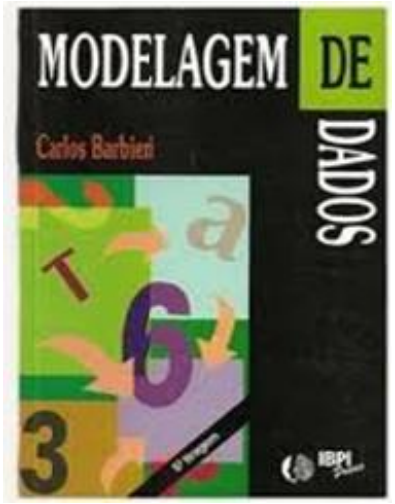
LGPD como Governança de Dados

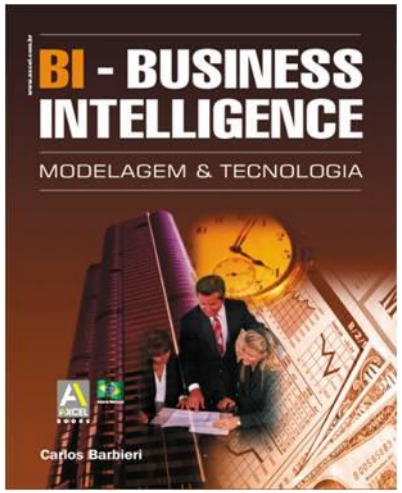
Carlos Barbieri
CBCA-Carlos Barbieri Consultores Associados

02/12/2020

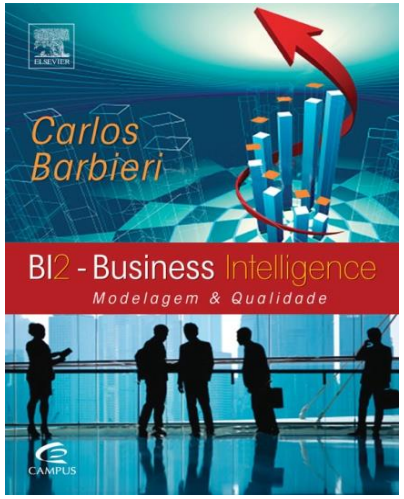
- Carlos Barbieri, Eng, 1970-MSc-INPE-1974, PG Informática-1975
- Cemig-30 anos na área de Dados(ABD,AD,BI), Gerente da Assessoria de Tecnologia **, BUG do Milênio**
- Professor de Pós-Graduação da PUC-MG na área de Dados e Data Governance, desde 2005
- Consultoria e treinamento em diversas empresa em Portugal e no Brasil
- Consultor de Processos e Dados- diversas empresas no BR
- Coordenador da área de Qualidade da Fumsoft-Sociedade Mineira de Software, responsável pelo Programa MPS.BR
  - Engenharia de Software-MPS.BR e Governança e Qualidade de Dados
- Revisor convidado do Modelo DMM-Data Management Maturity Model-CMMI e do DMBoK® V2-USA
- Participou da equipe de tradução do DMM para português
- CDMP-Certified Data Management Professional-DAMA-Data Management Association- CBIP(TDWI) e CDMP em DM, DW,DD,DOIP,DGS
- Participa da equipe de elaboração das provas CDMP-Dama-DMBoK- DAMA-International-USA
- Trabalhos de GD: Prodemge(MG), Petrobrás(RJ), FIEMG(MG), CEMIG(MG), NeoGrid(RS), etc
- Autor de 4 livros na área de Dados, Informações, BI e GD



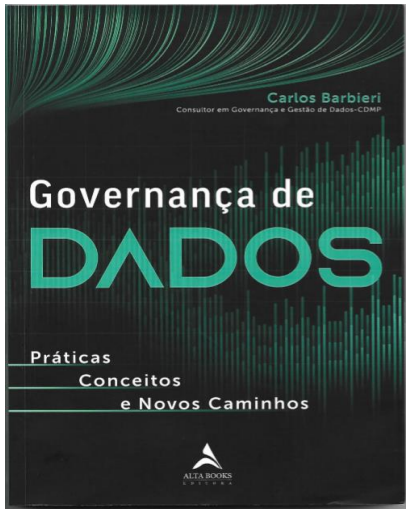
(1994)



(2002)



(2011)



(2020)

GD e LGPD

- Sobre cultura de dados
- LGPD e DMBoK
- Visões: Data Governance e Data Vênia
- 6 passos importantes
- 2 pontos críticos
- Conclusão

4ª revolução industrial

DADOS

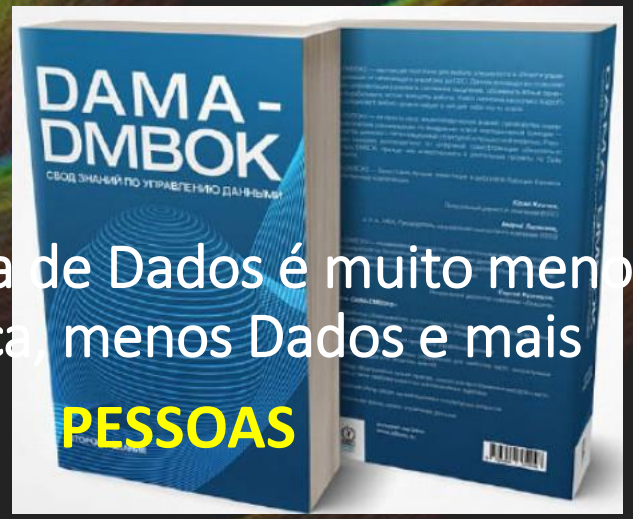
ESTRATÉGIA DE DADOS-DATA DRIVEN-DATA CENTRIC

“A melhor estratégia pode ser engolida pela Cultura da organização no café da manhã”-Peter Drucker

CULTURA DE DADOS

Não é somente o melhor Consumo de dados

FIND-UNDERSTAND-TRUST-PROTECT



Governança de Dados é muito menos Governança, menos Dados e mais **PESSOAS**

Cap. 17-Sobre Mudança Cultural

LEI LGPD

Sancionada em 18 de Setembro de 2020- Vigência
Penalidades em Agosto de 2021

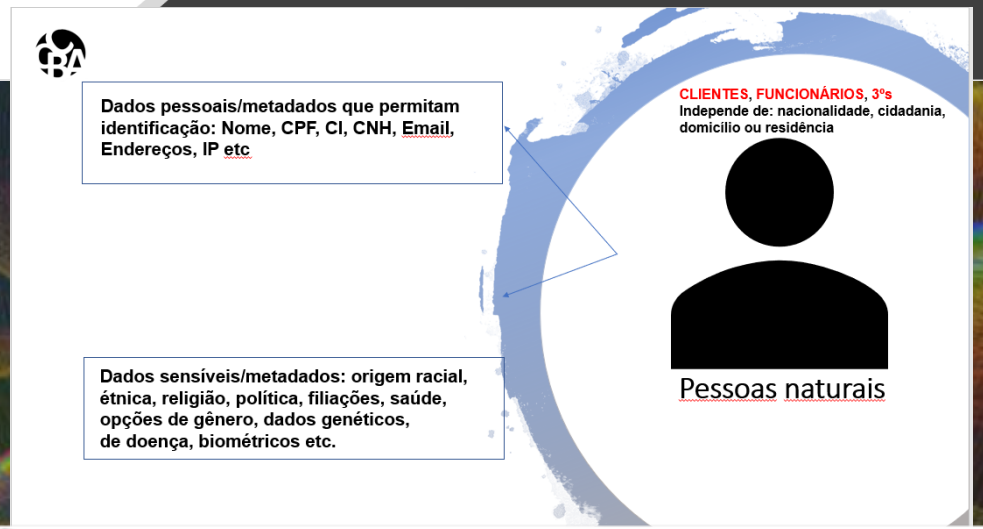
Patrocinador

“Se a cultura ainda tem certa resistência ao controle dos Dados”

