ICP363
Introdução ao Aprendizado de Máquina

Aula 1 - Introdução

Prof.a. Carolina G. Marcelino

O que ´e Aprendizado de Máquina?

• **O que é aprendizado ?**

’Processo de aprender’

• **O que é aprender ?**

• ’Adquirir conhecimento mediante o estudo, a observação ou a experiência.’

• ’Reter na memória mediante o estudo, a observação ou a experiência.’

• ’Aprender é qualquer processo pelo qual um sistema melhora sua performance através da experiência.’

O que ´e Aprendizado de Máquina?

- Como ensinar a máquina? Como fazer a máquina aprender?
  - **Algoritmo:** dizer, passo a passo, o que deve ser feito.
    - Jogar xadrez
    - Reconhecer um objeto em uma foto
    - Andar em uma sala cheia de objetos
    - Conversar com uma pessoa
    - Dirigir um carro,...

O que ´e Aprendizado de Máquina?

- **Dificuldades**
  - Antecipar todas as possíveis situações que podem ocorrer
  - Antecipar todas as mudanças ao longo do tempo
  - Não ter ideia de como programar uma solução de um problema

Aprendizado de Máquina

- **Aprendizado como busca:**
  - Enumerar o espaço de conceitos
  - Eliminar aqueles que não estão de acordo com os dados
  - As descrições restantes contém o conceito que se quer aprender

Aprendizado de Máquina

- **Aprendizado indutivo:**
  - Extrair informações gerais a partir de um conjunto de casos particulares.
  - Projetar experimentos
  - Fazer observações
  - Coletar dados
  - Tentar extrair conhecimento encontrando modelos simples que explicam os dados observados

Aprendizado de Máquina

Exemplo: Utilizando as observações astronômicas feitas pelo astrônomo dinamarquês Tycho Brahe (1546-1601), permitiu que o astrônomo alemão Johannes Kepler (1571-1630) pudesse formular as três leis fundamentais da mecânica celeste, hoje denominadas Leis de Kepler.

Aprendizado de Máquina - Aplicações

- Classificar se um email é spam ou não
- Determinar o assunto de um dado documento
- Determinar se uma página web é ou não inapropriada
- Jogar (xadrez, gamão, etc)
- Reconhecimento de fala
- Identificação de face
- Sistemas de recomendação

Visão Geral

• Inteligência Artificial: construção de sistemas inteligentes que se comportam como humanos. Exemplos: robótica, processamento de linguagem natural, visão computacional.

• Aprendizado de Máquina (Machine Learning): subárea de inteligência artificial que desenvolve algoritmos capazes de aprender.

• Aprendizado Profundo (Deep Learning): subárea do aprendizado de máquina que desenvolve modelos computacionais compostos por múltiplas camadas de processamento. Tem como objetivo apredender representações de dados com múltiplos níveis de abstração.

Visão Geral

• Ciência de Dados (Data Science): área que estuda a extração generalizável de conhecimento a partir de um conjunto de dados. Utiliza técnicas de mineração de dados, aprendizado de máquina, estatística, pesquisa operacional,etc.

• Mineração de Dados (Data Mining): área que estuda a aplicação de algoritmos para extração de padrões a partir de um conjunto de dados.

Um pouco de História

• **Teorema de Bayes** - (1763 - Thomas Bayes , 1774 - Pierre-Simon Laplace): descreve a probabilidade de um evento **E** ocorrer, com base no conhecimento prévio das condições que podem estar relacionadas a **E**.

• **Cadeias de Markov** - (1913 - Andrey Markov): modelo estocástico que descreve uma sequência de eventos possíveis em que a probabilidade de cada evento depende apenas do estado alcançado no evento anterior.

• **Neurônio Artificial** - (1943 - Warren McCulloch e Walter Pitts): modelo matemático que imitava o funcionamento de um neurônio biológico.

• **Máquina de Aprendizagem** - (1950 - Turing): proposta de uma máquina capaz de aprender e se tornar inteligente.

Um pouco de História

- **Perceptron** - (1957 - Frank Rosenblatt): algoritmo de aprendizado supervisionado que determina se uma dada entrada pertence ou não a uma certa classe.

