18 meses após publicação

Dados Pessoais



Dado Pessoal

Informação relacionada à pessoa natural identificada ou identificável

- "Dado Pessoal" inclui dados de
- Clientes (pessoas físicas)
 - Empregados
 - Empregados de Prestadores de Serviço;



Dado Anonimizado

Titular que não possa ser identificado, utilizando técnicas razoáveis* e disponíveis na ocasião do tratamento

Tratamento



Tratamento

Toda operação realizada com dados pessoais:

- | | |
|-----------------|------------------------|
| • Coleta | Arquivamento |
| • Produção | Armazenamento |
| • Recepção | Eliminação |
| • Classificação | Avaliação |
| • Utilização | Controle da informação |
| • Acesso | Modificação |
| • Reprodução | Comunicação |
| • Transmissão | Transferência |
| • Distribuição | Difusão |
| • Processamento | Extração |

Âmbito de Aplicação



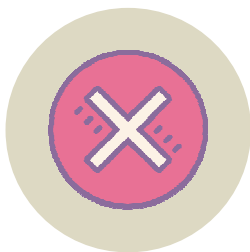
Se aplica a



Qualquer pessoa
ou empresa,
**em qualquer
segmento de
mercado,**
desde que:

- ✓ Tratamento realizado no Brasil
- ✓ Tratamento objective oferta de bens ou serviços a indivíduos localizados no Brasil
- ✓ Tratamento objective o tratamento de dados de indivíduos localizados no Brasil
- ✓ Dados tenham sido coletados no Brasil (onde o titular se encontra no momento da coleta)

Âmbito de Aplicação



Não se aplica

- Tratamento por pessoa natural sem fins económicos
- Fins jornalísticos, artísticos, académicos
- Fins de segurança pública, defesa nacional, segurança do Estado, investigação e repressão a infrações penais
- Dados em trânsito, provenientes de países com grau de proteção adequado

Princípios

Finalidade

- Propósitos legítimos, específicos, explícitos e informados
- Impossibilidade de tratamento posterior de forma incompatível

Adequação

- Compatibilidade com as finalidades informadas

Necessidade

- Limitação ao mínimo necessário para a finalidade
- Dados pertinentes, proporcionais e não excessivos

Livre Acesso

- Consulta facilitada e gratuita

Qualidade

- Exatidão, clareza, relevância e atualização dos dados

Princípios

Transparência

- Informações claras, precisas e facilmente acessíveis

Segurança

- Medidas técnicas e administrativas aptas a proteger os dados

Prevenção

- Medidas para impedir a ocorrência de danos em virtude do tratamento

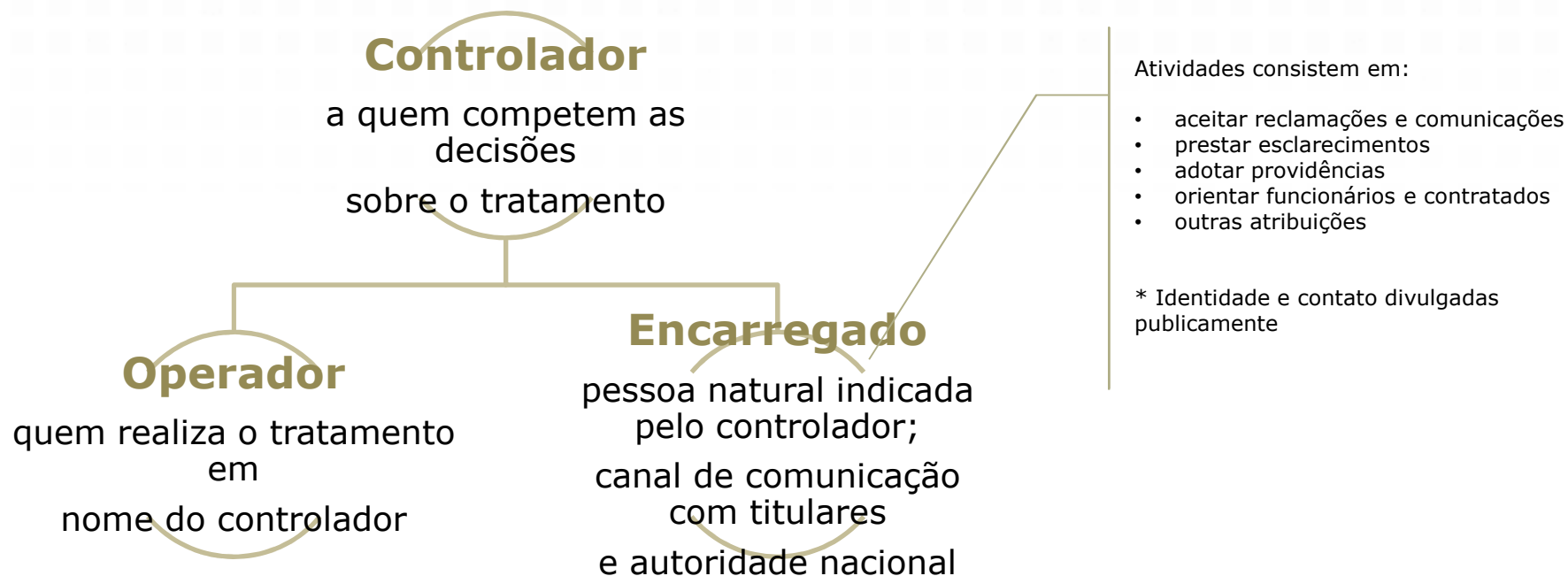
Não discriminação

- Impossibilidade de tratamento para fins discriminatórios, abusivos ou ilícitos

Responsabilidade

- Demonstração de adoção de medidas eficazes para observância da LGPD

Agentes de Tratamento / Players



Hipóteses de Tratamento

Aplicáveis à CPFL:

Consentimento

Obrigação
Legal

Execução de
Contrato

Exercício de
Direito em
Processo

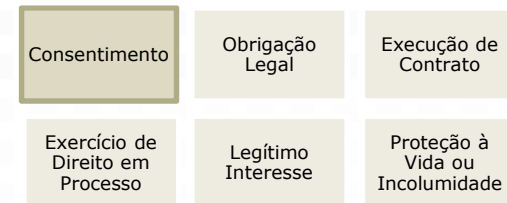
Legítimo
Interesse

Proteção à Vida
ou
Incolumidade

Outras hipóteses permitidas:

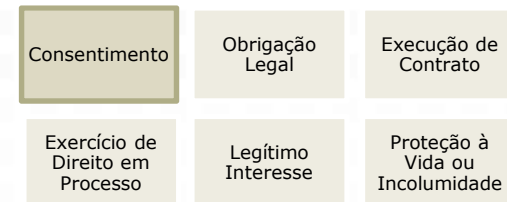
- Órgãos de pesquisa
- Administração pública
- Tutela da saúde
- Proteção do crédito

Hipóteses de Tratamento



- ✓ Por escrito (em cláusula destacada) ou por outro meio que demonstre a manifestação de vontade
- ✓ Ônus da prova do controlador
- ✓ Proibido o vício de consentimento (erro ou ignorância, dolo, coação)
- ✓ Referência a finalidades determinadas
- ✓ **Autorização genérica é nula**
- ✓ Revogável a qualquer tempo
- ✓ Para compartilhamento, exige-se consentimento específico

