



Lauro Grippa Neto

Governança de Dados LGPD NA PRÁTICA

MAGRATHEA

www.magrathealabs.com

MAGRATHEA

Lauro Gripa Neto
Engenheiro de Software



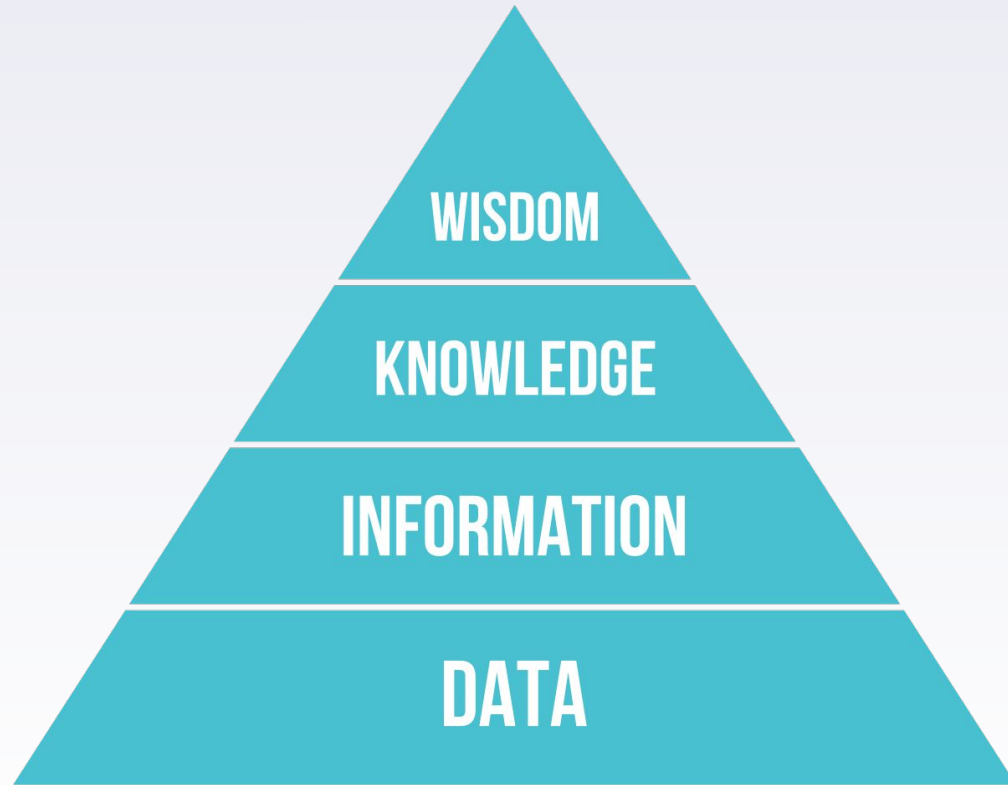
lauro@magrathealabs.com



[laurogripa](https://github.com/laurogripa)

A Origem das Leis de **Proteção** de **Dados**





PRINCIPIA MATHEMATICA

TO *56

BY

ALFRED NORTH WHITEHEAD

AND

BERTRAND RUSSELL, F.R.S.



CAMBRIDGE
AT THE UNIVERSITY PRESS

350 páginas pra provar que $1 + 1 = 2$

*54.43. $\vdash : \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . *54.26 . \supset \vdash : \alpha = \iota'x . \beta = \iota'y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

[*51.231]

$\equiv . \iota'x \cap \iota'y = \Lambda .$

[*13.12]