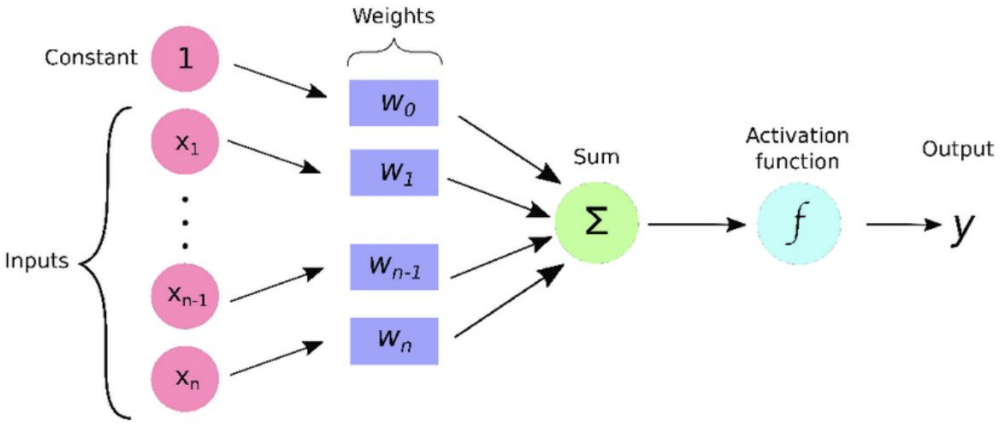
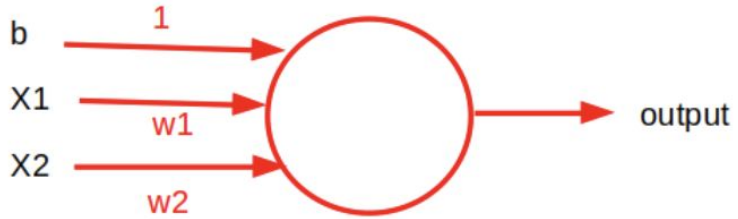


Figure: Lopez-Bernal et. al. (2021)

Perceptron

Exemplo OR

X1	X2	Output
1	1	1
1	0	1
0	1	1
0	0	0



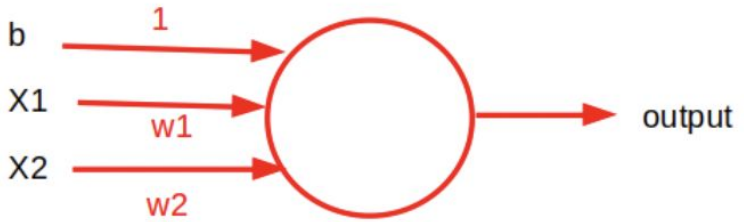
- Considere inicialmente $w_1 = w_2 = 1$ e $b = -1$.

$$\text{output} = \begin{cases} 0 & \text{if } w_1 x_1 + w_2 x_2 + b \leq 0 \\ 1 & \text{if } w_1 x_1 + w_2 x_2 + b > 0 \end{cases}$$

Perceptron

Exemplo OR

X1	X2	Output
1	1	1
1	0	1
0	1	1
0	0	0



- Considere inicialmente $w_1 = w_2 = 1$ e $b = -1$.

$$\text{output} = \begin{cases} 0 & \text{if } x_1 + x_2 - 1 \leq 0 \\ 1 & \text{if } x_1 + x_2 - 1 > 0 \end{cases}$$

Perceptron

Exemplo OR

X1	X2	Output
1	1	1
1	0	1
0	1	1
0	0	0

- Considere inicialmente $w_1 = w_2 = 1$ e $b = -1$.

$$\text{output} = \begin{cases} 0 & \text{if } x_1 + x_2 - 1 \leq 0 \\ 1 & \text{if } x_1 + x_2 - 1 > 0 \end{cases}$$

X1	X2	Output-Rede
1	1	1
1	0	0-erro
0	1	0-erro
0	0	0

Perceptron

Exemplo OR

X1	X2	Output
1	1	1
1	0	1
0	1	1
0	0	0

- Considere $w_1 = 2$, $w_2 = 1$ e $b = -1$.

$$\text{output} = \begin{cases} 0 & \text{if } 2x_1 + x_2 - 1 \leq 0 \\ 1 & \text{if } 2x_1 + x_2 - 1 > 0 \end{cases}$$

Perceptron

Exemplo OR

X1	X2	Output
1	1	1
1	0	1
0	1	1
0	0	0

- Considere $w_1 = 2$, $w_2 = 1$ e $b = -1$.

$$\text{output} = \begin{cases} 0 & \text{if } 2x_1 + x_2 - 1 \leq 0 \\ 1 & \text{if } 2x_1 + x_2 - 1 > 0 \end{cases}$$

X1	X2	Output-Rede
1	1	1
1	0	1
0	1	0-erro
0	0	0

Perceptron

Exemplo OR

X1	X2	Output
1	1	1
1	0	1
0	1	1
0	0	0

- Considere $w_1 = 2$, $w_2 = 2$ e $b = -1$.

$$\text{output} = \begin{cases} 0 & \text{if } 2x_1 + 2x_2 - 1 \leq 0 \\ 1 & \text{if } 2x_1 + 2x_2 - 1 > 0 \end{cases}$$

Perceptron

Exemplo OR

X1	X2	Output
1	1	1
1	0	1
0	1	1
0	0	0

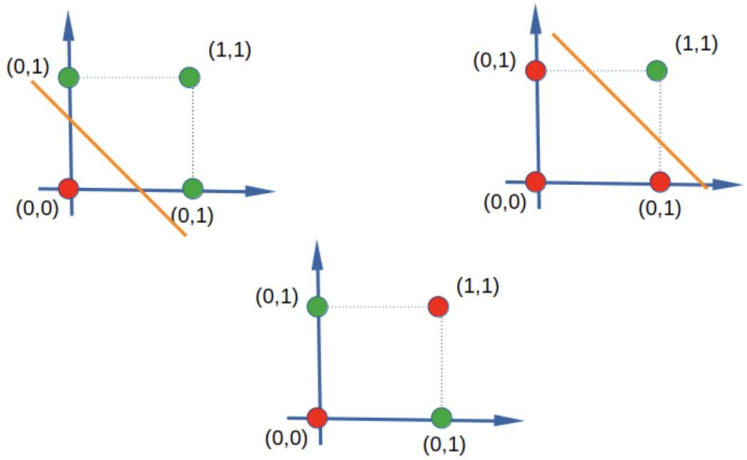
- Considere $w_1 = 2$, $w_2 = 2$ e $b = -1$.

$$\text{output} = \begin{cases} 0 & \text{if } 2x_1 + 2x_2 - 1 \leq 0 \\ 1 & \text{if } 2x_1 + 2x_2 - 1 > 0 \end{cases}$$

X1	X2	Output-Rede
1	1	1
1	0	1
0	1	1
0	0	0

Um pouco de História

• **Limitações das Redes Neurais** (1969 - Marvin Minsky e Seymour Papert): visto como um obstáculo para o desenvolvimento das redes neurais.



Um pouco de História

- **ELIZA** (1964-1967 - Joseph Weizenbaum) : foi o primeiro programa para processamento de linguagem natural da história

- **SHRDLU** (1968-1970 - Terry Winograd): é principalmente um analisador de linguagem que permite a interação do usuário usando termos em inglês . O usuário instrui SHRDLU a mover vários objetos no "mundo de blocos" contendo vários objetos básicos: blocos, cones, bolas, etc. O que tornou SHRDLU único foi a combinação de quatro ideias simples que se somaram para tornar a simulação de "entendimento" muito mais convincente.

Um pouco de História

- **Linguagem Prolog - 1972:** linguagem declarativa onde é feita uma descrição problema que se pretende computar

- **Backpropagation** (1986 - David Rumelhart, Geoff Hinton e Ronald J. Williams): algoritmo usado para o treinamento de redes neurais que utiliza a Regra da Cadeia (Leibniz - 1673). Também é conhecido como o modo reverso de diferenciação automática ou acumulação reversa, devido a Seppo Linnainmaa (1970).

Um pouco de História

• **Aprendizado por Reforço (1989 - Christopher Watkins:** algoritmo Q-learning.

• **TD-Gammon - (1992 - Gerald Tesauro):** programa para jogar gamão que utiliza rede neural.

• **IBM Deep Blue (1997):** programa que venceu o campeão mundial de xadrez Kasparov.

- **IBM's Watson (2011)**: sistema de computador capaz de responder perguntas feitas em linguagem natural, desenvolvido no projeto DeepQA da IBM.

Um pouco de História

• **Reconhecendo elementos em imagens (2012 - Andrew Ng e Jeff Dean):** reconhecimento de gatos em vídeos do Youtube.

• **Reconhecimento de Faces (2014):** o sistema DeepFace usa rede neural para identificar faces com 97% de acurácia.

- **AlphaGo** (2016): primeiro programa a vencer um campeão de Go. Seguido pelo AlphaZero (2017), capaz de jogar xadrez, shogi e go.
- **AlphaFold 1 (2018) e AlphaFold 2 (2021)**: previsão do formato 3D de proteína a partir de sua composição química.

Um pouco de História

• **Transformers (2017):** Uma arquitetura de aprendizagem profunda que utiliza um mecanismo paralelo de atenção. São uma arquitetura neural que transforma sequências de entrada em sequências de saída. Eles são uma importante tendência para a Inteligência Artificial (IA) do futuro.

Aplicações

- Processamento de linguagem natural (PLN)
- Reconhecimento de fala
- Tradução automática
- Análise de sequências de proteínas
- Análise de registros médicos
- Auxílio no diagnóstico
- Descoberta de novos medicamentos
- Geração de conteúdo educativo personalizado
- Análise de grandes volumes de dados financeiros
- Previsão de tendências de mercado

Um pouco de História

• **Transformers (2017):** Uma arquitetura de aprendizagem profunda que utiliza um mecanismo paralelo de atenção. São uma arquitetura neural que transforma sequências de entrada em sequências de saída. Eles são uma importante tendência para a Inteligência Artificial (IA) do futuro.

Funcionamento

- Os Transformers aprendem o contexto e rastreiam as relações entre os componentes da sequência
- Eles gerenciam com eficiência os dados sequenciais por meio de seu mecanismo exclusivo de autoatenção
- Eles superaram os RNNs tradicionais
- Eles têm a capacidade de lidar com sequências longas de forma mais eficiente

Um pouco de História

• **Transformers (2017):** Uma arquitetura de aprendizagem profunda que utiliza um mecanismo paralelo de atenção.

• **Família GPT (Generative Pre-trained Transformer)**

- **GPT-1 - 2018: BookCorpus -** conjunto de cerca de 7000 livros extraídos do site de e-books Smashwords
- **GPT-2 - 2019:** 8 milhões de textos web (Reddit)
- **GPT-3 - 2020:** textos da Common Crawl.
- **GPT-3.5 - 2022**
- **CharGPT - 2022**
- **GPT-4 - 2023**

Dados

• Os programas de aprendizado de máquina precisam ser treinados com dados.

• A proveniência destes dados é uma questão que tem se tornado cada vez mais importante.

• É preciso se tomar cuidado com relação a como os dados são coletados, usados e armazenados.

• Os dados devem ser coletados e usados de forma a respeitar a privacidade dos ”donos” destes dados.

Dados

• Os ”donos” dos dados deveriam ser capazes de ver quais informações são

coletadas, pedir que eventuais erros fossem consertados e até que os dados fossem completamente apagados.

• As empresas deveriam proteger tais informações, usá-las com responsabilidade e não compartilhá-las sem autorização.

Dados

Desenvolvendo sistemas de Aprendizado de Máquina

- Definição do problema
- Coleta dos dados
- Preparação dos Dados
- Treinamento do Modelo
- Avaliação do Modelo
- Entrega do Modelo

Dados

• **Definição do problema:** alguma tarefa que envolva processamento de Linguagem Natural

• **Coleta dos dados:** textos disponíveis na Wikipedia

• Em 01/12/2023 existiam 6.752.910 artigos na Wikipedia em inglês (≈ 10%) contendo mais de 4.3 bilhões de palavras (média de 658 palavras por artigo)

• Em português existiam 1.114.259 artigos (18a posição - (≈ 2.5%))

• Em termos de visualizações de páginas, o Brasil está em nono lugar com 2,6% do total global.

Dados

• **Definição do problema:** alguma tarefa que envolva processamento de Linguagem Natural

• **Coleta dos dados:** textos disponíveis na Wikipedia

• 15,4% preferem ler artigos em inglês (mais completos que os produzidos em português).

• Em Portugal, esse número sobe para 37,4%.

Dados

- **Coleta dos dados**: textos disponíveis na Wikipedia

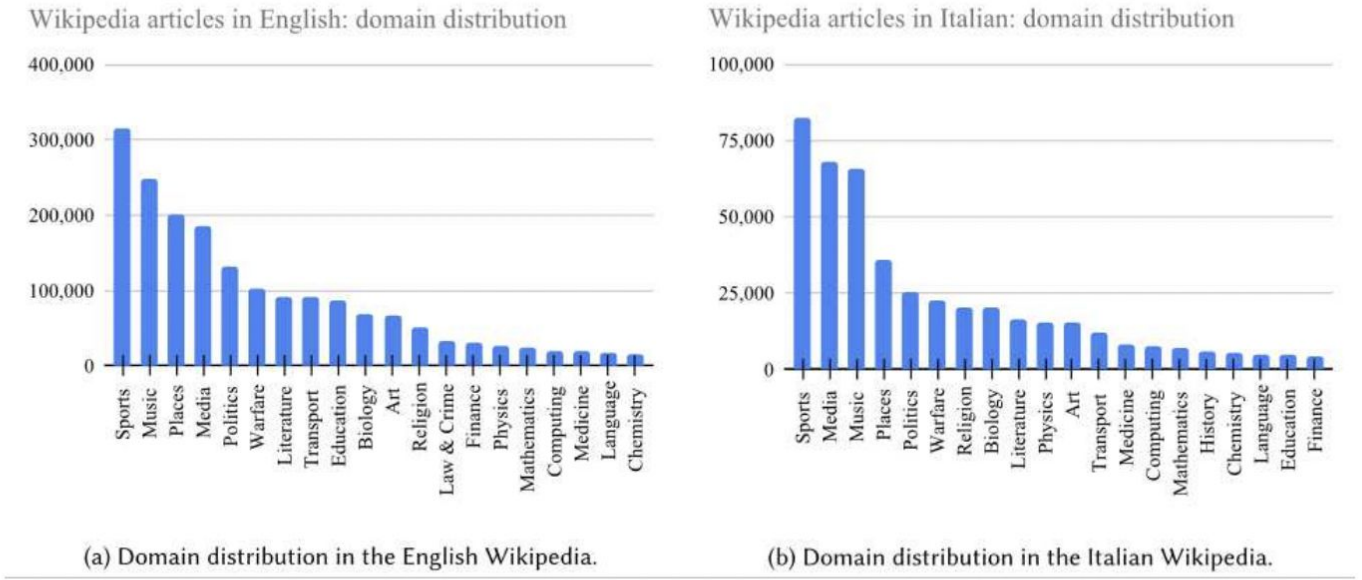


Figure: R. Navigli et al. - 2023

- Distribuição de Tópicos em Inglês e Italiano

Dados

- **Coleta dos dados:** textos disponíveis na Wikipedia
    - Distribuição de tópicos desbalanceada: Esporte, Música, Lugares, Mídia e Política
    - O desbalanceamento de domínios é um problema que aparece em outras aplicações
    - Balancear requer a classificação dos componentes do texto em classes bem definidas e identificáveis

Dados

• **Coleta dos dados:** textos disponíveis na Wikipedia

• excluir documentos que pertencem a um domínio/gênero super-representado pode levar ao descarte de informações de alta qualidade

• aumentar o número de documentos de uma classe sub-representada pode exigir esforços significativos.

Dados

- **Coleta dos dados:** textos disponíveis na Wikipedia

    - Diversidade: cultura, geografia, gênero, orientação sexual, grupo étnico, língua, entre outros

- **Outras fontes de dados**

    - Plataformas: Twitter, Facebook, Reddit, Blogs, etc
    - Questões
    - Quantidade vs. Diversidade
    - Acesso à Internet: jovens e países desenvolvidos

Dados

- **No Brasil**
  - Entre 2021 e 2022, alcançou 60 milhões de lares brasileiros (80% do total de domicílios)

Classe	Domicílios Conectados
A	100%
B	97%
C	87%
D e E	60%

Área	Domicílios Conectados
Urbana	82%
Rural	68%

Postagem na Internet (autoria própria -textos, imagens ou vídeos)
2021 - 31%
2022 - 43%

Table: Levantamento TIC Domicílios 2022

- Grande quantidade de postagens curtas e rápidas, feitas geralmente através de redes sociais e aplicativos de mensagens