LGPD e GD

LGPD-Lei Geral de Proteção de Dados

- Objetiva dar maior ***garantia aos dados das pessoas naturais*** , assegurando o direito à privacidade e à proteção dos dados pessoais
  - Regras claras para a empresa sobre **tratamento** de dados: coleta, produção, recepção, armazenamento, uso, compartilhamento etc. de dados pessoais (Artigo 5 Inciso X)
- Inspiração na GDPR-União Europeia
- Dividida em 10 capítulos



Artigo-17-Direitos do Titular

Artigo-46-49-Segurança-Sigilo

Artigo-41-DPO-Encarregado

Artigo-20-Decisões automatizadas

Artigo-16-Eliminação de dados

Artigo-12-Dados anonimizados

Artigo-50-51-Boas práticas e Governança

Artigo-18-Direitos de saber/obter seus dados

LGPD é um programa

Fonte de Imagem: NYTimes.com

Governança de DPN-Dados de Pessoas Naturais

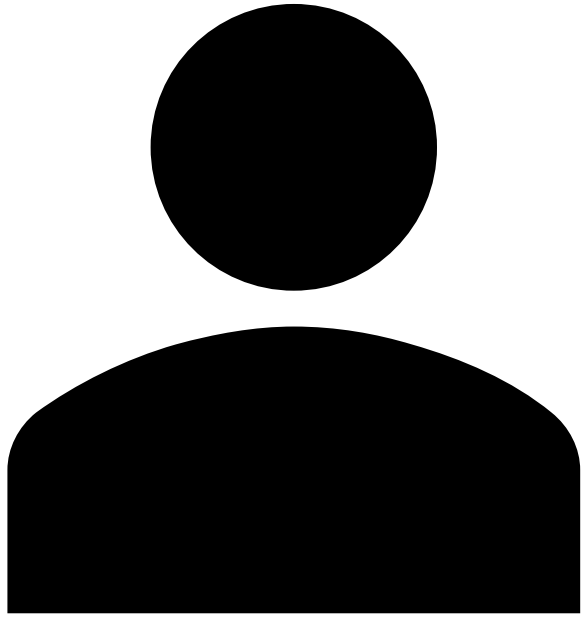
Lei Geral de Proteção de Dados-LGPD 13709/2018

LGPD-Penal-Segurança Pública e Investigação criminal

Dados pessoais/metadados que permitam identificação: Nome, CPF, CI, CNH, Email, Endereços, IP etc

Dados sensíveis/metadados: origem racial, étnica, religião, política, filiações, saúde, opções de gênero, dados genéticos, de doença, biométricos etc.

CLIENTES, FUNCIONÁRIOS, 3ºs, Visitantes
Independe de: nacionalidade, cidadania, domicílio ou residência



Pessoas naturais

Artigo 5-Parágrafo I-dado pessoal:
Informação relacionada à pessoa natural
IDENTIFICADA ou **IDENTIFICÁVEL**

Multas-GDPR
Maiores multas

- Google-50 milhões de Euros-Jan/2019
- TIM-27,8 milhões de Euros-Janeiro/2019
- H&M-27 milhões de Euros-Out/2019
- British Airways-20 milhões de Euros-Julho/2019
- Marriot International-18,4 milhões de Euros-Outubro/2020
- **+ Recente: TicketMaster UK-1.5 milhão de Euros-Novembro/2020**

Sanções no LGPD

MPDFT ajuíza 1ª ação civil pública com base na LGPD

Publicado: 22/09/2020 às 7:27

Compartilhar Tweet

Iniciativa é contra empresa de informática especializada em comercializar dados cadastrais de usuários

O Ministério Público do Distrito Federal e Territórios ofereceu a primeira ação civil pública com pedido de tutela, baseada na Lei Geral de Proteção de Dados Pessoais, nesta segunda-feira, 21 de setembro. A lei, que entrou em vigor na sexta-feira, enquadra como lesiva a conduta de uma empresa sediada em Belo Horizonte (MG).

De acordo com a ação movida pela Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec) do MPDFT, a empresa comercializa informações pessoais como nomes, e-mails, endereços postais ou contatos para SMS, bairro, Cidade, Estado e CEP's das vítimas por meio de site na internet. Acredita-se que só em São Paulo, 500 mil pessoas nascidas no município tenham sido expostas indevidamente. Foram identificadas vítimas em todas as unidades da Federação.

O site da empresa oferece, por exemplo, dados segmentados por profissões, como cabeleireiros, corretores, dentistas, médicos, enfermeiros, psicólogos, entre outros. Os "pacotes" eram vendidos de R$ 42 a R$ 212,90.

Por causa do prejuízo supraindividual que a atividade pode causar, o MPDFT requereu à Ju
Isso porque, pela LGPD, o tratamento dado às informações cadastrais foi totalmente irreg
ação destaca ainda que o direito à intimidade, à privacidade e à imagem, garantidos pela Co

O MPDFT pede que a empresa se abstenha de divulgar, de forma paga ou não, os dados
congelamento imediato do domínio do site em que é feita a comercialização, até que haja jul

Íntegra da ação civil pública.

