# Privacidade e Proteção de Dados - Impactos das Leis e Regulamentos para CSIRTs e Profissionais de Segurança

Danilo Doneda

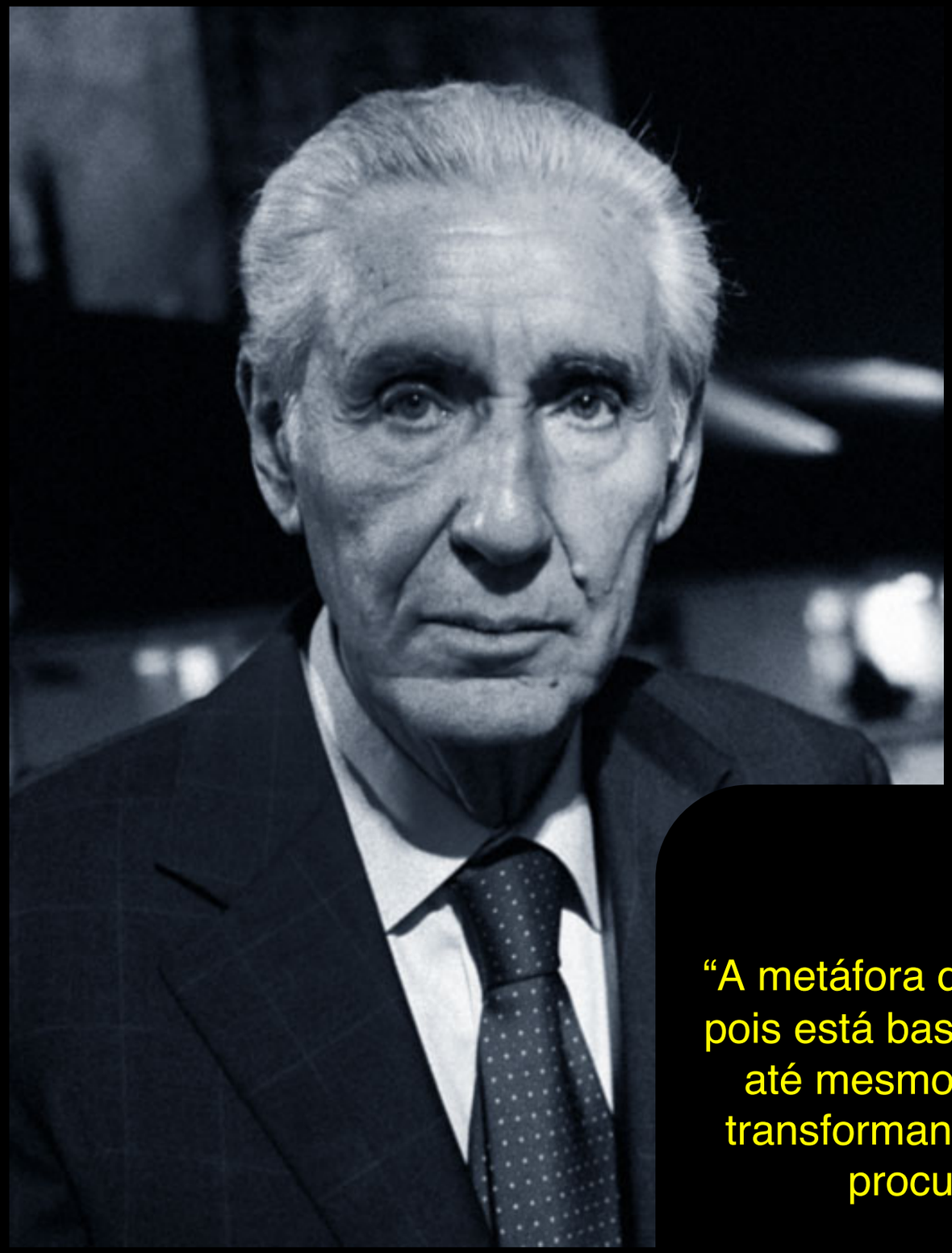
7º Fórum Brasileiro de CSIRTsCGI.br - NIC.br
Setembro 2018