Hipóteses de Tratamento

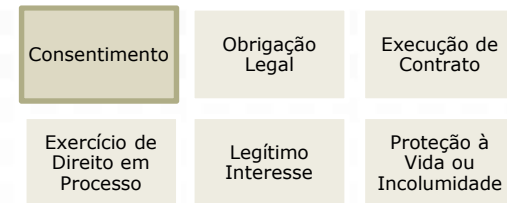


Consentimento deve ser precedido do acesso às seguintes informações de forma clara e inequívoca:

- ✓ Finalidade
- ✓ Forma e duração
- ✓ Identificação e contato do controlador
- ✓ Compartilhamento e finalidade do compartilhamento
- ✓ Responsabilidade dos agentes de tratamento
- ✓ Direitos do titular (menção explícita aos direitos contidos na LGPD)

Informação destacada se o tratamento de dados for **condição** para o fornecimento de produto ou de serviço junto com informação destacada sobre os **meios para exercer os direitos** do titular

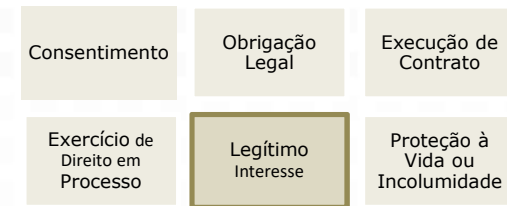
Hipóteses de Tratamento



Dispensado o consentimento para **dados tornados manifestamente públicos** pelo titular

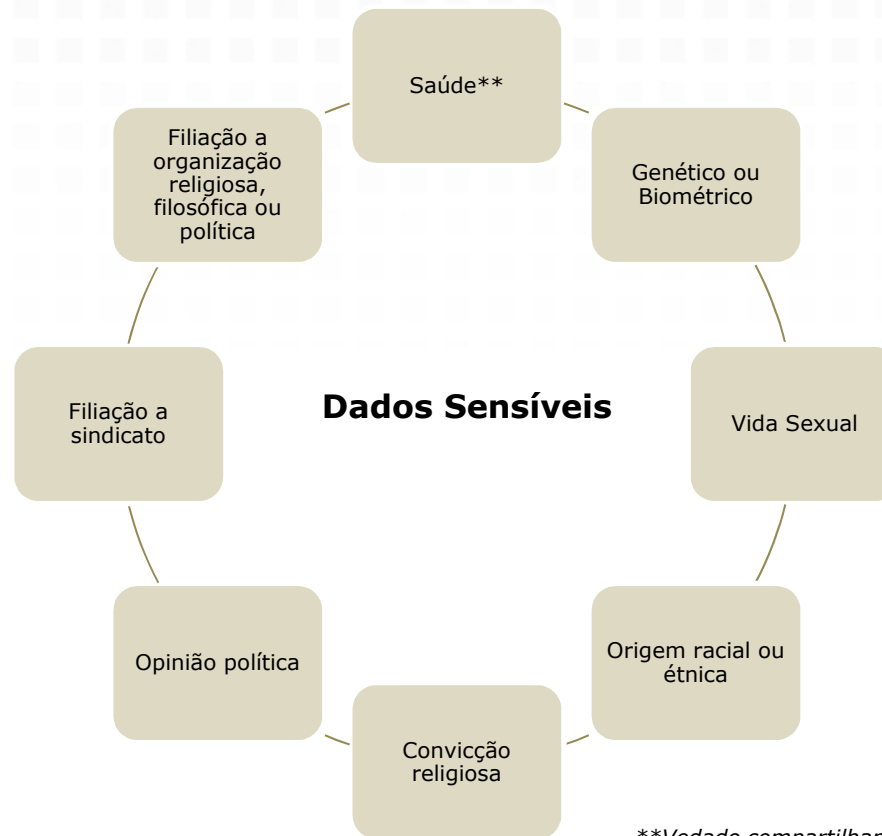
- ✓ Direitos do titular ainda devem ser observados
- ✓ Tratamento deve considerar finalidade, boa fé e interesse público que justificaram sua disponibilização

Hipóteses de Tratamento



- ✓ Finalidades legítimas:
 - Apoio e promoção das atividades do controlador
 - Proteção dos direitos do titular
 - Prestação de serviços que beneficiem o titular, respeitadas suas legítimas expectativas
- ✓ Somente dados estritamente necessários à finalidade
- ✓ Transparência

Dados Sensíveis



***Vedado compartilhamento para fins econômicos*

Dados Sensíveis

Hipóteses de Tratamento:

Consentimento	Obrigação Legal	Exercício de Contrato	Prevenção à fraude e segurança em processos de identificação/autentic ação de cadastro
Legítimo Interesse	Proteção à Vida ou Incolumidade	Exercício de Direito em Processo	<ul style="list-style-type: none">• Órgãos de pesquisa• Administração pública• Tutela da saúde• Proteção do crédito

Direitos dos Titulares de Dados

CONFIRMAÇÃO DE
EXISTÊNCIA DE
TRATAMENTO



simplificada e imediatamente; ou em 15 dias por declaração completa

ACESSO AOS DADOS



armazenamento em formato que favoreça o acesso

CORREÇÃO



de dados inexatos, incompletos ou desatualizados

ANONIMIZAÇÃO,
BLOQUEIO OU
ELIMINAÇÃO



de dados excessivos

PORTABILIDADE



a outro fornecedor (exceto se os dados já estiverem anonimizados)**

** Titular tem o direito de solicitar cópia eletrônica Integral em formato que permita sua utilização subsequente

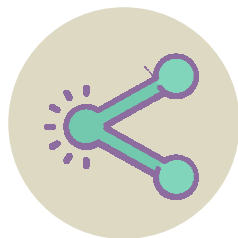
Direitos dos Titulares de Dados

ELIMINAÇÃO



de dados

INFORMAÇÃO SOBRE
COMPARTILHAMENTO



INFORMAÇÃO SOBRE A
POSSIBILIDADE DE NÃO
FORNECER CONSENTIMENTO



e consequências

REVOGAÇÃO DO
CONSENTIMENTO



REVISÃO POR PESSOA
NATURAL



De decisões
automatizadas
(inclusive criação de
perfil)

