

Direitos Humanos, Tecnologias e Inteligência Artificial

Heloisa Helena de Almeida Portugal

Direitos Humanos, Tecnologias e Inteligência Artificial

Heloisa Helena de Almeida Portugal

Sobre o E-book

Este e-book faz parte dos Cursos de Graduação e Pós-graduação do **Programa UFMS Digital**, coordenado pela Agência de Educação Digital e a Distância da Universidade Federal de Mato Grosso do Sul.

Coordenação Geral

Daiani Damm Tonetto Riedner

Coordenação Pedagógica

Álvaro José dos Santos Gomes

Ana Carolina Pontes Costa

Analígia Miranda da Silva

Heloisa Helena de Almeida Portugal

Mauro dos Santos de Arruda

Equipe Multidisciplinar

Amanda de Mattos Pereira Mano

Analígia Miranda da Silva

Desenho Instrucional

Pedro Salina Rodovalho

Projeto Gráfico

Maira Sônia Camacho

Diagramação

Luísa de Almeida Souza Santos da Costa

Revisão de Língua Portuguesa

Aline Cristina Maziero

Sandro Fabian Francilio Dornelles

Thyago José da Cruz



Respeitadas as formas de citação formal de autores de acordo com as normas da ABNT NBR 10520 (2023), a não ser que esteja indicado de outra forma, todo material desta apresentação está licenciado sob uma [Licença Creative Commons - Atribuição 4.0 Internacional](https://creativecommons.org/licenses/by/4.0/).



AGEAD
Agência de Educação
Digital e a Distância



agead.ufms.br

Disciplina

Direitos Humanos, Tecnologias e Inteligência Artificial

Carga Horária

45 horas

Autoria

Heloisa Helena de Almeida Portugal - [Currículo Lattes](#)

Ementa

Relação entre direitos humanos e tecnologias digitais. Discussão sobre ética, transparência e regulação jurídica no uso de inteligência artificial. Segurança digital, privacidade e proteção de dados pessoais. Estratégias de prevenção e enfrentamento de desinformação, discurso de ódio e cyberbullying.

Conteúdo Programático

Módulo 1 – Direitos Humanos, tecnologias e direitos digitais

Unidade 1 – Fundamentos dos Direitos Humanos na era digital

Unidade 2 – Direitos Digitais: liberdade de expressão, acesso à informação e inclusão digital

Módulo 2 – Ética, Direitos Humanos e inteligência artificial

Unidade 1 – Princípios éticos aplicados à inteligência artificial

Unidade 2 – O uso da inteligência artificial na promoção e na proteção dos direitos humanos

Módulo 3 – Segurança digital, privacidade e proteção de dados

Unidade 1 – Privacidade como direito humano: educação e proteção de dados na era digital

Unidade 2 – Educação para a cibersegurança e o combate à desinformação e ao discurso de ódio

Objetivo Geral

■ Capacitar os participantes para analisar criticamente a relação entre direitos humanos, tecnologias digitais e inteligência artificial, promovendo a ética, a transparência, a inclusão e a segurança digital, com foco na proteção de dados e no combate à desinformação e ao discurso de ódio.

Objetivos Específicos

■ Explorar a relação entre direitos humanos e tecnologias digitais, promovendo o uso ético e seguro das ferramentas tecnológicas.

■ Analisar as implicações éticas do uso de inteligência artificial na proteção dos direitos humanos.

■ Desenvolver estratégias para segurança digital, proteção de dados e combate à desinformação.

Sumário

Módulo 1

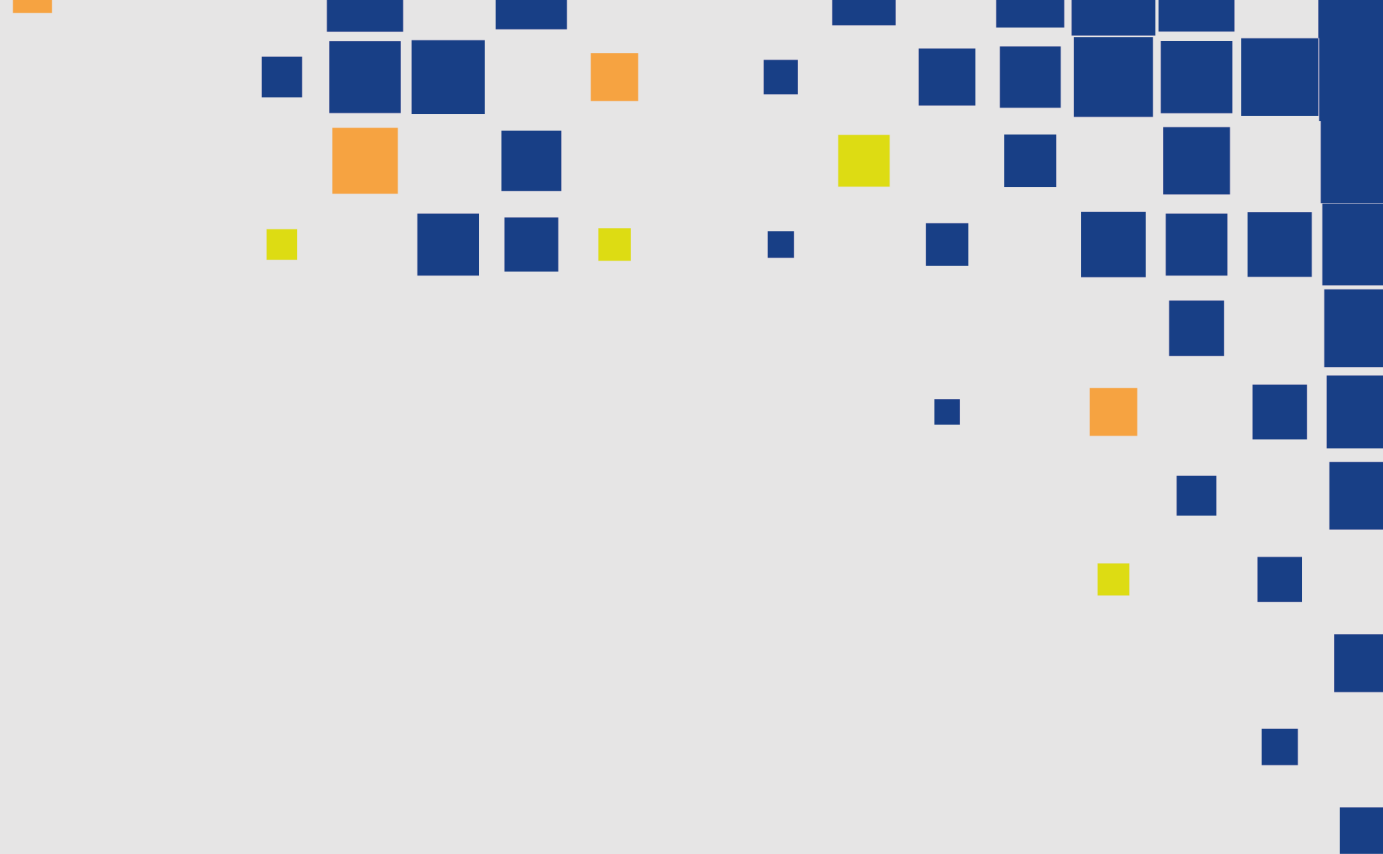
Direitos Humanos, Tecnologias e Direitos Digitais	06
Fundamentos dos direitos humanos na era digital	09
Direitos digitais fundamentais: liberdade, acesso e inclusão	19

Módulo 2

Ética, Direitos Humanos e Inteligência Artificial	32
Princípios éticos e desafios da IA para os direitos humanos	35
O Uso da Inteligência Artificial na Promoção e Proteção dos Direitos Humanos	46

Módulo 3

Segurança Digital, Privacidade e Proteção de Dados	62
Privacidade como Direito Humano: Educação e Proteção de Dados na Era Digital	65
Educação para a Cibersegurança e o Combate à Desinformação e ao Discurso de Ódio	76



Módulo 1

Direitos Humanos, Tecnologias e Direitos Digitais



Apresentação

Olá! Seja bem-vinda(o) ao primeiro módulo da disciplina **Direitos Humanos, Tecnologias e Inteligência Artificial**.

Vivemos em uma sociedade profundamente atravessada pelas tecnologias digitais. Ao longo do dia, usamos celulares, aplicativos, plataformas, redes sociais, ambientes virtuais de aprendizagem e diferentes sistemas digitais para estudar, trabalhar, nos informar, se comunicar e participar da vida social. As tecnologias, portanto, não são apenas ferramentas: elas passaram a compor o modo como vivemos, nos relacionamos e exercemos a cidadania.