# Lei 13.709/2018

# Lei Geral de Proteção de Dados (LGPD)

# Privacidade

# Proteção de Dados



“A metáfora do **'homem de vidro’** é uma metáfora totalitária, pois está baseada na pretenção do Estado de conhecer tudo, até mesmo os aspectos mais íntimos da vida do cidadão, transformando automaticamente em suspeitos aqueles que procurem salvaguardar a própria vida privada"

Stefano Rodotà

PROBLEMA:

# Assimetria informacional

A transparência deve ser diretamente proporcional ao poder

A privacidade deve ser inversamente proporcional ao poder

# Privacidade e Proteção de dados pessoais

## Do segredo ao controle

# Privacidade e Proteção de dados pessoais

Personalidade

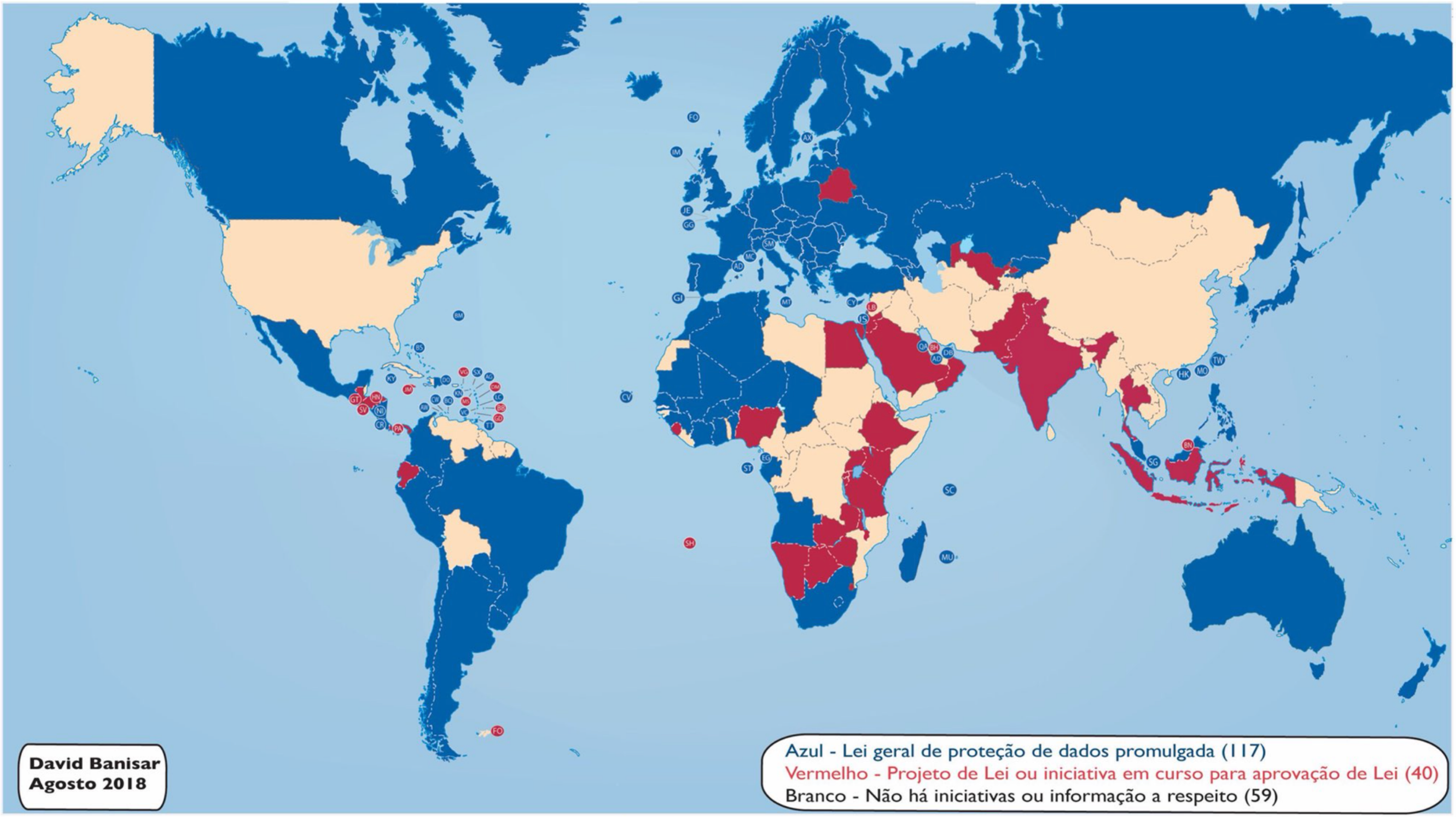
Liberdade

igualdade

# Marcos regulatórios

126 PAÍSES POSSUEM, HOJE, LEIS SOBRE PROTEÇÃO DE DADOS PESSOAIS

# Leis e Projetos de Lei gerais sobre proteção de dados e privacidade em 2018



# INSTRUMENTOS LEGISLATIVOS PARA PROTEÇÃO DE DADOS PESSOAIS

# MODELOS REGULATÓRIOS

## UNIÃO EUROPEIA

- Diretiva 95/46/CE
- Regulamento Europeu Geral de Proteção de Dados (GDPR, 2018)

# MODELOS REGULATÓRIOS

## Estados Unidos

- Privacy Act
- Modelo setorial

Novas leis de proteção de dados: um modelo ***ex-ante*** de proteção

1) não existe dado pessoal insignificante (conceito amplo: “identificado ou identificável”)

2) Necessidade de uma base legal para o tratamento de dados

3) Instrumentos de tutela coletiva e preventiva

# FAIR INFORMATION PRIVACY PRINCIPLES

FINALIDADE

CONSENTIMENTO

ACESSO

SEGURANÇA

TRANSPARÊNCIA

# Marco Civil da Internet
# Lei 12.965/2014

O Marco Civil da Internet não garante a privacidade e a proteção de dados de forma abrangente, completa e estruturada.

Nem todas as disposições sobre proteção de dados são de natureza protetiva

O Marco Civil da Internet NÃO É uma normativa geral sobre proteção de dados pessoais

# Marco Civil da Internet

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

...

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

# Marco Civil da Internet

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