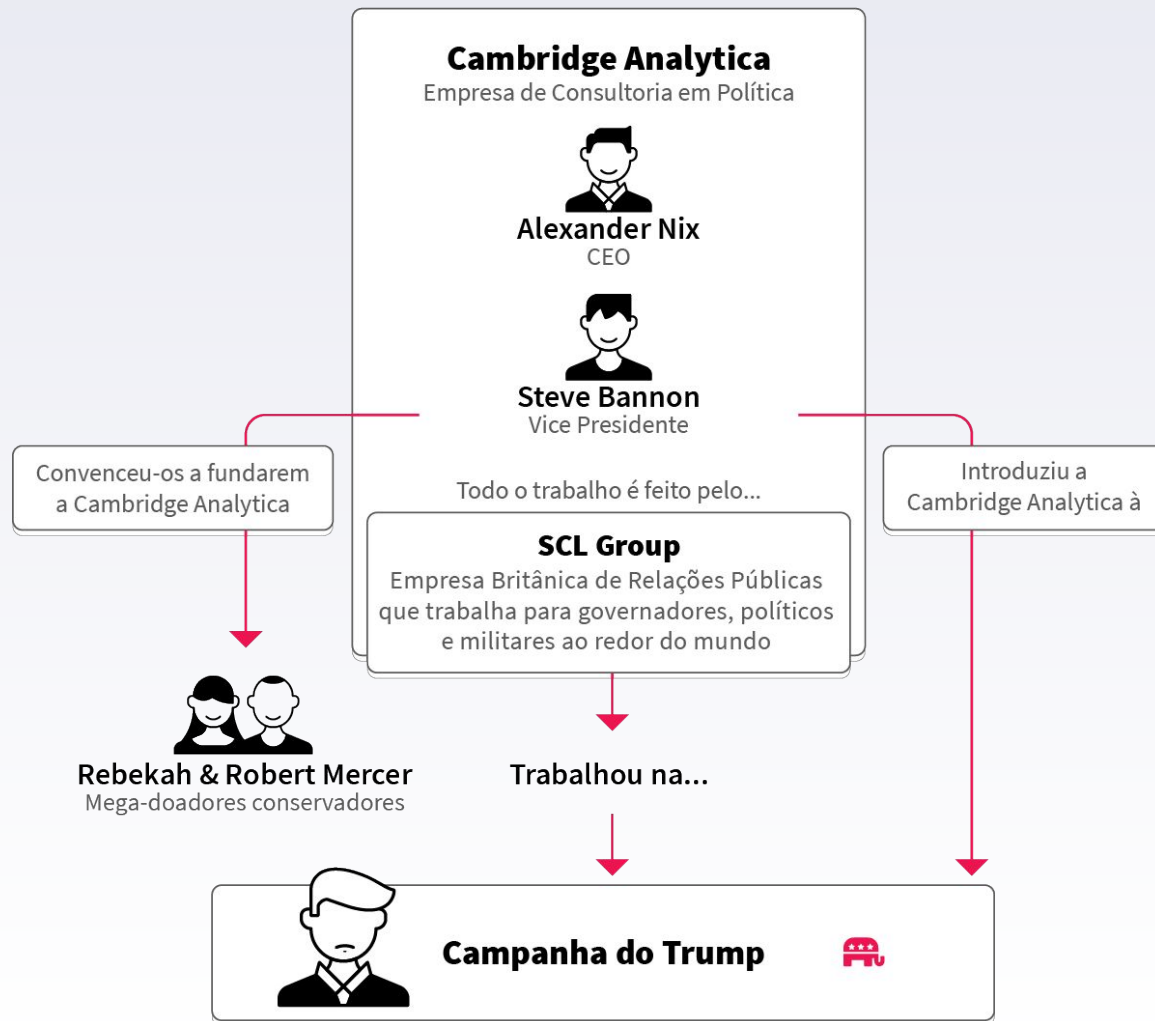
$\equiv . \alpha \cap \beta = \Lambda \quad (1)$

$\vdash . (1) . *11.11.35 . \supset$

$\vdash : (\exists x, y) . \alpha = \iota'x . \beta = \iota'y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda \quad (2)$

$\vdash . (2) . *11.54 . *52.1 . \supset \vdash . \text{Prop}$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.



Até 87 milhões de usuários do  Facebook
Tiveram seus dados expostos



Data crua exposta de até 87 milhões de perfis para a...




Cambridge Analytica
Empresa de Consultoria em Política

Usadas na...



Campanha do Trump



Até 87 milhões de usuários do  Facebook
Tiveram seus dados expostos



**270 mil usuários do Facebook
responderam uma pesquisa**



Eles usaram um App específico...



thisismydigitallife

App de Perguntas no Facebook



OPINION

Facebook is not free

The economics of much of the Internet is built on two valuable commodities: your time, and your content

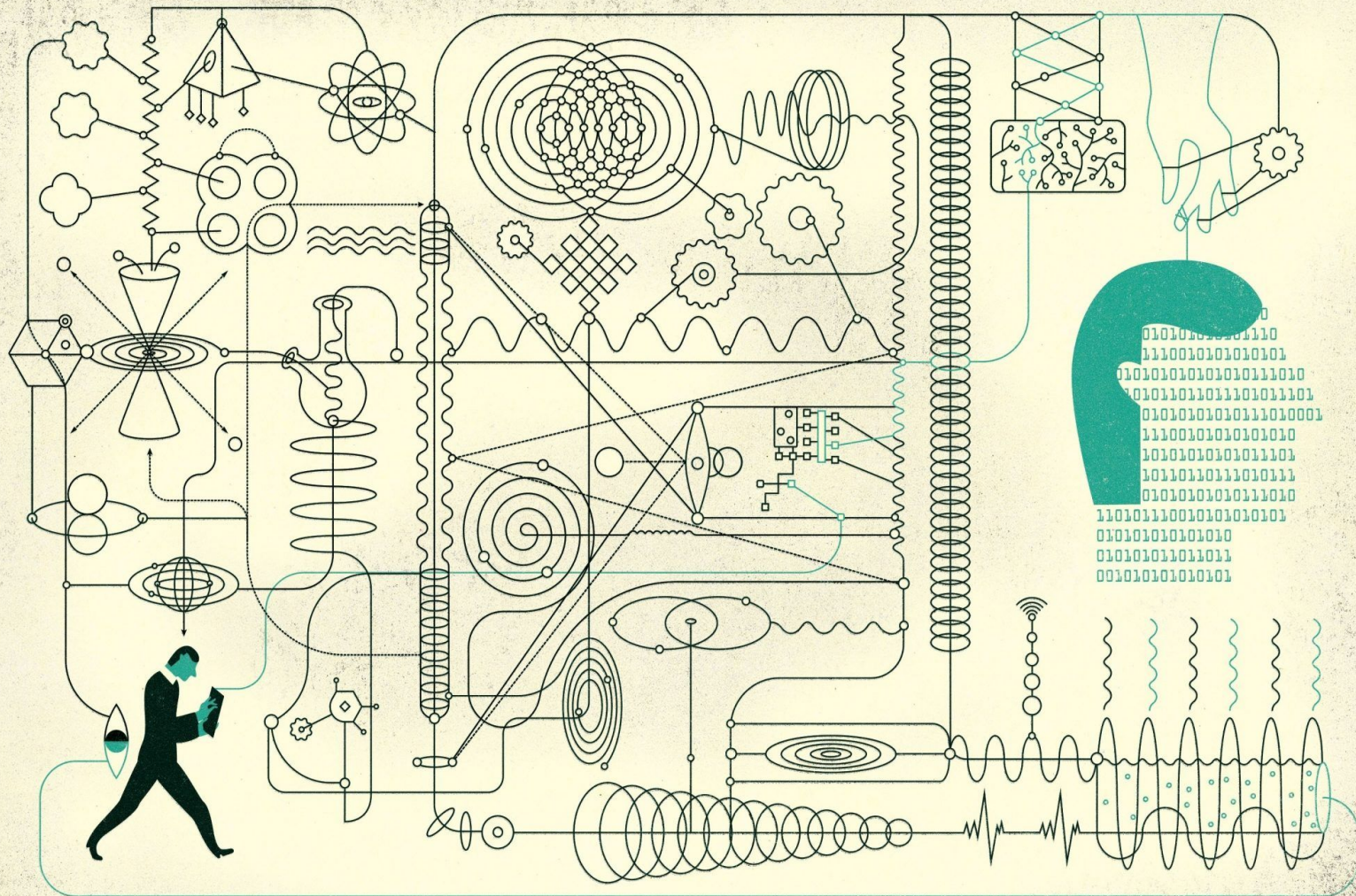


By Ira Winkler

Contributing Columnist, Computerworld

OCT 17, 2011 5:24 PM PST

**se você
não paga,
você é o
produto.**



fontes [aqui](#) e [aqui](#)

A NETFLIX ORIGINAL DOCUMENTARY

THE GREAT HACK

From the Academy Award
nominated filmmakers behind **THE SQUARE**



NOW STREAMING | NETFLIX

Medidas Imediatas (Curto Prazo)





Nomeação de **Data Protection Officer**, quando obrigatório

Realização de **Análise de Impactos de Proteção de Dados**

Certas **violações de dados** deverão ser reportadas

Algumas empresas do BR devem **nomear representantes na UE**

Proteção de dados como padrão e desde a **concepção** das aplicações

Multas de até €20 milhões ou 4% do faturamento anual

Possibilidade de abrangência a empresas brasileiras

Transparência, limitação da finalidade e minimização dos dados ...

Exigências mais rígidas para o **consentimento** junto ao titular dos dados

Dados incorretos/desatualizados devem ser **retificados**

Os dados não mais necessários deverão ser **excluídos**

Titular pode levar seus dados a outras empresas



Utilizando GDPR como base

LGPD é baseada na lei europeia **G**eneral **D**ata **P**rotection **R**egulation

Ambas são leis modernas, baseadas em princípios e direitos similares

Incentivam mudança na cultura (pessoas)

Existem diversas experiências com GDPR que servem de base para LGPD

<https://gdprchecklist.io/> · <https://www.portaldaprivacidade.com.br/home/categories/infoqr%C3%A1ficos-e-cartilhas>
<https://github.com/erichard/awesome-gdpr> · <https://github.com/bakke92/awesome-gdpr>

CONTEÚDO

CAPÍTULO 1 [Resumo](#)
Disposições Preliminares [↗](#)

CAPÍTULO 2 [Resumo](#)
Do Tratamento de Dados Pessoais [↗](#)

CAPÍTULO 3 [Resumo](#)
Dos Direitos do Titular [↗](#)

CAPÍTULO 4 [Resumo](#)
Do Tratamento de Dados Pessoais pelo Poder Público [↗](#)

CAPÍTULO 5 [Resumo](#)
Da Transferência Internacional de Dados [↗](#)

CAPÍTULO 6 [Resumo](#)
Dos Agentes do Tratamento de Dados Pessoais [↗](#)

CAPÍTULO 7 [Resumo](#)
Da Segurança e das Boas Práticas [↗](#)

CAPÍTULO 8 [Resumo](#)
Da Fiscalização [↗](#)

CAPÍTULO 9 [Resumo](#)
Da Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade [↗](#)

CAPÍTULO 10 [Resumo](#)
Disposições Finais e Transitórias [↗](#)

LGPD NA PRÁTICA

Desmistificamos interpretações da lei para te ajudar a entender como ela se aplica na prática. Consulte o texto completo da lei e veja comentários e vídeos feitos por especialistas no assunto.

Este conteúdo está em constante atualização, então adicione à sua lista de favoritos e volte sempre para ficar por dentro das novidades.

Simplificado por MAGRATHEA e Silva, Santana & Teoton Advogados

LEI GERAL DE PROTEÇÃO DE DADOS

CAPÍTULO 1 - DISPOSIÇÕES PRELIMINARES

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.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. [\(Incluído pela Lei nº 13.853 de 2019\) Vigência](#)

CAPÍTULO 1 - DISPOSIÇÕES PRELIMINARES

A disciplina da proteção de dados pessoais tem como fundamentos :

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.



WEBINAR LGPD NA PRÁTICA



QUAL O OBJETIVO DO LGPD NA PRÁTICA?



MAS AFINAL O QUE É A LGPD?



QUEM É QUEM NA LGPD?



QUAIS OS DADOS QUE A LGPD ABRANGE?





Minha organização precisa de um DPO (Encarregado)?

Independente de ser **controlador** ou **processador**, se sua **atividade principal** envolve o processamento de **dados sensíveis** em **larga escala** ou envolve **monitoramento de indivíduos regular e em larga escala**, a presença de um DPO é mandatória.

O que é um DPO (Encarregado)?

Data Protection Officer (pessoa física ou jurídica)

O DPO deve ter conhecimento **multidisciplinar**, conciliando temas das áreas de **tecnologia, gestão da informação e jurídica**, mas pode contar com o auxílio de comissões especializadas nestas áreas.

O DPO deve **responder às autoridades oficiais** e não deve possuir **conflitos de interesse** com a organização.

Denominado como **Encarregado** na lei brasileira.

Exemplos de organizações

DPO/Encarregado mandatário

um hospital processando **grandes conjuntos de dados sensíveis**

uma empresa de segurança responsável por **monitoramento** de espaços públicos

uma pequena empresa de recrutamento que traça **perfis de indivíduos**

DPO/Encarregado não mandatário

um médico local que processa dados dos pacientes

uma pequena empresa de advocacia que processa dados pessoais de seus clientes.

Técnicas e Ferramentas



Governança de dados



Governança de dados



- **Autoria:** de quem são os dados?
- **Acessibilidade:** quem pode acessar?
- **Segurança:** quais medidas e sistemas garantem a conformidade dos acessos?
- **Qualidade:** os dados estão estruturados e são rastreáveis?
- **Conhecimento:** agregam valor e tem um motivo para existir?

Anomização

“

Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Anomização

Strategy

Suppression

Random Substitution

Variance

Encryption

Shuffling

Faking / Mocking

Partial Suppression

Generalization

Data Types

All

All

Numeric / Dates

Text

All

All

Text

Numeric / Dates

When to use

Useless attributes

Useless attributes with integrity constraints

Analytics

Analytics / UNIQUE attributes

Analytics

Dev / CI / Functional Testing

Direct Identifiers

Analytics

Tecnologias
**GDPR COMPLIANT /
COMPLIANCE**



Exemplos de aplicações

Rails

https://github.com/prey/gdpr_rails

<https://github.com/ankane/ahov>

Redis

<https://redislabs.com/blog/dont-worry-happy-redis-labs-ready-gdpr/>

Postgres

<https://www.enterprisedb.com/>

Awesome Lists

<https://github.com/KevinColemanInc/awesome-privacy>

<https://github.com/nikitavoloboev/privacy-respecting>

<https://github.com/Kickball/awesome-selfhosted>

Hospedagem

AWS

<https://devcenter.heroku.com/articles/gdpr>

Azure

<https://azure.microsoft.com/en-us/blog/protecting-privacy-in-microsoft-azure-gdpr-azure-policy-updates/>

Heroku

<https://devcenter.heroku.com/articles/gdpr>

DigitalOcean

<https://www.digitalocean.com/legal/gdpr/>






























GDPR Tracker

Track the GDPR compliance of **+100** cloud services and subprocessors.



Search powered by [Algolia](#)

Track	Name	Status	HQ	Privacy	DPA	Subprocessors	Hosting partners	Data centers	Certifications	
<input type="checkbox"/>	 Amazon Web Serv...	<div></div>		Privacy	DPA		AWS	Global	EU-U.S. Privacy Shield ISO 27001 ...	Edit
<input type="checkbox"/>	 Officient 	<div></div>		Privacy			AWS	EU		Edit
<input type="checkbox"/>	 Netflix	<div></div>		Privacy			AWS	US		Edit
<input type="checkbox"/>	 PythonAnywhere 			Privacy	DPA		AWS	US	EU-U.S. Privacy Shield	Edit
<input type="checkbox"/>	 Lyft	<div></div>		Privacy			AWS	US		Edit
<input type="checkbox"/>	 Knowlex 	<div></div>		Privacy			AWS	EU		Edit
<input type="checkbox"/>	 Booking.com	<div></div>		Privacy			AWS	EU		Edit
<input type="checkbox"/>	 Baremetrics	<div></div>		Privacy			AWS	US	EU-U.S. Privacy Shield Swiss-U.S. Privacy Shield	Edit
<input type="checkbox"/>	 SupportHero			Privacy		Subprocessors	AWS	EU		Edit
<input type="checkbox"/>	 Hubspot	<div></div>		Privacy	DPA		AWS		EU-U.S. Privacy Shield ISO 27001 ...	Edit
<input type="checkbox"/>	 Airtable			Privacy			AWS	US	SOC 1 SOC 2 Type I ...	Edit
<input type="checkbox"/>	 Grammarly			Privacy			AWS	US	Swiss-U.S. Privacy Shield EU-U.S. Privacy Shield	Edit

Nossas Experiências



Desafios

OBTENÇÃO DE CONSENTIMENTO

Adquirir consentimento para uso de cookies e envio de e-mail marketing

Clientes de clientes

Desafios

OBTENÇÃO DE CONSENTIMENTO

Adquirir consentimento para uso de cookies e envio de e-mail marketing

Clientes de clientes

ACESSIBILIDADE

Developers não tem mais acesso a contas de usuários

Desafios

OBTENÇÃO DE CONSENTIMENTO

Adquirir consentimento para uso de cookies e envio de e-mail marketing

Clientes de clientes

ACESSIBILIDADE

Developers não tem mais acesso a contas de usuários

DIREITO DE SER ESQUECIDO

Remoção de dados (em até 7 dias)

Construção de interface para edição, deleção ou download dos dados

Clientes de clientes

Preocupações

Imagem/marketing

Preocupações

Imagem/marketing

Relações comerciais

Preocupações

Imagem/marketing

Relações comerciais

Produtividade

Preocupações

Imagem/marketing

Relações comerciais

Produtividade

Desempenho

Preocupações

Imagem/marketing

Relações comerciais

Produtividade

Desempenho

Escalabilidade

Soluções

OBTENÇÃO DE CONSENTIMENTO

Double Opt-in para conversão de Leads

Cookie consent para rastreamento

Soluções

OBTENÇÃO DE CONSENTIMENTO

Double Opt-in para conversão de Leads

Cookie consent para rastreamento

ACESSIBILIDADE

Anonimização dos dados

Soluções

OBTENÇÃO DE CONSENTIMENTO

Double Opt-in para conversão de Leads

Cookie consent para rastreamento

ACESSIBILIDADE

Anonimização dos dados

DIREITO DE SER ESQUECIDO

Foco em qualidade

Gerenciar consentimento

Nem todos os dados precisam ser deletados. Alguns podem ser mantidos em **legítimo interesse**, porém, sempre busque o **consentimento**.

Dicas

Pensamento sistêmico

Dicas

Pensamento sistêmico

Princípios

Dicas

Pensamento sistêmico

Princípios

Framework de governança de dados

Dicas

Pensamento sistêmico

Princípios

Framework de governança de dados

Pessoas > Processos/Tecnologia

Dicas

Pensamento sistêmico

Princípios

Framework de governança de dados

Pessoas > Processos/Tecnologia

Disseminação de conhecimento (mudança na cultura)

Dicas

Pensamento sistêmico

Princípios

Framework de governança de dados

Pessoas > Processos/Tecnologia

Disseminação de conhecimento (mudança na cultura)

Desenvolver pensando em dados (data-driven)

Dicas

Pensamento sistêmico

Princípios

Framework de governança de dados

Pessoas > Processos/Tecnologia

Disseminação de conhecimento (mudança na cultura)

Desenvolver pensando em dados (data-driven)

Transparência e boa vontade de estar em conformidade

Tendências: Priorizando Privacidade (Longo Prazo)





OP-ED

By 2030, You'll Be Living in a World That's Run by Google

And it may be both the best and worst thing to happen to humanity.

[fonte](#)

Privacy by Design / Privacy by Default

★ Recomendado pela GDPR

GDPR Privacy by Design

"Privacy by Design" and "Privacy by Default" have been frequently-discussed topics related to data protection. The first thoughts of "Privacy by Design" were expressed in the 1970s and were incorporated in the 1990s into the RL 95/46/EC data protection directive. According to recital 46 in this Directive, technical and organisational measures (TOM) must be taken already at the time of planning a processing system to protect data safety.

[fonte](#)

Privacy by Design / Privacy by Default

X Criticado por ser muito vago

Engineering Privacy by Design

Seda Gürses, Carmela Troncoso, and Claudia Diaz

K.U. Leuven/IBBT, ESAT/SCD-COSIC
firstname.lastname@esat.kuleuven.be

Local-First / Offline-First

Local-First Software: You Own Your Data, in spite of the Cloud

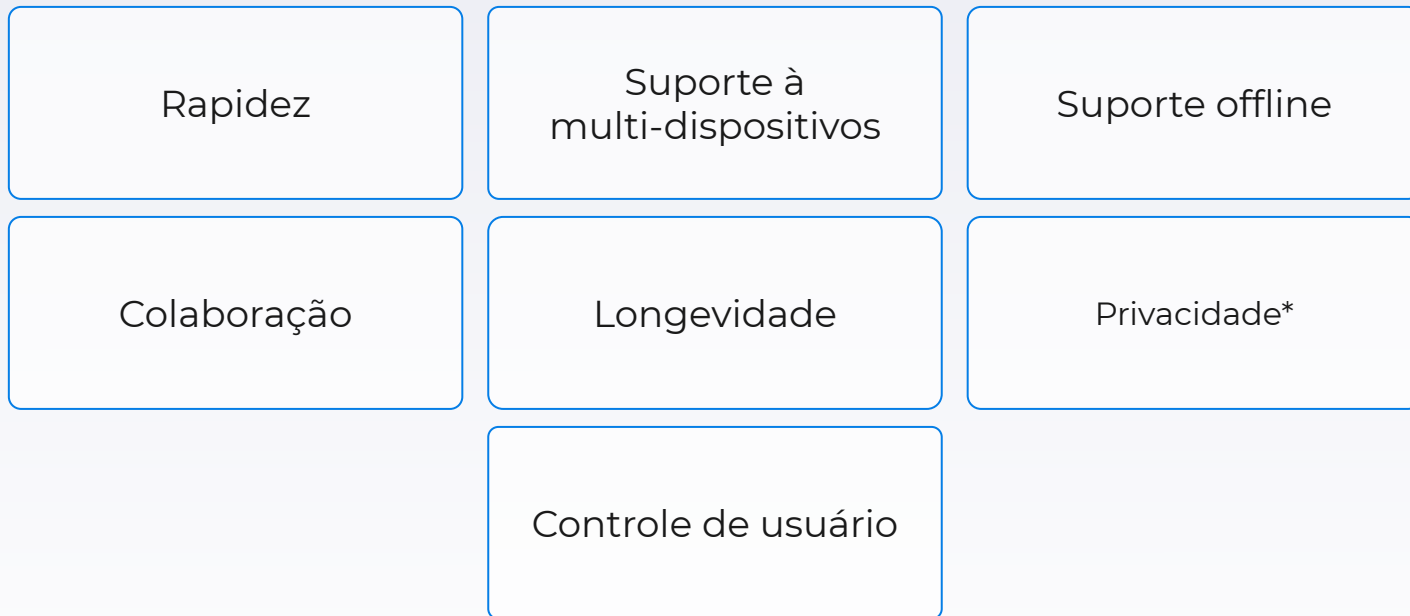
Martin Kleppmann
Department of Computer Science and Technology
University of Cambridge
Cambridge, United Kingdom
martin.kleppmann@cl.cam.ac.uk

Peter van Hardenberg
Ink & Switch
San Francisco, CA, USA
pvh@inkandswitch.com

Adam Wiggins
Ink & Switch
Berlin, Germany
adam@inkandswitch.com

Mark McGranaghan
Ink & Switch
Seattle, WA, USA
mark@inkandswitch.com

Local-First / Offline-First

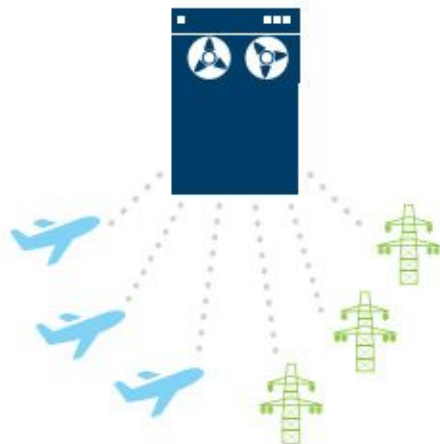


* aplicativos na nuvem são **fundamentalmente não-privados**

Quer ser dono dos seus dados?
Comece pela sua **identidade digital**



Before 2005



Closed and centralized
IoT networks

Today



Open access IoT networks,
centralized cloud

2025 and beyond



Open access IoT networks,
distributed cloud



2025 and beyond



Open access IoT networks,
distributed cloud

Obrigado!

MAGRATHEA

www.magrathealabs.com / github.com/laurogripa/presentations