Término do Tratamento e Eliminação de Dados

Atingida a finalidade

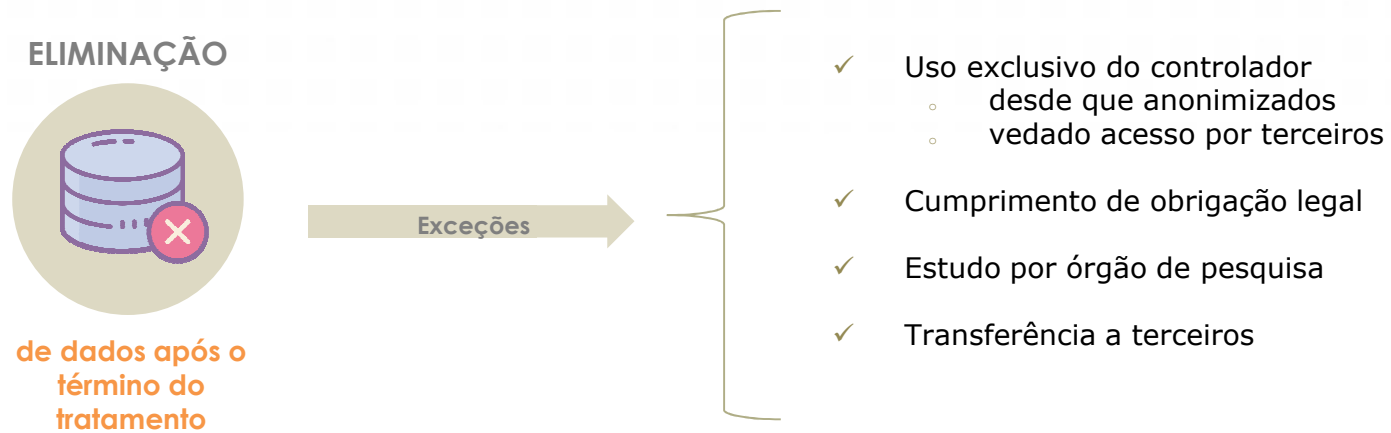
Dados não mais necessários ou pertinentes à finalidade

Fim do período de tratamento

Comunicação do titular, resguardado o interesse público

Determinação de autoridade nacional

Término do Tratamento e Eliminação de Dados



Transferência Internacional

- ✓ **Para países com grau de proteção adequado à LGPD**
- ✓ **Quando o controlador comprovar e garantir o cumprimento da LGPD por meio de:**
 - ✓ **Cláusulas contratuais**
 - ✓ **Cláusulas padrão**
 - ✓ **Normas corporativas globais**
 - ✓ **Selos, certificados e códigos de conduta regularmente emitidos**
- ✓ **Consentimento específico e em destaque do titular**

Transferência Internacional

- ✓ **Cumprimento de obrigação legal ou regulatória**
- ✓ **Execução de contrato a pedido do titular**
- ✓ **Exercício de direito em processo**
- ✓ **Quando autorizada por autoridade nacional**

Transferência Internacional

- ✓ **Cooperação jurídica internacional entre órgãos públicos**
- ✓ **Para proteção da vida ou incolumidade física**
- ✓ **Compromisso em acordo de cooperação internacional**
- ✓ **Quando necessária para execução de política pública ou atribuição legal de ser público**

Responsabilidade civil na Lei Geral de Proteção de Dados

- Art. 42. O controlador **ou** o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, **é obrigado a repará-lo.**
- § 1º A fim de assegurar a **efetiva indenização** ao titular dos dados:
 - I - **o operador** responde **solidariamente** pelos danos causados pelo tratamento **quando descumprir as obrigações da legislação de proteção de dados** ou **quando não tiver seguido as instruções lícitas do controlador**, hipótese em que o **operador equipara-se ao controlador**, salvo nos casos de exclusão previstos no art. 43 desta Lei;
 - II - **os controladores** que estiverem **diretamente envolvidos no tratamento** do qual decorreram danos ao titular dos dados **respondem solidariamente**, salvo nos casos de exclusão previstos no art. 43 desta Lei.

RESPONSABILIDADE É **INDIVIDUAL, SUBJETIVA, NÃO SOLIDÁRIA E ADMITE EXCLUDENTES**

Responsabilidade civil na Lei Geral de Proteção de Dados

- Art. 43. Os agentes de tratamento **só não serão responsabilizados quando provarem:**
- I - que **não realizaram o tratamento de dados pessoais** que lhes é atribuído;
- II - que, embora **tenham realizado o tratamento de dados pessoais** que lhes é atribuído, **não houve violação à legislação de proteção de dados;** ou
- III - que o **dano** é decorrente de **culpa exclusiva do titular dos dados ou de terceiro.**
- **Causas excludentes de responsabilidade:**
- I – ausência de ação ou omissão
- II – ausência de ato ilícito
- III – ausência de nexo de causalidade

Responsabilidade civil na Lei Geral de Proteção de Dados

- Art. 44. O tratamento de dados pessoais será **irregular** quando **deixar de observar a legislação** ou quando **não fornecer a segurança** que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
 - I - o modo pelo qual é realizado;
 - II - o resultado e os riscos que razoavelmente dele se esperam;
 - III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
- Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador **ou** o operador que, **ao deixar de adotar as medidas de segurança** previstas no art. 46 desta Lei, der causa ao **dano**.
- Ausência de segurança no tratamento de dados: ilegalidade do tratamento e responsabilização
- **Responsabilidade individual, subjetiva, não solidária e que admite excludentes**

Responsabilidade civil na Lei Geral de Proteção de Dados

- Art. 45. As hipóteses de **violação do direito do titular no âmbito das relações de consumo** permanecem sujeitas às **regras de responsabilidade previstas na legislação pertinente**.
- Discussão legislativa sobre menção expressa ao Código de Defesa do Consumidor – desnecessidade
- Necessidade de identificação da natureza da relação
- Mesmo na relação de consumo: identificação da causa do dano
- **Convivência harmônica de responsabilidade de acordo com CDC e com a LGPD?**

Responsabilidade civil na Lei Geral de Proteção de Dados

- Microsistema de responsabilização civil
- Responsabilidade subjetiva: depende de prova de ação ou omissão, nexo causal e dano
- Responsabilidade solidária: excepcional e hipóteses específicas
- Estímulo ao cumprimento da lei pelos diferentes agentes de tratamento
- Possibilidade de convivência com diferentes regras de responsabilização: diferentes causas
- Paradigma do Marco Civil da Internet: relações de consumo e remoção de conteúdo de terceiros
- Primeiras versões previam responsabilidade objetiva e solidária: estrutura do CDC
- Evolução do texto legislativo da LGPD: objetivo de criar um sistema próprio e harmônico de responsabilidade