# Marco Civil da Internet

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

...

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

# Marco Civil da Internet

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

# Marco Civil da Internet

X - EXCLUSÃO DEFINITIVA DOS DADOS PESSOAIS QUE TIVER FORNECIDO A DETERMINADA APLICAÇÃO DE INTERNET, A SEU REQUERIMENTO, AO TÉRMINO DA RELAÇÃO ENTRE AS PARTES, RESSALVADAS AS HIPÓTESES DE GUARDA OBRIGATÓRIA DE REGISTROS PREVISTAS NESTA Lei;

# Marco Civil da Internet

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

# Marco Civil da Internet

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

# Lei 13.709/2018

# Lei Geral de Proteção de Dados (LGPD)

# Escopo

Aplica-se ao setor publico e privado

Aplica-se a qualquer tratamento de dados pessoais de pessoas naturais

*“por **tratamento de dados pessoais** entende-se '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.'”*

# Escopo

Aplicabilidade à internet?

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

# Escopo

Não se aplica em:

- tratamentos por pessoa natural para fins exclusivamente pessoais;

- Tratamentos para fins exclusivamente jornalísticos, literários ou acadêmicos;

# Escopo

- Não se aplica para tratamentos para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais.

Neste caso o tratamento será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

# DEFINIÇÕES

**Dado pessoal**: dado relacionado à pessoa natural identificada ou identificável

# DEFINIÇÕES

**Dado pessoal**: dado relacionado à pessoa natural identificada ou identificável

(redação anterior): dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;

(GDPR): «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

# Dados anonimizados

**Dado anonimizado**: dado relativo a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

**Serão considerados dados pessoais** quando

- o processo de anonimização ao qual foram submetidos for **revertido** ou quando, com **esforços razoáveis**, puder ser revertido.

