41º CONGRESSO DE TÉCNICOS CONTABILISTAS E ORÇAMENTISTAS PÚBLICOS

LGPD
Lei Geral de Proteção de Dados

Fábio Correa Xavier

Fábio Correa Xavier

CIO do TCESP | Professor
Colunista MIT Technology Review Brasil
Mestre em Ciência da Computação

fabio@tce.sp.gov.br
https://www.linkedin.com/in/fabiocorreaxavier
@fabiocx
fabioxavier.com.br

+30 ANOS

EXPERIÊNCIA PROFISSIONAL

EM GESTÃO, GOVERNANÇA E TECNOLOGIA DA INFORMAÇÃO

MIT Technology Review
Publicado por TEC

COLUNISTA MIT TECHNOLOGY REVIEW
mittechreview.com.br/author/fabio-xavier/

JOTA

ARTIGOS PARA O PORTAL JOTA
www.jota.info/autor/fabio-correa-xavier

Migalhas

ARTIGOS PARA O PORTAL MIGALHAS
www.migalhas.com.br/autor/fabio-correa-xavier

01

O básico (e fundamental) da LGPD

Lei Geral de Proteção de Dados

Lei 13.709/2018

- É uma regulação específica para tratamento de dados pessoais

- Protege o direito fundamental à privacidade sob a ótica dos dados pessoais

- Prevê a Inaugura um novo rol de direitos aos titulares de dados pessoais

- proteção de dados em quaisquer meios – digitais ou analógicos

- Traz regras claras para instituições públicas e privadas que realizam tratamento de dados pessoais

- Apresenta sanções próprias – multas, publicização da infração, eliminação dos dados, bloqueio do tratamento

Multidisciplinar

Legislação e Regulamentos Setoriais

LGPD e legislação e regulamentação setorial, como para a área de saúde e financeira

Privacidade e Proteção de dados pessoais

Programa de Governança em Privacidade e boas práticas de proteção de dados

Segurança da Informação

Conhecimento das boas práticas em soluções em Segurança da Informação

Gestão de Risco e Incidentes

Conhecimento de análise e medidas para mitigação de riscos

Gestão de Demandas e Atendimento

Para atendimento à ANPD, titulares, colaboradores e terceiros

O que são esses dados pessoais?

Art. 5º, I

Dado Pessoal

Informação relacionada a pessoa natural identificada ou identificável

Placa de carro

Foto e imagem

Localização por GPS

Documentos de identificação como CI, CPF, matrícula

Endereço, telefone, e-mail

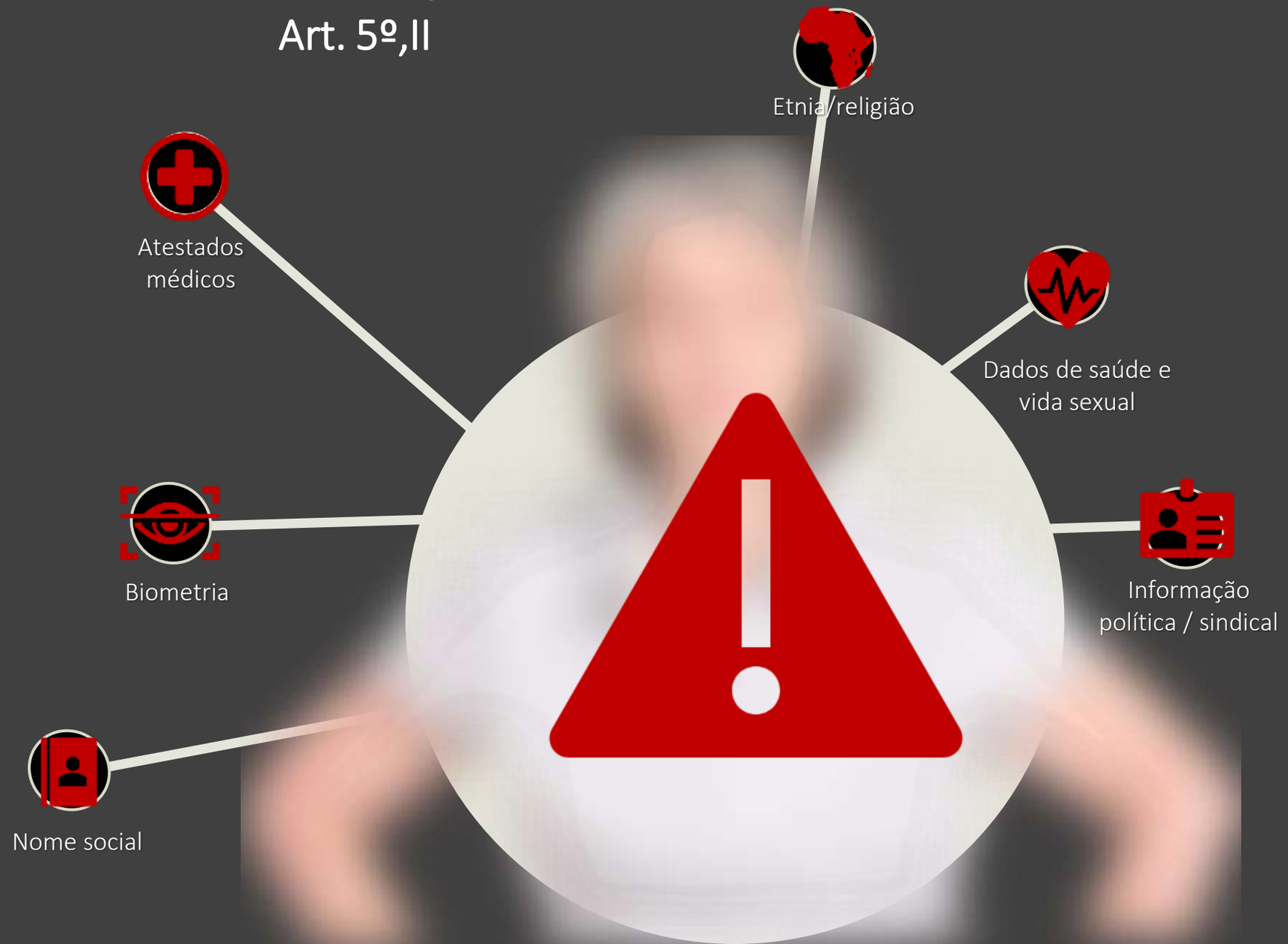
Endereço IP

O que são esses dados pessoais sensíveis?

Art. 5º,II

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, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.



Quais são os dados "normais"?

https://youtu.be/uHZs3ADb6RQ

Princípios da LGPD

art. 6º, inciso I LGPD

1. **Finalidade**
   Propósitos legítimos, específicos, explícitos e informados ao titular
2. **Adequação**
   Compatibilidade entre o tratamento e a finalidade informada ao titular
3. **Necessidade**
   Limitação do tratamento ao mínimo necessário para a realização de suas atividades
4. **Livre acesso**
   Consulta facilitada e gratuita sobre a forma e duração do tratamento
5. **Qualidade dos dados**
   Atualização, retificação dos dados pelos titulares
6. **Transparência**
   Informações claras, precisas e acessíveis
7. **Segurança**
   Medidas técnicas e administrativas para proteção dos dados pessoais
8. **Prevenção**
   Medidas para prevenir a ocorrência de dados no tratamento dos dados
9. **Não discriminação**
   Impossibilidade de tratamento para fins discriminatórios ilícitos ou abusivos
10. **Responsabilização e Prestação de Contas**
    Demonstração da adoção de medidas eficazes
+ **BOA-FÉ**

Finalidade do Tratamento

art. 6º, inciso I LGPD

1

Finalidade
Propósitos legítimos, específicos, explícitos e informados ao titular

Legítima
Legal, justificado, bom senso, razoável, justo

Específica
Exclusivo, próprio

Explícita
Claro, transparente, sem ressalvas ou restrições

Informada
Com destaque, apartada

Adequação

2

Adequação
Compatibilidade entre o tratamento e a finalidade informada ao titular

Adequado
Perfeita conformidade com a finalidade, ajustado, conveniente

Dados devem ser adequados à finalidade

Procedimento realizado para se alcançar a finalidade

Não eliminar os dados após atingir a finalidade contraria o princípio da adequação

Necessidade

3

Necessidade
Limitação do tratamento ao mínimo necessário para a realização de suas atividades

Dados necessários
Absolutamente preciso, essencial, indispensável, imprescindível

Minimização de Dados
Limitação do tratamento ao mínimo necessário, dados pertinentes, proporcionais e não excessivos

Perguntas orientadoras

1) *A finalidade pretendida pode ser atingida com menos dados?*
2) *Precisa mesmo usar todos esses dados e por quê?*
3) *Todos os titulares deram consentimento?*
4) *Esse BD é exclusivo ou foi adquirido?*
5) *Vale a pena correr os riscos de armazenar todos esses dados?*

Hipótese de Tratamento

arts. 7º e 11 da LGPD

Tratamento pelo Poder Público

Art. 23 da LGPD autoriza Poder Público a realizar o tratamento para o atendimento de sua finalidade pública, persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que as hipóteses de tratamento sejam informadas ao titular

Cumprimento de obrigação legal ou regulatória (art. 7º, II e art. 11, II)

Previsão Legal

Lei, Decreto, normativo ou regulamento que respalda a finalidade do tratamento de dados pessoais realizado.

Execução de políticas públicas (art. 7º, III e art. 11, II)

(i) existência de ato formal que institui a política pública;
(ii) a definição de um programa ou ação governamental específico, a ser executado por uma entidade ou por um órgão público; e
(iii) o tratamento seja realizado para o atendimento da finalidade pública, na persecução do interesse público com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público

Com ressalvas:

- **Consentimento** (art. 7º, I e 11, I);
- **Legítimo interesse**, não válida para dados pessoais sensíveis (art. 7º, IX)

02

E quem faz o tratamento dos dados?

Agentes de Tratamento

Atenção

Não são considerados agentes de tratamento os **funcionários, os servidores públicos ou as equipes de trabalho** de uma organização, já que atuam sob o poder diretivo do agente de tratamento.

Agentes de Tratamento (Caráter institucional)

Controlador	**Operador**
Pessoa natural ou jurídica, de direito público ou privado	
Poder de decisão sobre o tratamento	**Segue as instruções do Controlador**
Define **regras** para os operadores	
Define a **Finalidade**, **natureza** dos dados e **duração** do tratamento	

03

O Encarregado pelo tratamento de dados pessoais

Obrigatoriedade

Setor Público deve indicar um encarregado (art. 23, inciso III, da LGPD)

Divulgação dos dados de contato

A identidade e informações de contato do encarregado devem ser publicadas no site institucional (§ 1º do artigo 41)

Atribuições

Garantir a conformidade de uma organização;
Canal de comunicação entre o controlador com o titular e ANPD

Requisitos

Liberdade, independência e autonomia
Acesso direto à Alta Administração
Bom nível de conhecimento multidisciplinar
Recursos humanos, orçamentários e infraestrutura

Atribuições do encarregado

§ 2º do art. 41

Comunicação com o titular

Interagir com os titulares, prestando esclarecimentos e adotando providências necessárias em razão desses contatos ou reclamações dos titulares

Comunicação com a ANPD

Interagir e cooperar com a ANPD

Orientação e conformidade com a LGPD

Orientar os funcionários e contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais

... E o que mais o controlador definir

Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares

Perfil do encarregado

Quem pode ser?

Funcionário da instituição ou agente externo, de natureza física ou jurídica

E como deve ser feito?

Ato formal, como um contrato de prestação de serviços ou um ato administrativo.

Pode ser qualquer colaborador?

Evitar conflito de interesses com outras funções que ele eventualmente exerça na organização

E o que diz a ANPD?

Regulamentação na agenda regulatória de 2023-2024
(Portaria ANPD Nº 35, de 4 de novembro de 2022)

Gostei! Quer ser o encarregado!

Autonomia e independência

Liberdade, independência e autonomia na realização de suas atribuições

Conhecimento técnico multidisciplinar

Privacidade e proteção de dados pessoais, análise jurídica, gestão de riscos, governança de dados e acesso à informação no setor público

Acesso direto à Alta Administração da instituição.

É o cara que vai mexer nas feridas

Estrutura

Recursos humanos, tempo, orçamentários e infraestrutura adequados

04

Jornada de adequação: como começar?

Qual é a missão institucional de privacidade?

*A **declaração de missão de privacidade** descreve o propósito e as ideias em apenas algumas frases. Sua leitura deve levar menos de 30 segundos.*

Microsoft

Na Microsoft, nossa missão é empoderar cada pessoa e cada organização do planeta a alcançar mais. Estamos fazendo isso criando uma nuvem inteligente, reinventando processos de produtividade e negócios e tornando a computação mais pessoal. Em tudo isso, podemos manter o valor atemporal da privacidade e preservar a capacidade de você controlar seus dados.

Isso começa com a garantia de que você faça escolhas significativas sobre como e por que os dados são coletados e usados e garantindo que você tenha as informações necessárias para fazer as escolhas que são ideais para você em nossos produtos e serviços.

Universidade de Stanford

O Departamento de Privacidade da Universidade de Stanford trabalha para proteger a privacidade da universidade, de funcionários, pacientes e outras informações confidenciais. Nosso departamento ajuda a garantir o uso e a divulgação adequada de tais informações, assim como fomentar uma cultura que valoriza a privacidade por meio da conscientização. O Departamento de Privacidade fornece conselhos e orientações significativas sobre as "Melhores Práticas" e expectativas de privacidade para a comunidade universitária.

A visão da Autoridade da Bélgica

Em suas considerações e atividades, a Autoridade tem como objetivo salvaguardar o equilíbrio entre o direito à proteção da privacidade e outros direitos fundamentais

Programa de Governança em Privacidade

art. 50, inciso I LGPD

A — Demonstrar **comprometimento** do controlador

B — Englobar **todos os dados pessoais**

C — **Considerar** estrutura, escala, volume e sensibilidade dos dados

D — **Conter Políticas e salvaguardas adequadas** e **avaliação** de **riscos**

E — Criar/manter relação **de confiança com o titular**

F — **Integrar** à **governança** corporativa

G — **Conter Planos de resposta a incidentes**

H — Atualizar e **monitorar continuamente**

Inciso II — Deve demonstrar sua **efetividade**

05

[Onde estão os dados pessoais?]

Inventário de Dados Pessoais

O Inventário de Dados Pessoais – IDP consiste no registro das operações de tratamento dos dados pessoais realizados pela instituição (LGPD, art. 37).

Art. 37. O controlador e o operador devem manter ***registro das operações de tratamento de dados pessoais*** *que realizarem, especialmente quando baseado no legítimo interesse.*