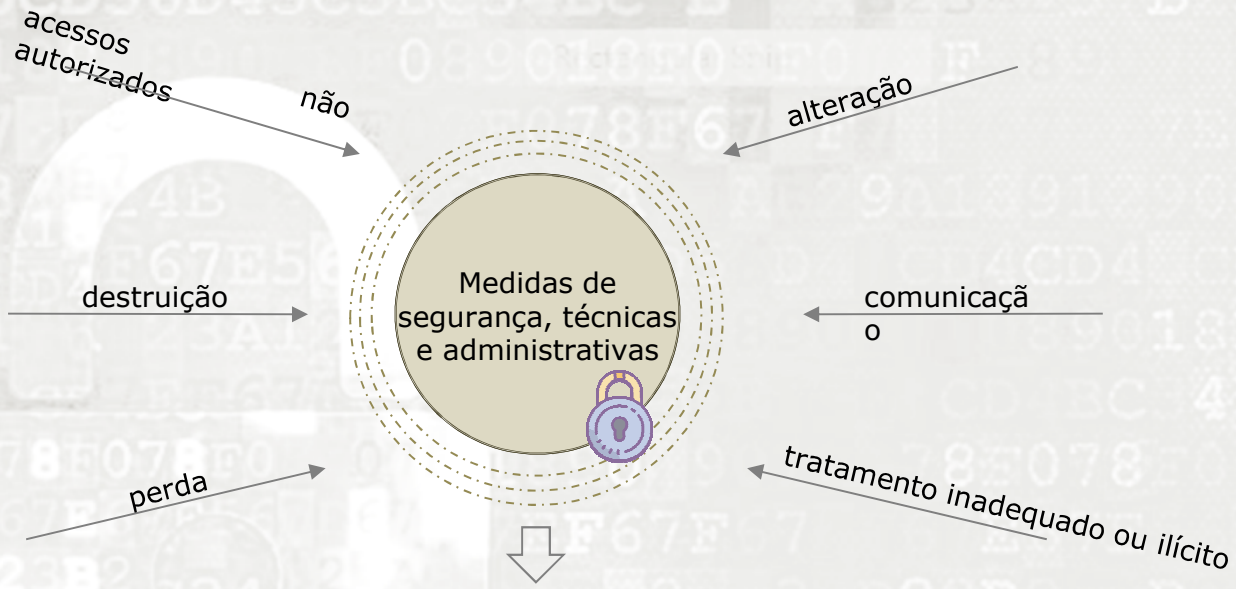
Responsabilidade civil na Lei Geral de Proteção de Dados

- Regulamentação futura pela ANPD não poderá criar novas hipóteses de responsabilidade
- Delimitação de atividades dos agentes de tratamento de dados
- Diferenciação de aplicação de regras do MCI, da LGPD, CDC e outros regulamentos administrativos específicos
- Tendência de criação de sub microssistemas setoriais
- Necessidade de harmonização com a LGPD

Responsabilidade pelo tratamento de dados pelo Poder Público

- Art. 31. Quando houver **infração a esta Lei** em decorrência do **tratamento de dados pessoais por órgãos públicos**, a autoridade nacional poderá enviar **informe com medidas cabíveis** para fazer cessar a violação.
- Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.
- Qual o regime de responsabilidade aplicável ao Poder Público em razão da violação dos direitos dos titulares no tratamento de dados pessoais?
- **Regime geral** previsto na **LGPD** **ou** responsabilidade **objetiva** do Poder Público?
- **Poder Público** será considerado **como controlador** para fins de responsabilização?
- Veto a determinadas sanções administrativas: impacto a operações de tratamento de dados pelo Poder Público

Segurança e Boas Práticas



Da fase de concepção à execução do produto/serviço

Responsabilidade por violação da segurança se ao deixar de adotar medidas de segurança, der causa ao dano

Segurança e Boas Práticas

Comunicação de incidente de segurança em prazo razoável informando:

- ✓ Descrição dos dados
- ✓ Titulares
- ✓ Medidas de proteção adotadas
- ✓ Riscos relacionados ao incidente
- ✓ Motivo da demora caso comunicação não imediata
- ✓ Medidas adotadas para reverter ou mitigar

Comprometimento

**Atualização
Constante**

**Avaliação
sistemática de
impacto e riscos**

**Transparência e
Confiança**



Descumprimento e Sanções Administrativas



Advertência
com prazo para
correção



Multa
até 2% do
faturamento Limite R\$
50.000.000,00



Multa diária



Publicização da
infração



Bloqueio e eliminação
dos dados pessoais



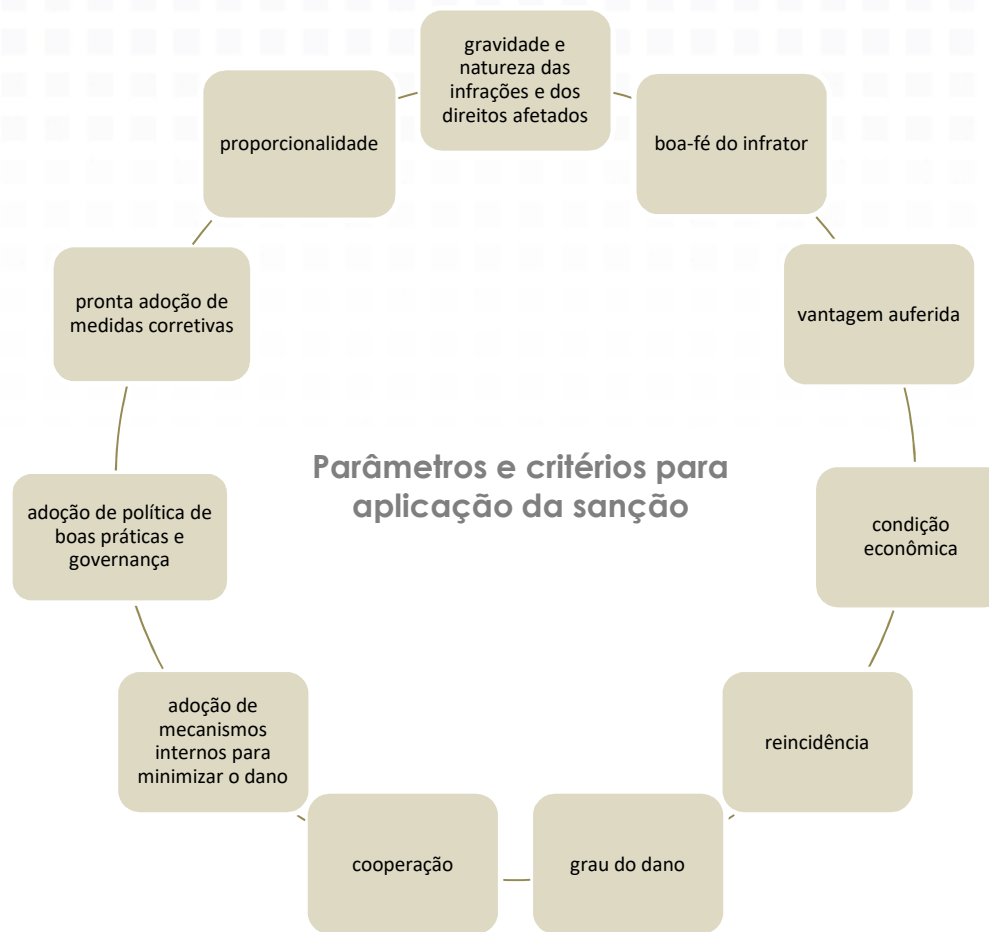
Suspensão parcial ou
total do banco de
dados por 6 meses
prorrogáveis



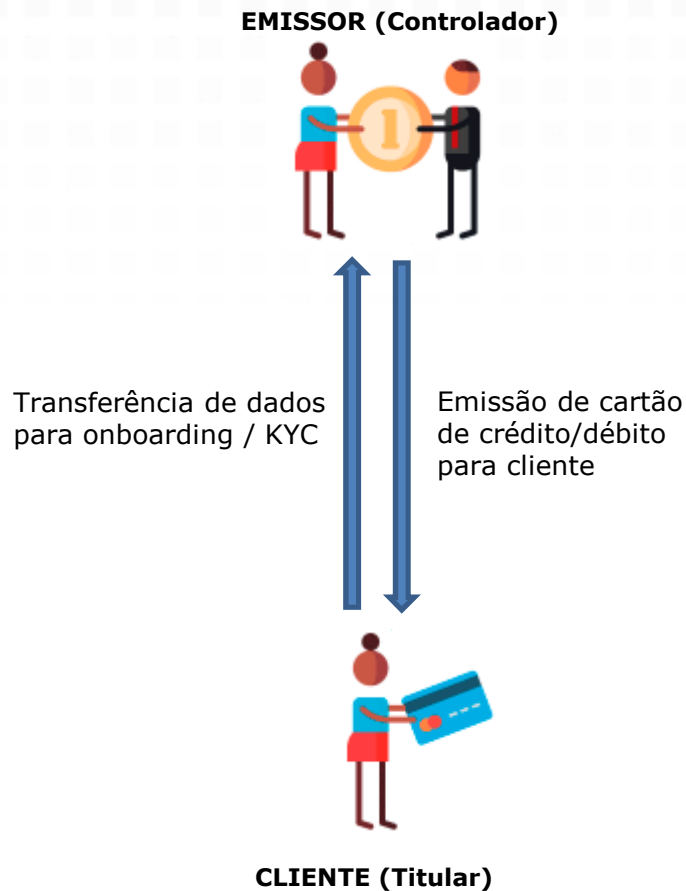
Suspensão da
atividade de
tratamento por 6
meses prorrogáveis



Proibição parcial ou
total de atividades de
tratamento

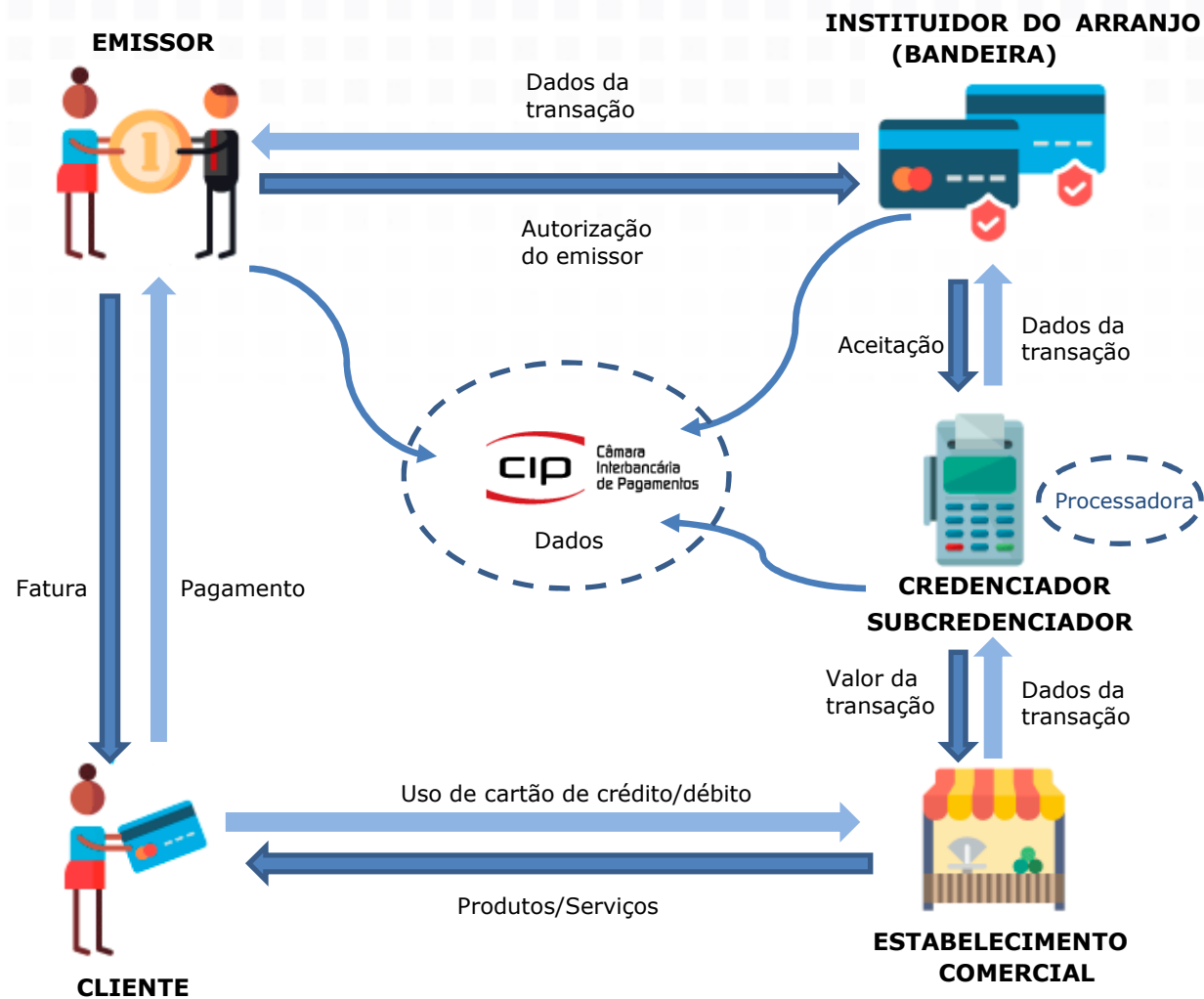


Relação entre Emissor e Cliente – Onboarding e KYC



- **Hipótese de tratamento:** obrigação legal
 - ✓ Circular nº 3.680/2013 (onboarding)
 - ✓ Lei 9.613/1998 (KYC)
 - ✓ Circular nº 3.461/2009 (KYC)
 - ✓ Cumprimento de obrigação legal independente de consentimento
- **Princípios para o tratamento:**
 - ✓ Finalidade (propósito específico)
 - ✓ Adequação (compatibilidade do tratamento)
 - ✓ Proporcionalidade (limitação)