Quebra de sigilo

Senha vaza e dados de 16 milhões de pacientes de covid são expostos

Funcionário do Albert Einstein divulgou na internet acesso aos bancos de dados do Ministério da Saúde; autoridades como Bolsonaro, Doria e ministros tiveram privacidade violada

- Capacidade de hospitais está menor e podemos chegar mais rápido ao colapso, diz pesquisador
- Puxado pelos EUA, mundo registra recorde diário de mortes por covid-19

Semana passada

Quebra de sigilo

Nova falha do Ministério da Saúde expõe dados pessoais de mais de 200 milhões de brasileiros

02/12/2020

Erro em sistema federal de registro de casos de covid permitiu acesso, durante seis meses, a informações pessoais de todos os cadastrados no SUS e clientes de plano de saúde

Vazamento de dados da Enel atinge 300 mil clientes em São Paulo

Concessionária diz que casos estão concentrados na cidade de Osasco e já começou a alertar potenciais envolvidos sobre o vazamento das informações

Da Redação, editado por Daniel Junqueira 11/11/2020 13h02

serasa experiar

Justiça determina suspensão de vendas de dados de consumidores pela Serasa

Segundo o Ministério Público, Serasa Experian oferecia serviço que fere a LGPD (Lei Geral de Proteção de Dados)

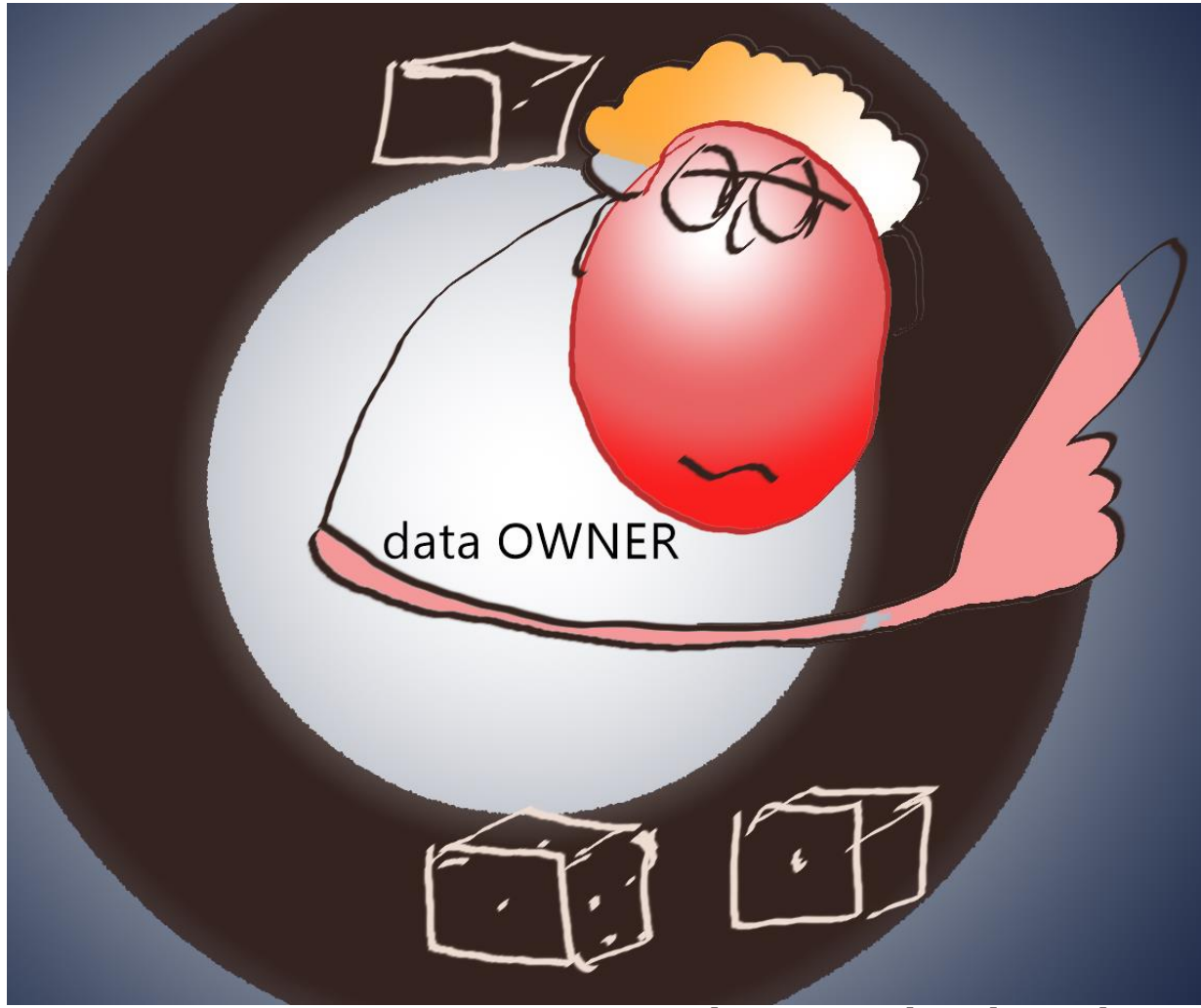
Imagem: Reprodução/YouTube

Do UOL, em São Paulo

23/11/2020 19h12 | Atualizada em 24/11/2020 10h59

Fonte: https://olhardigital.com.br/noticia/em-sp-enel-vaza-dados-pessoais-e-bancarios-de-300-mil-clientes/110074#:~:text=Dados%20de%20cerca%20de%20300,base%20da%20cidade%20de%20Osasco

LGPD-BR-Lei Geral de Proteção de Dados



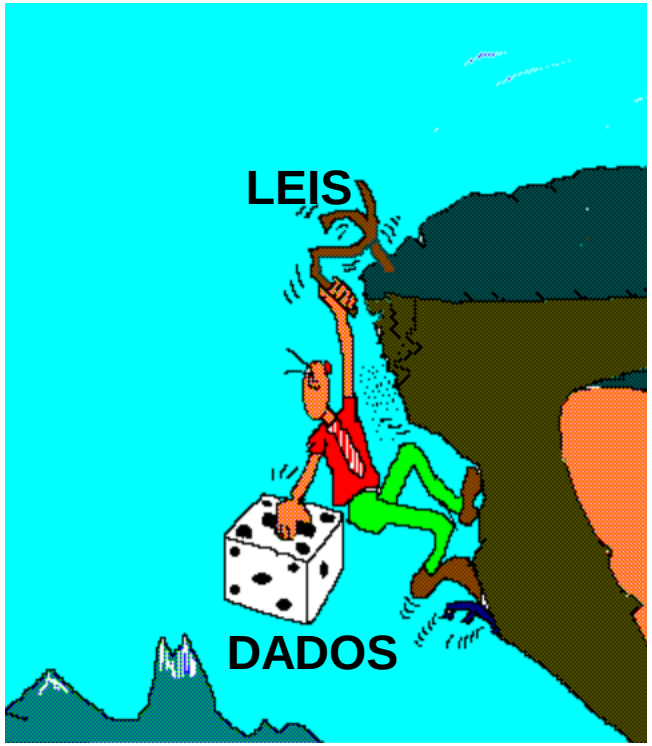
LGPD: 2% do Faturamento da empresa *até* R$50 milhões de reais

GDPR: Multa: 20 milhões de Euros ou 1 a 4% da Receita anual do último exercício(*o que for maior*)

CCPA: US$2.500-US$7.500,00/ Californian Consumer-*Cambridge Analytica* - FB: 24 mi de CC US$60-US100 Bilhões