- Se forem utilizados para a formação do **perfil comportamental** de uma determinada pessoa natural, ainda que não identificada.

órgão competente poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização

# Pseudonimização

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1o A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2o O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3o O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4o Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

# Definições

**Titular**: a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

**Controlador**: a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

**Operador**: a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

**Encarregado**: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;

# Requisitos para tratamento de dados

CAPÍTULO II
DO TRATAMENTO DE DADOS PESSOAIS

Seção I
Dos **Requisitos** para o Tratamento de Dados Pessoais

Art. 7o O **tratamento** de dados pessoais **somente poderá ser realizado** nas seguintes **hipóteses**:

# Requisitos para tratamento de dados

**consentimento** livre e inequívoco;

cumprimento de uma **obrigação legal ou regulatória** pelo responsável;

Realização de **estudos** por órgão de **pesquisa**;

pela **administração pública**;

para a proteção da **vida** e tutela da **saúde**;

necessário para a execução de um **contrato**;

exercício regular de direitos em **processo** judicial ou administrativo;

se necessário para atender aos **interesses legítimos** do responsável

Para a proteção do **crédito**

# Consentimento

Art. 7o O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de **consentimento** pelo titular;

Art 5º, XII - **consentimento**: manifestação **livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

# CONSENTIMENTO

**Marco Civil da Internet, art 7º**

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante **consentimento livre, expresso e informado** ou nas hipóteses previstas em lei;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais

**Lei 13.709/2018**

Art. 5º XII – consentimento: **manifestação livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

# Consentimento

Art. 8º O **consentimento** previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1o Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2o Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3o É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4o O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5o O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

# Interesse legítimo

Art. 7º, IX - quando necessário para atender aos **interesses legítimos do controlador ou de terceiro**, **exceto no caso de prevalecerem direitos e liberdades fundamentais do titular** que exijam a proteção dos dados pessoais; ou

# Interesse legítimo

Para finalidades legítimas do controlador ou de terceiro

Em situações concretas

Teste de proporcionalidade

Sujeito a;

- Minimização
- Transparência
- Relatório de impacto

# Interesse legítimo

Art. 10. O **legítimo interesse** do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1o Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2o O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3o A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

# Princípios

Finalidade

Adequação

Necessidade

Livre acesso

Qualidade

Transparência

Segurança

Prevenção

Não Discriminação

responsabilização e prestação de contas

# Direitos

Confirmação

Acesso

Retificação

Cancelamento

Oposição

Portabilidade

Anonimização

Informação

Revogação do consentimento

# SEGURANÇA DA INFORMAÇÃO

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1o A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6o desta Lei.

§ 2o As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

# SEGURANÇA DA INFORMAÇÃO

Devem ser adoradas medidas adequadas

- O órgão competente poderá dispor sobre padrões técnicos e organizacionais

- Privacy by Design

Privacy by Default

# SEGURANÇA DA INFORMAÇÃO

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

# INCIDENTES DE SEGURANÇA

Devem ser comunicados ao órgão competente e ao titular

- será verificada a potencial extensão do dano

- medidas preventivas (utilização de criptografia) são levadas em consideração

- pode haver a determinação de comunicação pública

# INCIDENTES DE SEGURANÇA

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1o A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;
V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

# INCIDENTES DE SEGURANÇA

§ 2o A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3o No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

.

# INCIDENTES DE SEGURANÇA

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

# Transferência Internacional de dados pessoais

É possível com:

- Adequação;
- Consentimento;
- Autorização da Autoridade;
- Acordos Internacionais
- Cláusulas corporativas globais;
- Cláusulas-padrão;
- Cláusulas contratuais para determinada transferência;
- Selos, Certificados e Códigos de Conduta

# SANÇÕES

- advertência
- multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil limitada, no total, a R$ 50.000.000,00 por infração;
- multa diária
- publicização da infração
- bloqueio de dados pessoais
- eliminação dos dados pessoais a que se refere a infração

# Enforcement

ANPD - Agência Nacional de Proteção de Dados

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade