



**Arthur Guilherme de Salamanka Lima  
Albuquerque**  
01411574

**Cauã Machado Leite**  
01438266

**Danilo Miguel Bezerra da Silva**  
01422952

# **PRIVACIDADE EM SISTEMAS DE BIG DATA: DESAFIOS E SOLUÇÕES**

# INTRODUÇÃO AO BIG DATA

## CONCEITO

Big Data refere-se à capacidade de gerenciar, processar e extrair rapidamente grandes quantidades de dados diversos.

## OS 5Vs

Pilares sustentáveis do núcleo tecnológico.

## VOLUME

Grandes quantidades de dados gerados diariamente.

Exemplo:

Armazenamento em nuvem e processamento distribuído (Hadoop, Spark).

## VELOCIDADE

Análise em tempo real.  
Exemplo: Ferramentas de streaming (Kafka, Flink) e automação de processos.

## VARIEDADE

Dados estruturados e não estruturados.

Exemplo: Redes sociais, sensores, vídeos; integração com pipelines de dados.

## VERACIDADE

Qualidade e confiabilidade dos dados.

Exemplo: Governança e monitoramento de dados para identificar anomalias.

## VALOR

Transformar dados em insights acionáveis.

Exemplo: Análise exploratória, machine learning, visualização (Tableau, Power BI).



# Impacto do Big Data

O Big Data revolucionou diversos setores ao permitir a análise massiva de dados, gerando insights rápidos e precisos para tomada de decisões estratégicas.

## SAÚDE

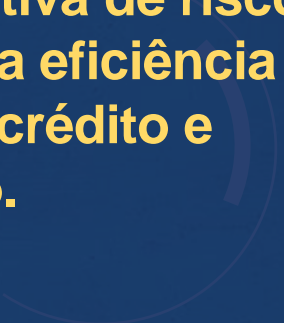
Previsão de surtos de doenças e personalização de tratamentos com base em dados genéticos.

## MARKETING

Campanhas segmentadas e personalizadas, com análise de comportamento de consumo e preferências em tempo real.

## FINANÇAS

Detecção de fraudes e análise preditiva de riscos, melhorando a eficiência nas decisões de crédito e investimento.







# PRIVACIDADE EM BIG DATA

O uso de Big Data levanta preocupações significativas sobre a privacidade, pois envolve a coleta, armazenamento e análise de grandes volumes de dados pessoais.

## RISCOS PRINCIPAIS

### Vazamento de dados

Grandes volumes aumentam o risco de brechas de segurança.

### Reidentificação

Mesmo dados anônimos podem ser combinados para identificar indivíduos.

### Uso indevido

Informações sensíveis podem ser exploradas sem consentimento adequado.

# PRINCIPAIS PONTOS

**Consentimento:** Requerido de forma clara e explícita para tratamento de dados.

**Direitos dos Titulares:** Acesso, retificação, exclusão (esquecimento), portabilidade e objeção.

**Finalidade:** Dados só podem ser usados para objetivos específicos e legítimos.

**Responsabilidade (Accountability):** Empresas devem demonstrar medidas de conformidade e nomear um DPO (Encarregado).

**Segurança:** Implementar medidas técnicas para proteção de dados.

**Notificação de Violações:** Informar autoridades e titulares sobre incidentes.

**Transferência Internacional:** Regras rigorosas para envio de dados a outros países.

# PENALIDADES

**LGPD:** Multas até 2% do faturamento, máximo de R\$ 50 milhões por infração.

**GDPR:** Multas até €20 milhões ou 4% do faturamento global.

# IMPORTÂNCIA

Evita multas elevadas e danos reputacionais.

Garantia de proteção aos direitos de privacidade e dados.

# A CONFORMIDADE COM A LGPD E GDPR

# QUAIS SÃO OS DESAFIOS E RISCOS À PRIVACIDADE?

## 1. Coleta de Dados Sem Consentimento

Quando os dados são coletados sem o conhecimento ou consentimento explícito dos indivíduos, isso representa um sério risco à privacidade. Muitas vezes, aplicativos, sites e dispositivos podem obter informações sensíveis como localização, comportamento de navegação, e até dados biométricos, sem que o usuário tenha ciência ou tenha dado permissão para isso. Este tipo de coleta pode ocorrer de forma oculta, por exemplo, por meio de cookies ou rastreamento de dispositivos, comprometendo o controle que o usuário tem sobre suas próprias informações pessoais.

## 2. Uso Indevido de Dados

Mesmo que os dados sejam coletados com consentimento, eles podem ser reutilizados de maneira não autorizada, seja por venda para terceiros, para fins de marketing, ou até mesmo para manipulação de comportamento de consumidores, sem o devido aviso ao usuário. Por exemplo, uma empresa pode coletar dados para oferecer um serviço e depois repassá-los para outras empresas, sem que os usuários saibam ou tenham permitido essa prática. Isso pode violar a confiança do consumidor e colocar informações sensíveis em risco.

## 3. Reidentificação de Dados

A anonimização de dados é frequentemente vista como uma solução para proteger a privacidade dos usuários. No entanto, em muitos casos, dados considerados "anonimizados" podem ser reidentificados. Isso ocorre quando os dados são cruzados com outras fontes de informação, revelando novamente a identidade da pessoa. Por exemplo, informações de hábitos de consumo, combinadas com localização ou histórico de navegação, podem ser suficientes para identificar um indivíduo específico, mesmo sem a presença de dados explicitamente identificáveis, como nome ou número de CPF.