7 informações que não podem faltar no IDP

I. Como os dados são coletados?

II. Quais dados são coletados?

III. Onde os dados são armazenados? Qual é o formato dos dados?

IV. Para onde vão os dados?

V. Para que são usados os dados?

VI. Por quanto tempo os dados são mantidos?

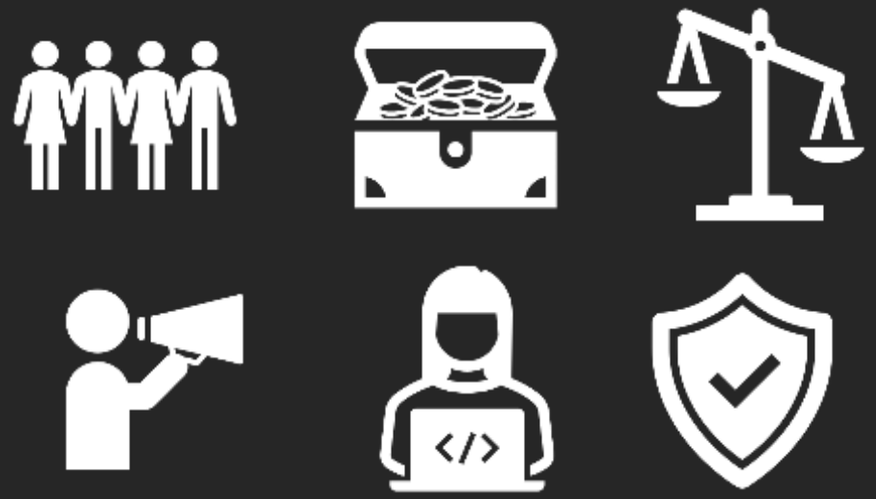
VII. Quais as medidas de segurança e privacidade aplicadas?

7 informações que não podem faltar no Inventário de Dados Pessoais
MIT Technology Review Brasil
https://bit.ly/3F1OHCv

06

[Devo me virar sozinho?]

Stakeholders e parcerias necessárias



Patrocinador da Alta Administração

*Um **embaixador da privacidade** no nível executivo atua como defensor e patrocinador para promover ainda mais a privacidade como um conceito central da organização.*

Estratégias para engajamento

Entender o uso dos dados na Instituição

Identificar a importância e relevância dos dados no dia a dia.

Proteção de Dados e privacidade como diferencial positivo

Oferecer soluções e não problemas.

Workshop e Conscientização

Nivelamento do conhecimento

07

Quem é o responsável?

Definição clara de papéis e responsabilidades

Para criação de expectativas e metas de desempenho individuais

Avaliação de resultados

Para determinar pontos fortes e fracos, para correção. PDCA

Foco no titular

Considerar as diferentes necessidades dependendo da natureza dos produtos e serviços que a organização oferece

Divulgação dos benefícios

Para a organização, clientes e stakeholders, alinhados aos objetivos e metas

08

[E a tal segurança da informação?]

Regra de Pareto

3 ações que podem resolver 80% dos incidentes

Tem que atualizar!!

“as 10 vulnerabilidades mais exploradas para o comprometimento de sistemas e redes governamentais são conhecidas e possuem correções, algumas há mais de 5 anos.”

Não para a configuração padrão

“especialmente para mudar configurações de fábrica alterando, por exemplo, usuário e senhas amplamente conhecidas e desabilitando protocolos inseguros ou não utilizados”

Tem que ter senha forte!!

“sistemas que utilizam apenas senhas como forma de autenticação são alvos mais fáceis para golpes digitais. Uma forma de melhorar a segurança dos sistemas é utilizar múltiplos fatores de autenticação”

Fonte: CETIC.br, detalhado em meu artigo: *Regra de Pareto para a Segurança Digital: 3 ações que mitigam 80% dos ataques*
https://bit.ly/2WcBanG

O **elo humano** é constantemente **negligenciado** em ações institucionais. Em relação à LGPD, é essencial que a instituição promova **treinamentos, capacitação, sensibilização e campanhas constantes** para servidores, contratados, jurisdicionados e parceiros que versem sobre **segurança da informação, privacidade** e cuidados necessários com o tratamento dos dados pessoais.


SUPORTE_
ALÔ! QUERO FALAR COM O COMITÊ RESPONSÁVEL PELA ADEQUAÇÃO DA EMPRESA À LGPD.
POIS NÃO?
VOCÊ FAZ PARTE DO COMITÊ?
EU SOU O COMITÊ.
SÓ VOCÊ?!
TAMBÉM TEM O ASPIRA, MAS ELE NÃO ESTÁ NO MOMENTO. ALGUÉM PEDIU PRA ELE PROCURAR UM ALICATE PRA CONSERTO DE VAZAMENTO DE DADOS.
vidadesuporte.com.br