Relação entre Cliente e Participantes

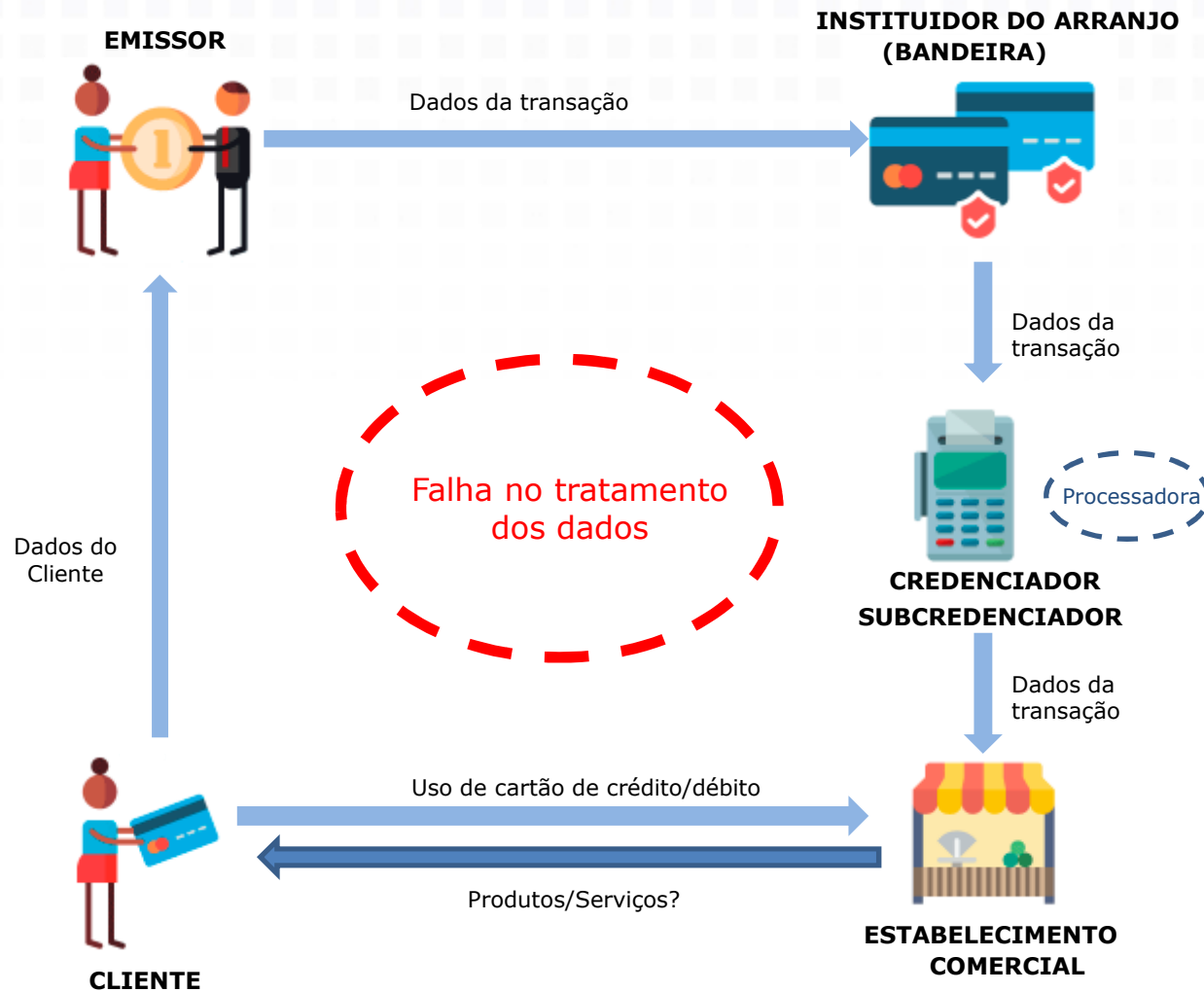


Questões

- Compartilhamento de dados da transação* entre participantes precisa de consentimento do cliente?
 - ✓ Não, desde que não haja a circulação de dados pessoais
- Cliente tem direito a rever decisão automatizada? (operação no cartão de crédito)
 - ✓ Não, desde que as decisões automatizadas sigam os critérios de crédito contratados com o cliente

*Dados da transação: Número do cartão; valor da transação

Responsabilidade solidária

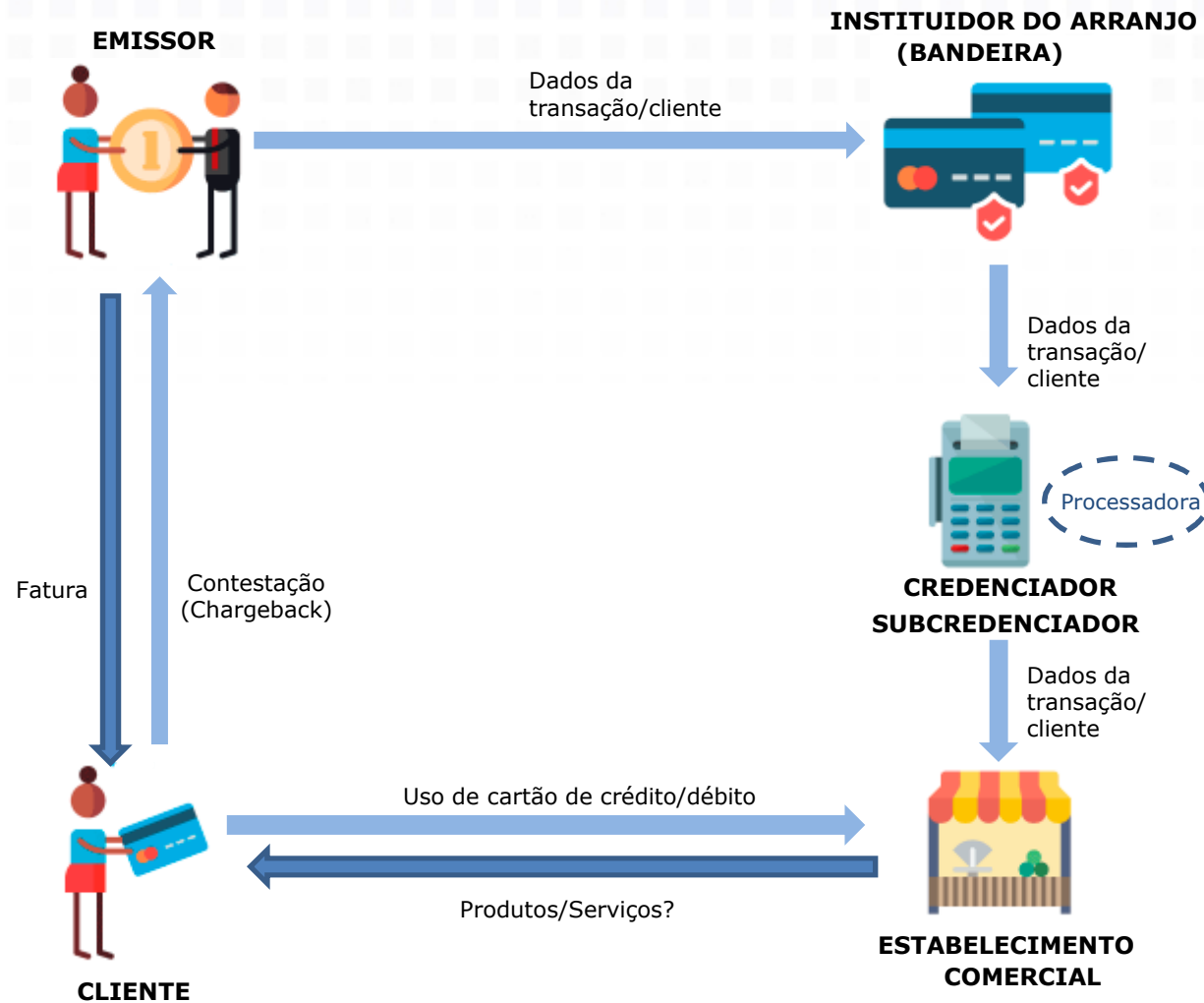


*Dados da transação: Nome do cliente; Número do cartão; valor da transação

Questões

- Responsabilidade entre controlador e operador é solidária?
 - ✓ A princípio não. Controlador e operador são responsáveis com base nas suas atribuições. Responsabilidade solidária não é imediata
- Responsabilidade solidária do operador:
 - ✓ Descumprimento da LGPD
 - ✓ Inobservância das instruções do controlador
- Responsabilidade entre participantes é solidária?
 - ✓ A princípio não. Cada participante deve ser responsável com base em suas atribuições. Necessidade de harmonização da LGPD com o Código de Defesa do Consumidor
- Inversão do ônus da prova
 - ✓ Alegação verossímil
 - ✓ Hipossuficiência; ou
 - ✓ Ônus excessivo

Chargeback

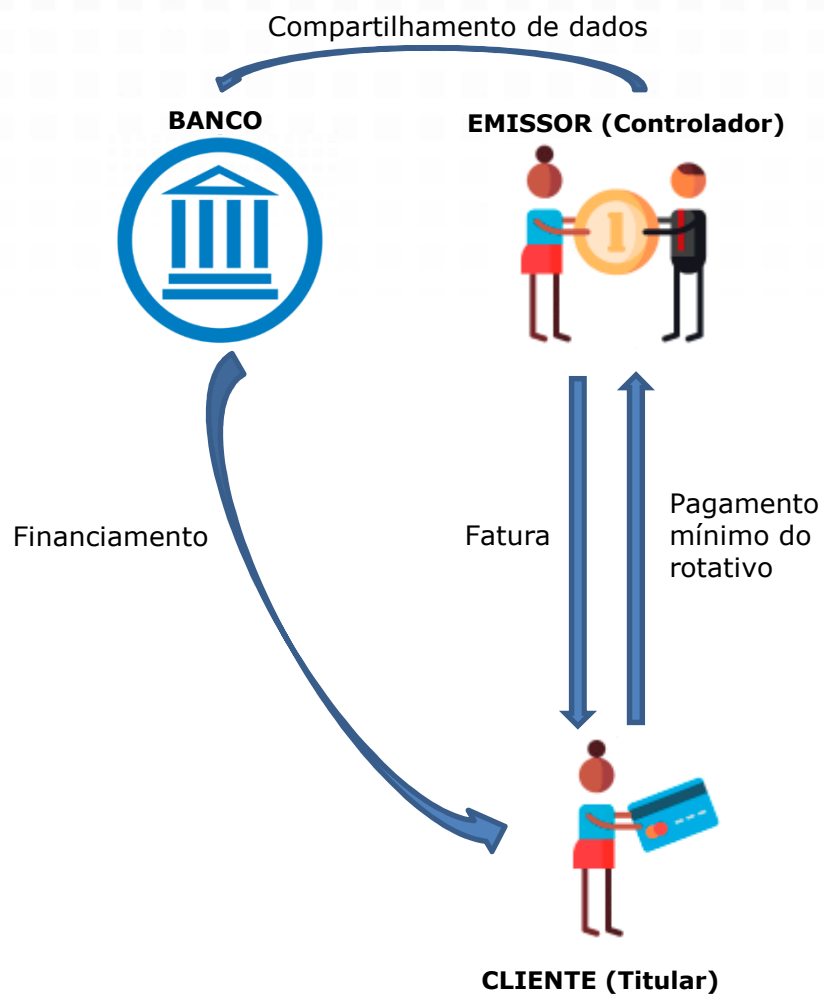


Questões

- Compartilhamento de dados da transação/cliente* entre participantes na hipótese de chargeback precisa de consentimento do cliente?
- ✓ **Sim, tendo em vista que não decorre de previsão legal ou de previsão do contrato celebrado com o cliente**

*Dados da transação: Nome do cliente; Número do cartão; valor da transação

Financiamento da fatura

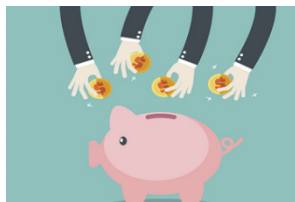


Questões

- Compartilhamento de dados do cliente com banco para fins de financiamento precisa de consentimento específico do cliente para tratamento?
- ✓ Não é necessário obtenção de consentimento específico para cada operação de financiamento, desde que haja cláusula mandato no contrato que autorize o emissor contratar financiamento em nome do cliente e compartilhar os seus dados.

Securitização

FUNDO DE INVESTIMENTO



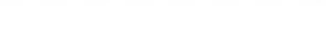
EMISSOR (Controlador)



Compartilhamento de dados



Compra da operação



Fatura



Pagamento parcelado



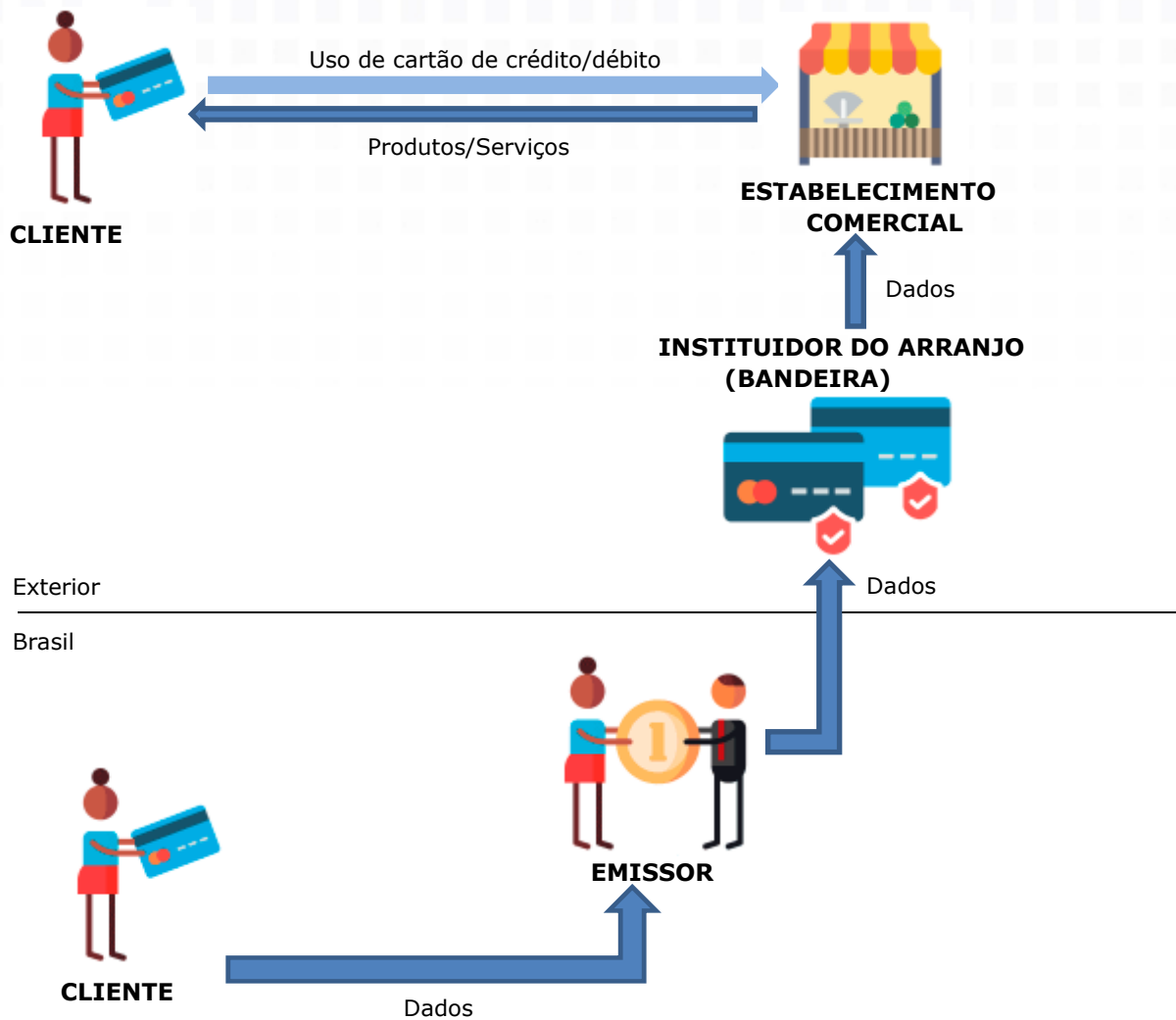
CLIENTE (Titular)