# EXEMPLOS DE CASOS REAIS

## **Facebook-Cambridge Analytica (2018)**

Esse escândalo envolveu o uso indevido de dados pessoais de milhões de usuários do Facebook sem o consentimento adequado.

## **Caso de Reidentificação em Pesquisa Médica (2019)**

Pesquisadores conseguiram reidentificar cerca de 85% dos americanos a partir de dados "anonimizados" de DNA e algumas informações básicas, como sexo e idade.

## **Vazamento da Equifax (2017)**

Um dos maiores vazamentos que expôs informações financeiras e pessoais de cerca de 147 milhões de pessoas, comprometendo dados sensíveis.

# SOLUÇÕES E FUTURO DA PRIVACIDADE

A privacidade dos dados depende de uma série de técnicas que fortalecem a segurança e limitam o acesso indevido a informações sensíveis. As principais ferramentas incluem:

**Anonimização:** Remove identificadores pessoais dos dados, impossibilitando a identificação direta de indivíduos.

**Pseudonimização:** Substitui identificadores por pseudônimos, permitindo certo grau de privacidade, mas ainda possibilitando a reidentificação com informações adicionais.

**Criptografia:** Garante que os dados, mesmo que interceptados, não possam ser lidos sem as chaves apropriadas.

**Controle de Acesso:** Define quem pode acessar e manipular dados sensíveis, reduzindo riscos de violação interna e externa.



# CONSENTIMENTO INFORMADO

O consentimento informado da base técnica e ética é um pilar central

## TRANSPARÊNCIA

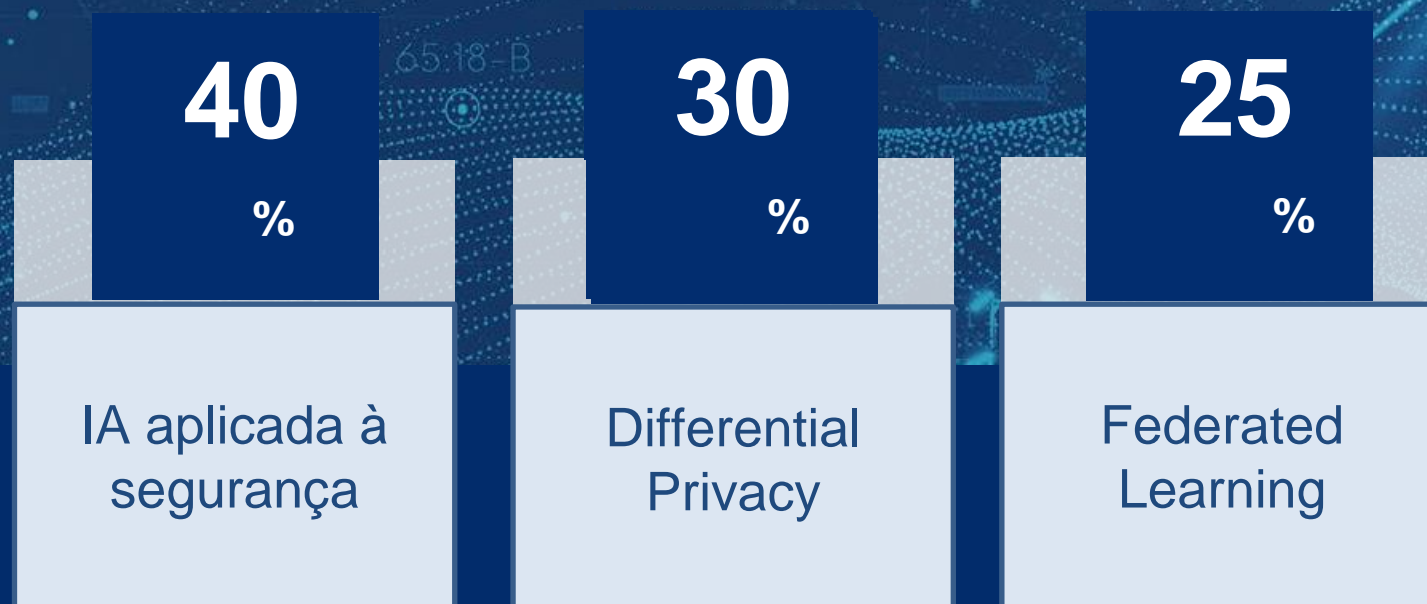
As organizações devem fornecer uma explicação clara, acessível e compreensível sobre como os dados serão coletados, utilizados, armazenados e, eventualmente, compartilhados. Isso envolve evitar o uso de jargões técnicos ou termos confusos, e apresentar políticas de privacidade de forma simplificada.

## CONSENTIMENTO CLARO

Os usuários precisam dar permissão de forma ativa para o uso de seus dados, com a possibilidade de escolher quais informações estão dispostos a compartilhar e para quais finalidades. O consentimento não pode ser generalizado ou implícito; deve ser específico, informado e, sempre que possível, atualizado.

# TENDÊNCIAS FUTURAS

O futuro da privacidade ao avanço tecnológico



Essas inovações prometem transformar a forma como gerimos a privacidade em larga escala.

# LEGISLAÇÕES FUTURAS

A evolução das leis de privacidade sendo moldada pelo crescimento exponencial do Big Data e das tecnologias emergentes

## GDPR e LGPD

Criar regulamentos mais adaptados às novas tecnologias.

## LEIS

Incluir aspectos futuros de privacidade, como IA, vigilância e segurança de dados.

## BIG DATA

Confiar nas empresas para processar dados e adotar medidas proativas de conformidade.