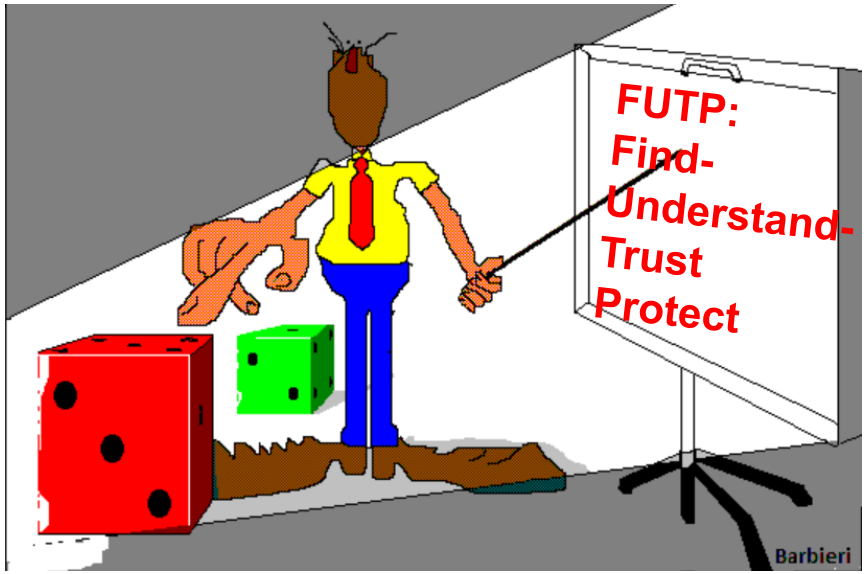
HOW MUCH-Grande patrocinador-Risco pecuniário e reputacional

LGPD-Conceitos fundamentais



LGPD:
2 áreas de Conhecimentos
que implicam Riscos

Dados



Data Culture
Data Governance
-Qualidade
-Metadados
-Linhagem de dados

Jurídico

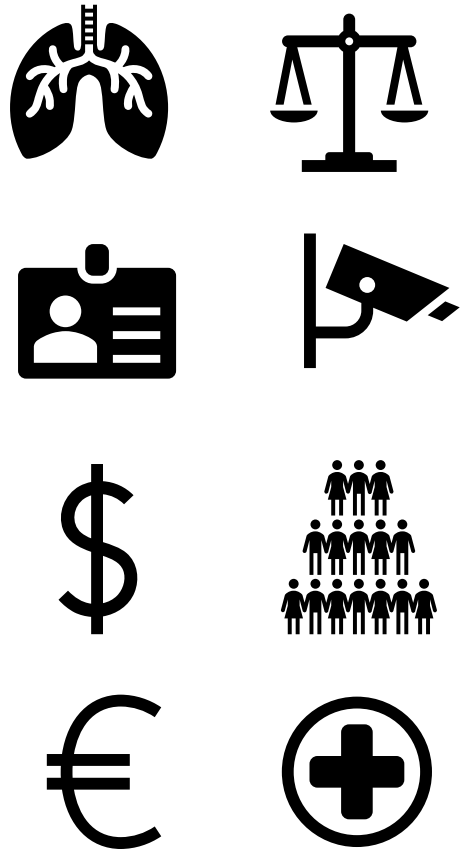
Data Venia

- (Zonas cinzentas da Interpretação)
  Aguardar Jurisprudência
  Posição ANPD

JURÍDICOS DADOS

Bases Legais

- ***Consentimento***
- ***Legítimo interesse***
- Obrigação legal
- Procedimentos Judiciais e administrativos
- Contratos e termos
- Situações de riscos de vida(Proteção da vida)
- Tutela da saúde
- Proteção ao Crédito
- Interesse/políticas públicas



LGPD-Conceitos fundamentais

6
Passos

Mix de trabalho de Data Governance e Data Venia(JR)

LGPD-Passos fundamentais

1

Mapeamento de Dados

Data Mapping

Áreas ou Processos de negócios

- **Which/What** - Quais ***dados e metadados*** de Pessoas naturais
- **Where** - Onde estão sendo usados, transferidos(interna ou externa)
- **Who** – Quem responde por isso
- **How** - Processos-Como o tratamento está sendo feito
- **Why** - Com que objetivos e bases legais

GD

2

Bases legais de uso

- ***Consentimento(+ forte), porém pode ser revogado***
- ***Legítimo interesse do Controlador ou 3ºs (- forte), mais subjetivo***

JR

LGPD-Passos fundamentais

3

Legítimo interesse

- Buscar o equilíbrio entre os (**interesses comerciais** e as atividades da empresa, com aquele dado) **com *as expectativas das pessoas naturais e os seus direitos básicos***
- Teste de **proporcionalidade** que envolve ***Objetivos*** e ***Necessidades***
- (Propósito x Proporção)

JR

Dos que apontaram **BL** como ***LI***, faz-se um **LIA-Assessment**

4

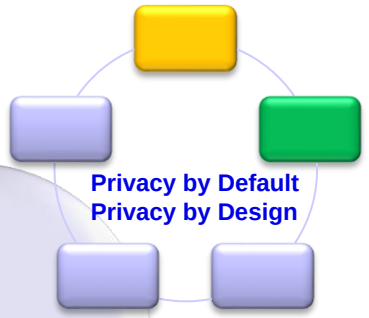
Descoberta física dos dados

Data Discovery

- ***Complementação do Passo 1***
- Confirmação dos dados e metadados nas fontes sugeridas
- ***Ação mais tecnológica, envolvendo ferramentas/ações de GD:***
- ***Discovery, Metadados, Qualidade(profiling, cleansing), Catálogo de dados***

GD

LGPD-Passos fundamentais



5

Avaliação de impacto de Privacidade dos dados

DPIA-Data Privacy Impact Assessment

- Visão contínua de GD sobre os novos movimentos de uso de dados DPN
- ***Espécie de default a partir do movimento inicial***
- ***Avaliar o impacto das novas iniciativas: novo projeto, novo sistema, novo produto - devem fazer um DPIA(RIPD)***
- ***Mesmos dados coletados no Gap inicial***
- ***Detalhes do "Privacy by Default e Design"***

GD

CAP-1 Lei objetivos Art-1 Pag-01

CAP-1 Fundamentos Art-2 Pag-01

CAP-1 Operação de tratamento Art-3 Pag-01

CAP-1 Não se aplica LGPD-Art-4 Pag-01

CAP-1 Definições Art-5 Pag-02

CAP-1 Princípios Art-6 Pag-03

CAP-2 Requisitos p/ Tratamento de dados Art-7 Pag-04

CAP-2 Consentimento-Art-8 Pag-05

CAP-2 Direito do Titular Art-9 Pag-05

CAP-2 Legítimo interesse Controlador art-10 Pag-06

CAP-2 Dados sensíveis-Hipóteses tratamento Art 11 Pag-06

CAP-2 Dados anonimizados-Art-12 Pag-07

CAP-2 Estudos Saúde Pública Art-13 Pag-07

CAP-2 Crianças e Adolescentes Art-14 Pag-07

CAP-2 Encerramento Art-15 Pag-08

CAP-2 Eliminação de DPN-Art-16 Pag-08

CAP-3 Direito do Titular Art-17 Pag-08

CAP-3 Direito de saber/obter Pag-09

P´s da GD

Conjunto de P´s da GD: Políticas, Procedimentos, Padrões

Plataformas:

Data Mapping-Data Discovery-Web Site-Catálogo de dados

Pessoas-Papéis:

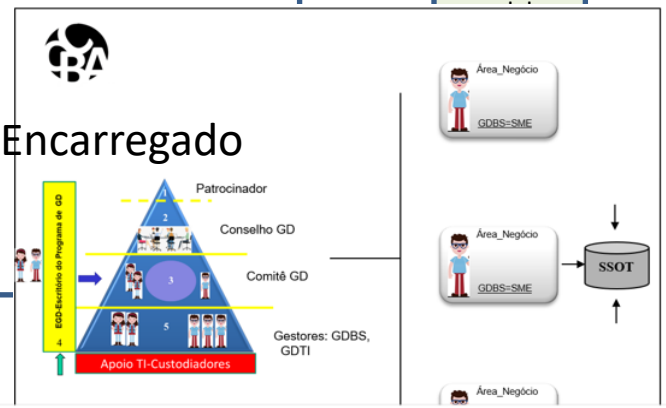
Encarregado-DPO-Agentes/Gestores Segurança/Gestores de dados

Patrocínio:

Pronto

6

DPO-Encarregado



CAP-10 Dispostivos finais Art-60-65 Pag-22

CAP-9 ANPD-CNPD Art-55-59 Pag-18

CAP-8 Fiscalização Art-52-54 Pag-16

CAP-7 Boas práticas e Governança Art-50-51 Pag-16

CAP-7 Segurança &Sigilo Art-46-49 Pag-15

Pag-13 Responsabilidade. Ressarciment

Pag-13 DPO-Encarregado

Pag-13 Agentes tratamentos-

Pag-12 Transferência internacional-

Pag-10 LGPD-Poder Público-

PONTOS DE ATENÇÃO

LGPD-Direitos do titular

Políticas-Normas/Padrões/Procedimentos

Direitos

- Direito à notificação de vazamento/violações
  - GDPR: 72 h - BR: tempo “razoável”
- Direito ao acesso aos seus dados
- Direito ao conhecimento de ***como*** e ***por quem*** os seus dados são processados
- Direito à explicação do uso (***para que***)
- Direito ao esquecimento (eliminação) (*)
- Direito à portabilidade (troca) (*)
- Direito à explicitação de uso por consentimento de forma inteligível
  - Separado para dados sensíveis
- Direito à revogação gratuita e facilitada(*)
- Direito a qualidade dos dados
- Direito à revisão de decisões automatizadas
- Direito à privacidade por projeto(privacy by design)
- Observar técnicas de anonimização de dados

GD

(*)-Sujeito a considerações

GD 2.0 Expansão de Escopo

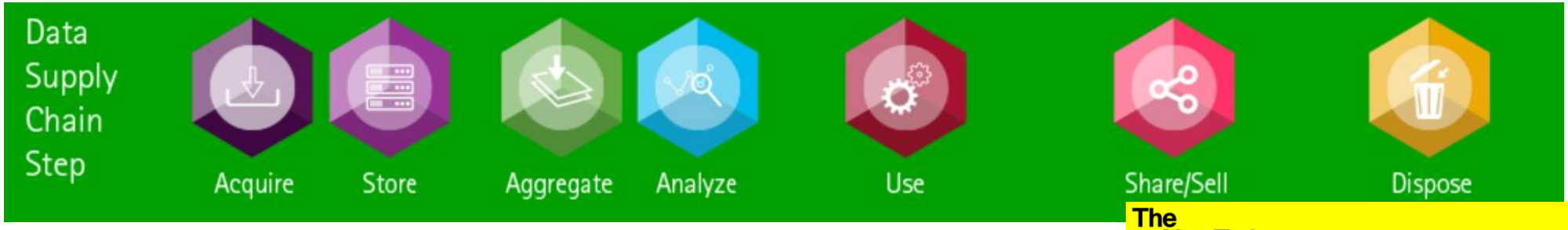
- Computação em Nuvem
- Data Lakes
- ETL (Data Wrangling)
- SSBI
- Metadados
- Privacidade e Ética

Fonte da imagem: NYTimes.com

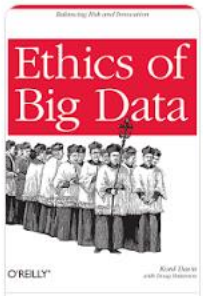
Dado-Sociedade Digital-Transformação Digital

- Pesquisa-USA:
  - 2018-Backup e Archive de **DPN**-*10%* empresas avaliavam como risco
  - 2020- **70%** empresas avaliam como risco
  - ----------
  - 2021-As empresas preveem **100%** a mais de multa por aspectos de PRIVACIDADE e ÉTICA DE DADOS
  - 2022-**70%** dos problemas de Privacidade serão por aspectos de (***falta de controle de***) Ética/privacidade nos dados
  - 2023-**75%** das grandes empresas terão papel de "avaliadores de IA", visando reduzir os riscos das decisões automatizadas (Artigo-20-LGPD-Decisões automatizadas)

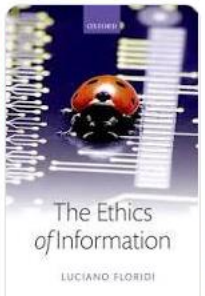
Kelle O´Neal-Curso de NGDG-Nova Geração de Governança de Dados-GD 2.0-Dataversity-2019



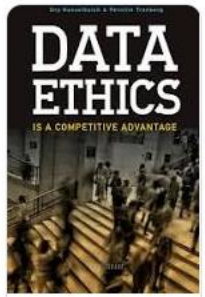
ACCENTURE: https://www.accenture.com/ro-en/insight-data-ethics



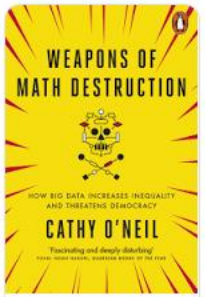
Ethics of Big Data: Balancing...



The Ethics of Information



Data Ethics: The New Com...



Weapons of Math Destruction

Ethics and Data Science

Big Data and Ethics: The Medi...

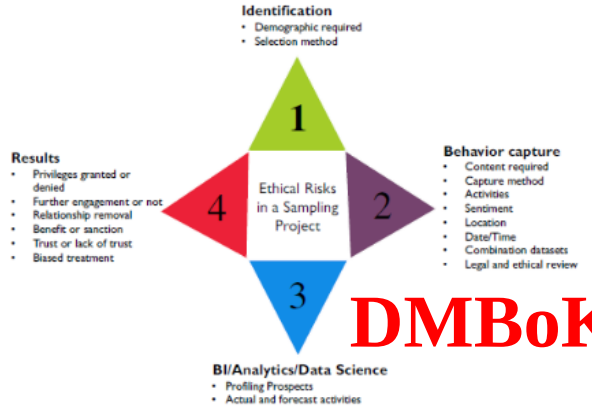
The Data Ethics Canvas

Use the Data Ethics Canvas to help you identify and manage ethical issues in your data project

The Alan Turing Institute

UK

Home + Research + Publications & policy submissions



DMBoK2

Figure 13 Ethical Risk Model for Sampling Projects

ÉTICA

LGPD: Artigo 2-Princípios/Fundamentos

Essa sensibilização já chega à Sociedade

NetFlix-Privacidade "hackeada"-2019

NetFlix-O Dilema das Redes Sociais-2020

Cambridge Analytica

Segurança e Privacidade

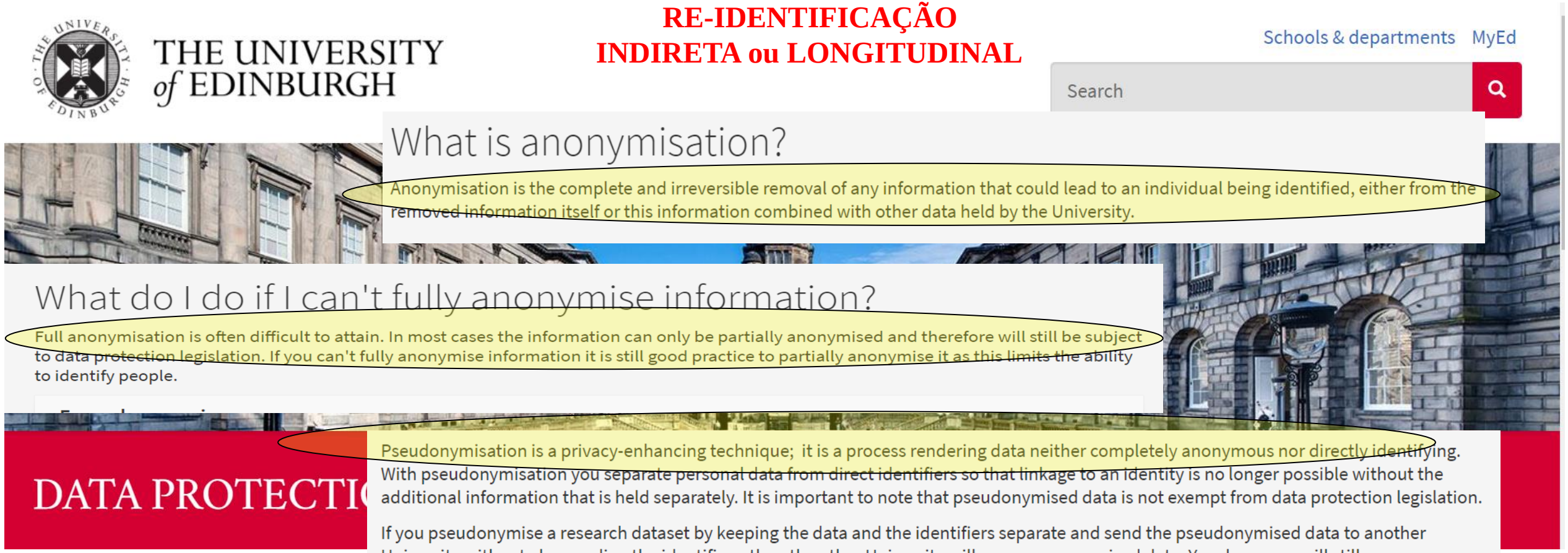
Anonimização-Pseudonimização

1

Anonimização e Pseudonimização

- Lei LGPD e GDPR- isenta dos controles os ***dados anonimizados*** , mas não os **pseudonimizados**
- Entretanto a sutileza o conceito de anonimização...

RE-IDENTIFICAÇÃO
INDIRETA ou LONGITUDINAL



Anonimização

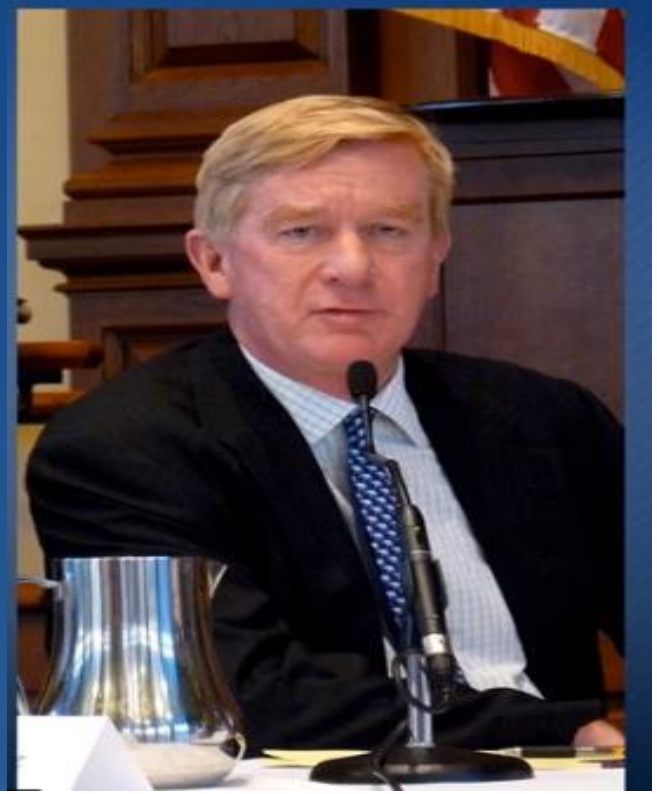
Descoberta indireta

Massachusetts Re-identification

Comissão estadual de
Seguros Gerais de Massachussets,
liberou registros abertos contendo
zip-code, data de nascimento e sexo de segurados

Pesquisadora ***Latanya Sweeney*** usou os dados
para localizar os registros de saúde do
Governador **William Weld**, incluindo
diagnósticos e prescrições