Dados

- **Mais Questões**
  - Movimentos sociais produzem novas normas, linguagens e maneiras de se comunicar
  - Necessidade de identificar tais mudanças
  - Risco de descartar informação sem saber sua real relevância
  - Ponto de vista predominante é privilegiado
  - Necessidade de incluir ativamente comunidades sub-representadas na Internet

Dados

- **Mais Questões**
  - Considerar processos de decisão de forma a curar os dados usados na construção dos modelos
  - Necessidade de grandes investimentos na curadoria e documentação dos dados usados
  - Coletar uma quantidade de dados que possa ser curada e documentada

Lei Geral de Proteção de Dados Pessoais - LGPDP

A Lei no 13.709/2018 (LGPDP) é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7o e 16 do Marco Civil da Internet. Fundamentos da Proteção de Dados (Artigo 2º):

- o respeito à privacidade;
- a autodeterminação informativa;
- a liberdade de expressão, de informação, de comunicação e de opinião;
- a inviolabilidade da intimidade, da honra e da imagem;

Lei Geral de Proteção de Dados Pessoais - LGPDP

A Lei no 13.709/2018 (LGPDP) é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7o e 16 do Marco Civil da Internet. Fundamentos da Proteção de Dados (Artigo 2º):

• o desenvolvimento econômico e tecnológico e a inovação;

• a livre iniciativa, a livre concorrência e a defesa do consumidor; e

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

Lei Geral de Proteção de Dados Pessoais - LGPDP

A Lei não se aplica ao tratamento de dados pessoais: (Artigo 4º):

- realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
- realizado para fins exclusivamente:
  - jornalístico e artísticos;
  - acadêmicos (garantida, sempre que possível, a anonimização dos dados pessoais);
- segurança pública;
- defesa nacional;
- segurança do Estado;
- atividades de investigação e repressão de infrações penais; ou
- provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Lei Geral de Proteção de Dados Pessoais - LGPDP

Definições: (Artigo 5^{0}):

- **dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;
- **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;
- **dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Lei Geral de Protecão de Dados Pessoais - LGPDP

Definições: (Artigo $5^{\underline{0}}$):

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

Lei Geral de Proteção de Dados Pessoais - LGPDP

Direitos dos titulares de dados pessoais (Artigo $18^{\underline{0}}$):

- Confirmação da existência de tratamento.
- Acesso aos seus dados.
- Correção de dados incompletos, inexatos ou desatualizados.
- Anonimização, bloqueio ou eliminação de dados tratados em desconformidade com a LGPD.
- Portabilidade dos dados a outro fornecedor de serviço ou produto.
- Eliminação dos dados pessoais tratados com o consentimento do titular

Lei Geral de Proteção de Dados Pessoais - LGPDP

Direitos dos titulares de dados pessoais (Artigo $18^{\underline{0}}$):

- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
- Revogação do consentimento.
- Oposição ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na lei.
- Revisão de decisões automatizadas.

Lei Geral de Proteção de Dados Pessoais - LGPDP

A ANPD é o orgão da administração pública direta federal do Brasil que faz parte da Presidência da República e possui atribuições relacionadas a proteção de dados pessoais e da privacidade.

Realiza a fiscalização do cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD).

Atribuições

- elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade;
- fiscalizar e aplicar sanções;
- promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e as medidas de segurança; e
- promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transacional.

Fonte: Agência Câmara de Notícias

Lei Geral de Proteção de Dados Pessoais - LGPDP

Vinculado à ANPD e composto por 23 representantes titulares dos seguintes órgãos:

- seis representantes do Executivo federal;
- um representante indicado pelo Senado Federal;
- um representante indicado pela Câmara dos Deputados;
- um representante indicado pelo Conselho Nacional de Justiça;
- um representante indicado pelo Conselho Nacional do Ministério Público;
- um representante indicado pelo Comitê Gestor da Internet no Brasil;
- quatro representantes da sociedade civil com atuação comprovada em proteção de dados pessoais;
- quatro representantes de instituição científica, tecnológica e de inovação; e
- quatro representantes de entidade representativa do setor empresarial ligado à área de tratamento de dados pessoais.

A participação dos conselheiros, com mandato de dois anos, é não remunerada.

Fonte: Agência Câmara de Notícias