Questões

- Compartilhamento de dados do cliente com fundo de investimento precisa de consentimento do cliente?
- ✓ Sim, é necessário obter consentimento específico

Uso do cartão no exterior

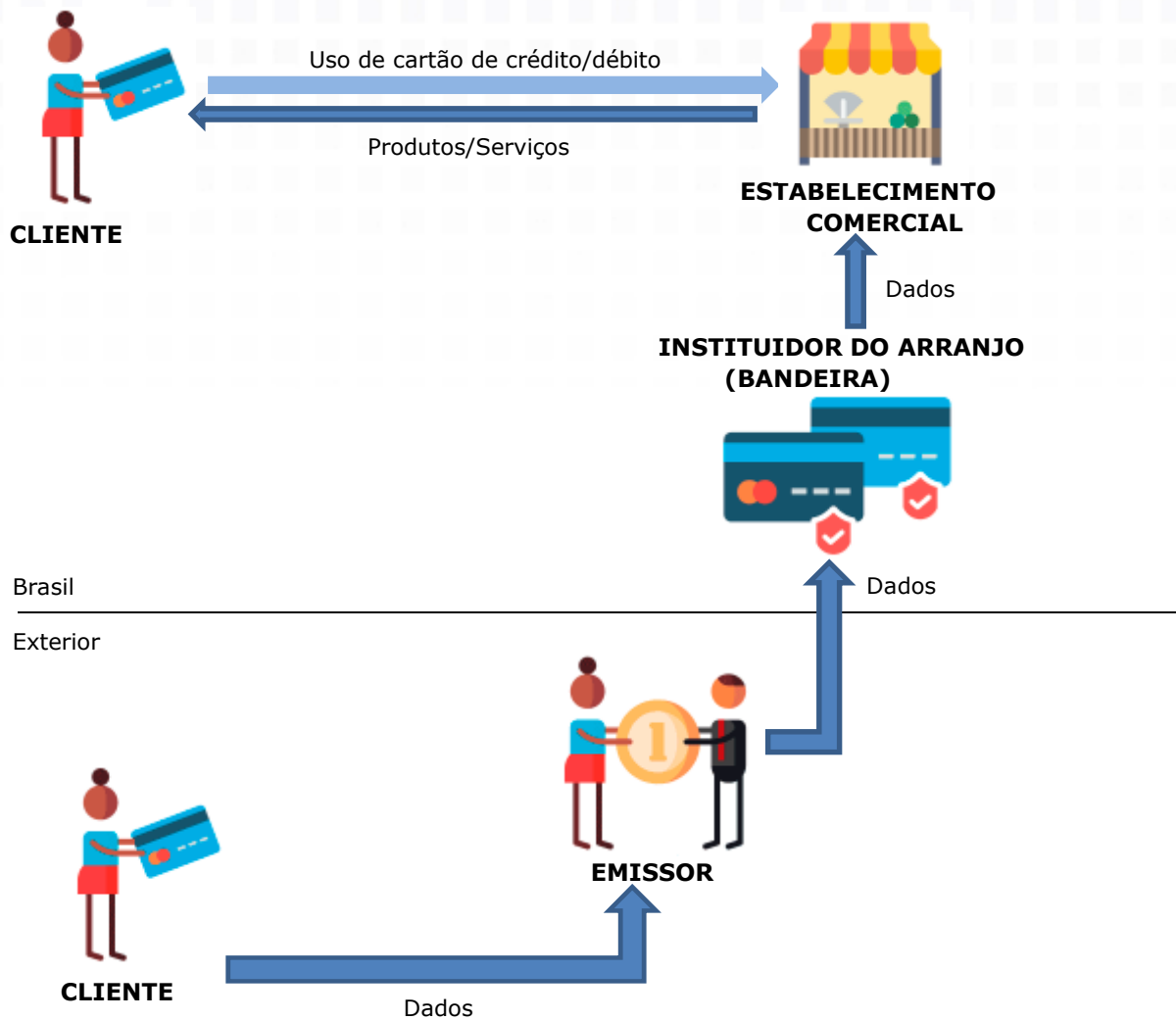


Questões

- Uso de cartão no exterior configura transferência internacional de dados?

*Dados da transação: Número do cartão; valor da transação

Uso de cartão estrangeiro no Brasil



Questões

- LGPD se aplica nessa hipótese?

*Dados da transação: Número do cartão; valor da transação

Recomendações

- Investimento em segurança e tecnologia
 - ✓ Tratamento será considerado irregular quando não fornecer a segurança adequada
- Elaboração de regras de boas práticas e de governança, que estabeleçam:
 - ✓ Condições de organização
 - ✓ Normas de segurança
 - ✓ Padrões técnicos mínimos
 - ✓ Obrigações específicas de cada participante no tratamento

PINHEIRONETO

ADVOGADOS



São Paulo

R. Hungria, 1.100
01455-906
São Paulo . SP
t. +55 (11) 3247 8400
f. +55 (11) 3247 8600
Brasil

Rio de Janeiro

Rua Humaitá, 275 . 16º andar
22261-005
Rio de Janeiro . RJ
t. +55 (21) 2506 1600
f. +55 (21) 2506 1660
Brasil

Brasília

SAFS, Quadra 2 . Bloco B
Ed. Via Office . 3º andar
70070-600 . Brasília . DF
t. +55 (61) 3312 9400
f. +55 (61) 3312 9444
Brasil

Bruno Balduccini

f. +55(11) 3247 8927

E-mail bbalduccini@pn.com.br

André Giachetta

f. +55(11) 3247 8686

E-mail azgiachetta@pn.com.br

Gabriel de Almeida Conceição

f. +55(11) 3247 6243

E-mail galmeida@pn.com.br