87,1%-ReID



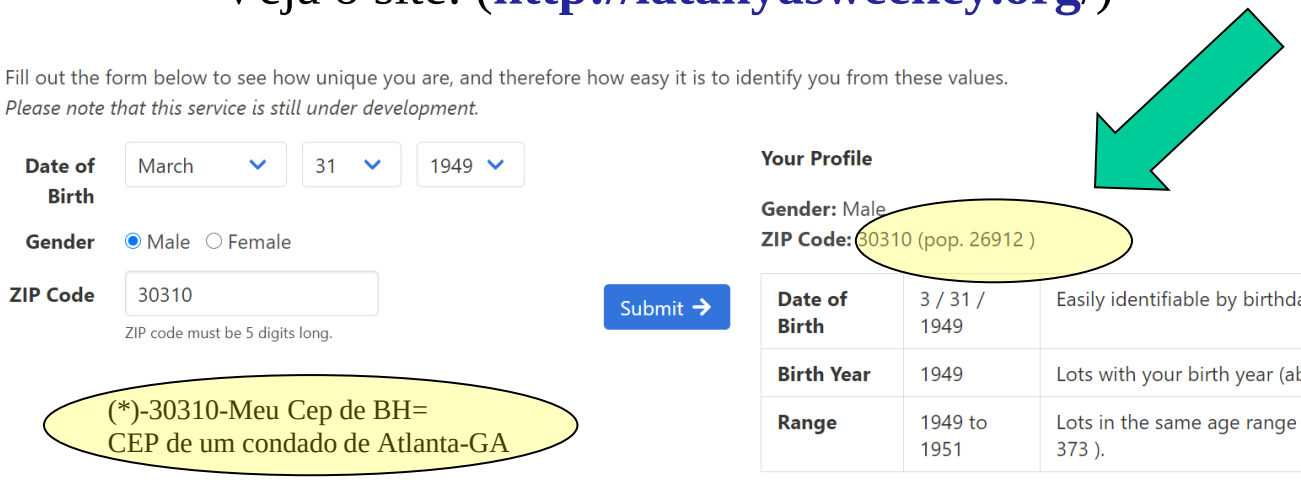
Fonte: Curso EAD-Ethics on Data Science-De-Identification has limited value-University of Michigan-H.V.Jagadish-2017

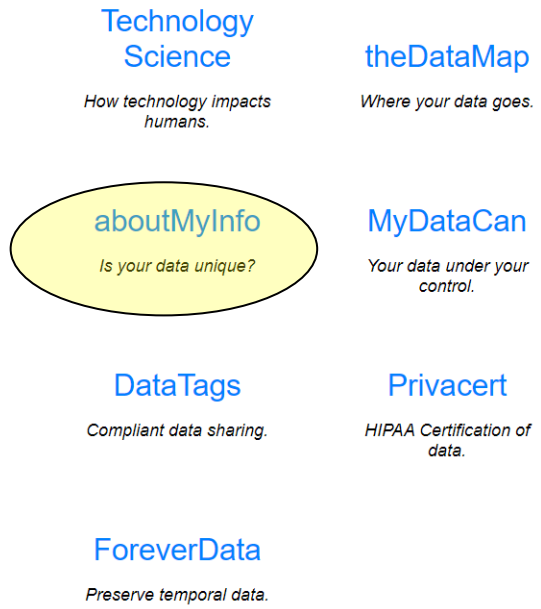
Lathania Sweeney

- Doutora (PHD) em Práticas de Governança e Tecnologia-Harvard
- Diretora do Lab. de Privacidade. Formada no MIT com extensão em Harvard
- Foi CTO do Federal Trade Comission(FTC)-'Procon' dos EUA
- Especialista em:
  - Algoritmos discriminatórios etc
- **thedatamap.org** - site que pesquisa e comprova o espalhamento dos dados pessoais, seu uso e vulnerabilidades
- **Vulnerabilidades da Anonimização(pseudonimização) dos dados e possibilidades de Re-identificação, em função de mapeamentos indiretos de fontes**

Exemplos de Re-ID por cruzamento de dados

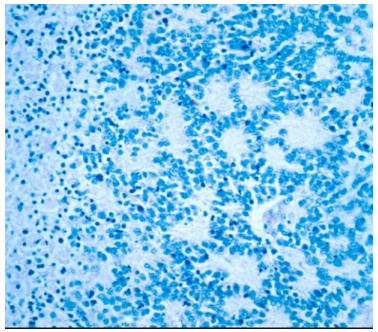
- 1997-Estado do Massachussets-dados de saúde publicados pelo Governo. Cientista de dados(Latania Sweeney), estudante do MIT-analisou os dados da população que estavam anonimizados, porém com ***CEP-Gênero-Data-Nascimento***.
  - Identificou 87,1%
  - Chegou no **Governador do estado**
  - Veja o site: (**http://latanyasweeney.org**/)





Exemplos de Re-ID por cruzamento de dados

Fonte: Our Bodies Our Data-Adam Tanner



1998-Identificadas 20 de 22 Crianças-dados pseudonimizados-Neuroblastoma

Personal Genome Project

Combinação de zipc-gênero-dat-nasc. 84% dos perfís

Est. Washington-Dados de Saúde Cep-gênero-idade(não data-nasc) Match de 43%, via palavra "hospitalized"

Boston- Hub Bicycle-somente 3 dígitos do Zipc e Ano-nascimento-Diversos matches

The New York Times

Reporters-identificaram uma mulher entre 657.000, via análise de search da AOL

IMDb

Concurso-Netflix-Dados pseudonimizados de aluguel de filme cruzados com com opiniões no IMDB

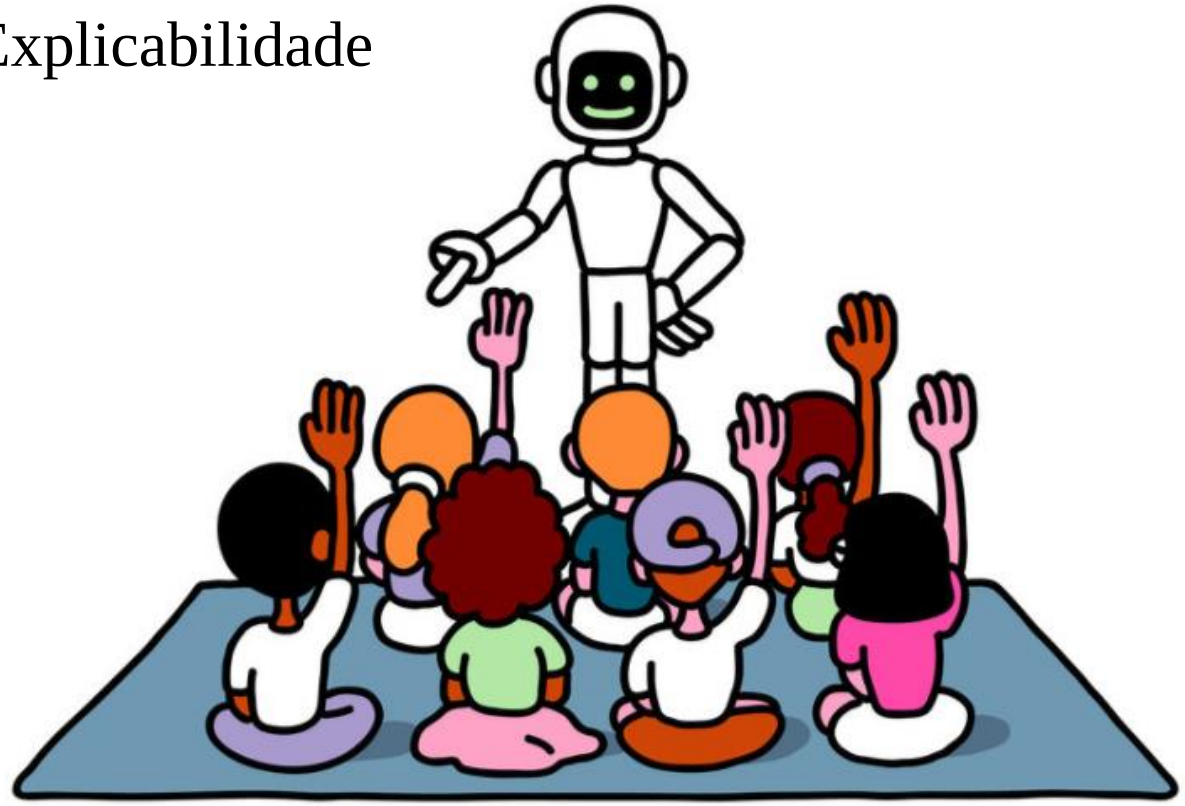
NYC Taxi & Limousine Commission

Dados sobre percursos de taxis
Cruzamento com artistas, revistas, rotas frequentes para sex-club etc.
Par de artistas famosos(BC e JÁ) detectados

ÉTICA
IA-Inteligência Artificial

Decisões automatizadas e Explicabilidade

2



Oscar Bolton Green

2023-**75%** das grandes empresas terão papel de "avaliadores de IA", visando reduzir os riscos das decisões automatizadas

Preocupações-Inteligência artificial **Princípios (FAT/ML*)**

- Princípios de Imparcialidade-Responsabilidade- Transparência-GDPR

- 1-***Responsabilidade***: claramente definido, com modos de remediação dos efeitos adversos, tanto no nível individual ou mais amplo (social)
- 2-***Explicabilidade***: Deverá ser possível explicar como as decisões foram feitas, sem uso de termos técnicos e com os dados que participaram daquela decisão
  - **Artigo 20-LGPD: Decisões automatizadas(revisão automatizada e humana)**
  - **Artigo 13 e 22-GDPR: Decisões automatizadas e revisão humana**
- 3-***Acurácia***: As fontes de erros ou de incertezas no algoritmo ou nos dados devem ser identificados, "logados-registrados" e articulados, a fim de prover entendimento dos riscos e das mitigações
  - **Aspectos de DNN-ataques adversariais**
- 4-***Auditabilidade***:Permitir a abertura do algoritmo para 3as partes, para auditoria de Código, documentação, API´s,etc
  - **Algoritmos mais leves, abertos e inteligíveis**
- ***5-Imparcialidade:*** Garantir que os resultados da decisão não são discriminatórios, desproporcionais ou injustos quando comparados no universo demográfico

(*)-Organização para Fairness, Accountability and Transparency, em Machine Learning-Baseados no GDPR

Governança de dados

Governança de Dados

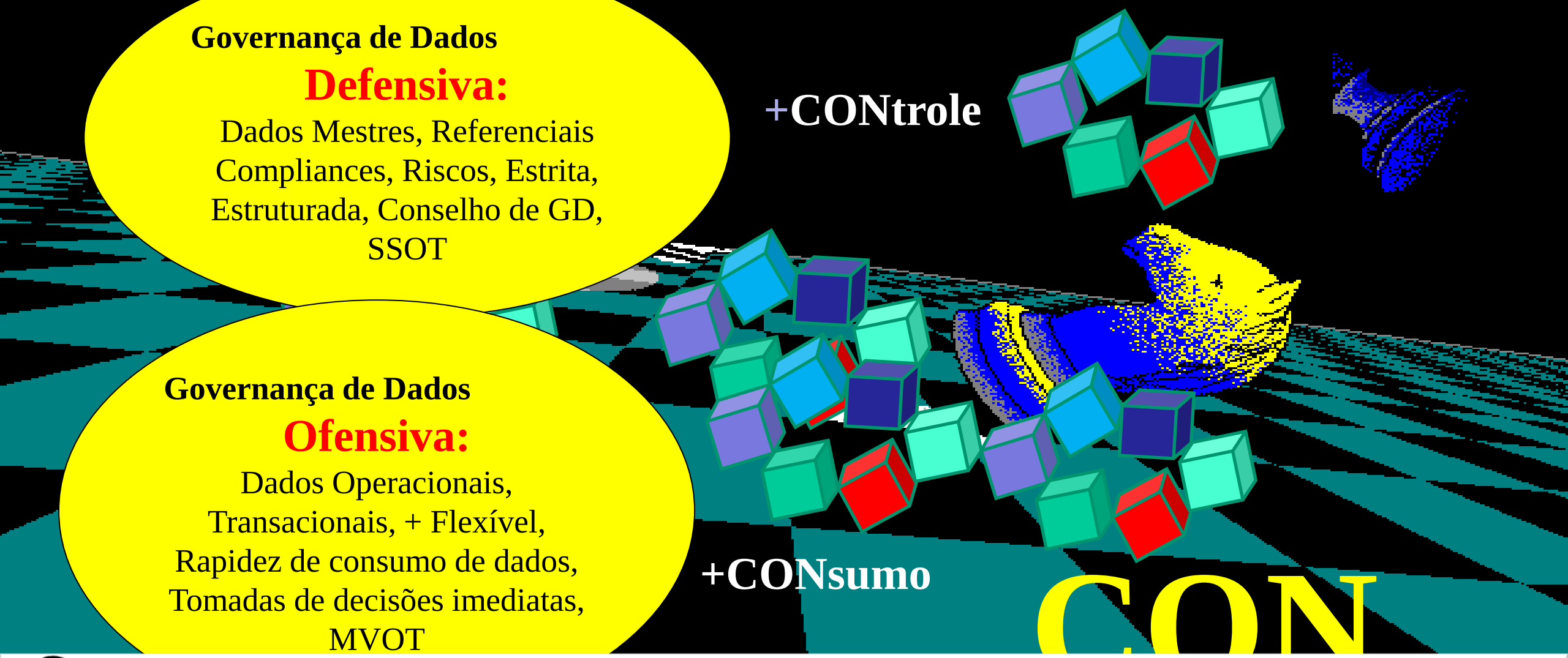
Defensiva:

Dados Mestres, Referenciais
Compliances, Riscos, Estrita,
Estruturada, Conselho de GD,
SSOT

Governança de Dados

Ofensiva:

Dados Operacionais,
Transacionais, + Flexível,
Rapidez de consumo de dados,
Tomadas de decisões imediatas,
MVOT



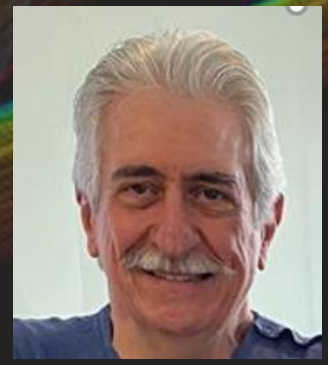
Whitepaper

Data Governance for GDPR Compliance: Principles, Processes and Practices

GD e LGPD compartilham intrinsecamente dos mesmos problemas e das mesmas soluções, com ligeiras variações nos domínios dos dados

LGPD = GD

Obrigado!



Carlos Barbieri

Carlos Barbieri Consultores Associados