Diante desse cenário, surge uma questão central: **de que maneira as tecnologias digitais impactam os direitos humanos?** Em alguns contextos, elas ampliam o acesso à informação, favorecem a circulação de conhecimento, fortalecem mobilizações sociais e criam novas possibilidades de participação. Em outros, porém, também podem aprofundar desigualdades, ampliar mecanismos de vigilância, expor dados pessoais, disseminar desinformação e intensificar violências contra grupos historicamente vulnerabilizados.

Basta pensar em situações já bastante conhecidas em nosso cotidiano: estudantes que não conseguem acompanhar atividades escolares por falta de acesso adequado à internet; discursos de ódio impulsionados por algoritmos em plataformas digitais; vazamentos de dados pessoais; barreiras de acessibilidade em ambientes virtuais; e desigualdades de acesso e uso das tecnologias em diferentes regiões e classes sociais. Essas situações mostram que os direitos humanos continuam plenamente atuais no ambiente digital, mas exigem novas formas de compreensão, proteção e promoção.

Neste módulo, você será convidada(o) a refletir criticamente sobre a relação entre direitos humanos e tecnologias digitais. Ao longo das unidades, discutiremos fundamentos históricos e jurídicos, marcos regulatórios, direitos digitais, liberdade de expressão, acesso à informação, inclusão digital e acessibilidade. Também analisaremos como as desigualdades estruturais atravessam a experiência digital e por que a educação em direitos humanos precisa incorporar esse debate de forma crítica e comprometida com a justiça social. Para

Ao final deste módulo, espera-se que você seja capaz de:

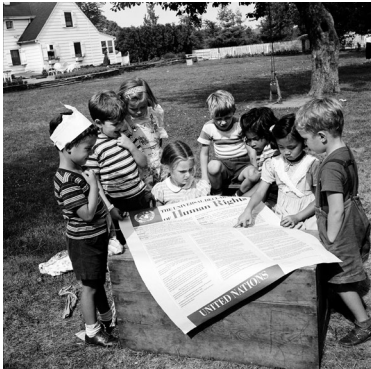
- compreender as transformações dos direitos humanos na era digital e identificar os principais marcos regulatórios nacionais e internacionais;
- analisar criticamente os impactos das tecnologias digitais sobre diferentes grupos sociais, considerando desigualdades e interseccionalidades;
- reconhecer direitos digitais fundamentais, como liberdade de expressão, acesso à informação, inclusão e acessibilidade digital;
- aplicar estratégias pedagógicas para a educação em direitos digitais em diferentes contextos formativos;
- desenvolver uma postura ética, crítica e comprometida com a proteção dos direitos humanos no ambiente digital.

orientar sua trajetória de aprendizagem, o módulo foi organizado em duas unidades complementares. Na Unidade 1, discutiremos os fundamentos dos direitos humanos na era digital, seus marcos regulatórios e as tensões entre tecnologia, dignidade e cidadania. Na Unidade 2, aprofundaremos o debate sobre direitos digitais fundamentais, com destaque para liberdade de expressão, acesso à informação, inclusão e acessibilidade.

Vamos começar?

Unidade 1

Fundamentos dos direitos humanos na era digital



Descrição: Crianças lendo a Declaração Universal dos Direitos Humanos (DUDH), pouco após sua adoção. **Fonte:** Wikimedia

Os direitos humanos não surgiram de forma pronta e acabada. Eles são resultado de processos históricos de luta por dignidade, liberdade, igualdade e justiça. Ao longo do tempo, foram sendo formulados, ampliados e reinterpretados em resposta a diferentes contextos sociais, políticos e culturais.

A [Declaração Universal dos Direitos Humanos](#), proclamada pela Organização das Nações Unidas em 1948, representa um marco nesse processo ao afirmar que todos os seres humanos nascem livres e iguais em dignidade e em direitos.

Embora tenha sido formulada em um contexto anterior à internet, aos computadores pessoais e às redes sociais, seus princípios permanecem atuais e continuam fundamentais para pensar os desafios do presente.

A Resolução A/HRC/RES/20/8 da ONU, de 2012, reafirma essa compreensão ao reconhecer que os mesmos direitos assegurados às pessoas offline também devem ser protegidos online. Isso reforça a ideia de que o ambiente digital não constitui um espaço separado da vida social, mas uma extensão dela, atravessada por disputas, desigualdades, oportunidades e conflitos.

Nesse contexto, a proteção dos direitos humanos passa a demandar também uma articulação entre os planos nacional e internacional. Como destaca Piovesan (2021), os direitos humanos devem ser compreendidos de forma dialógica, especialmente diante de violações que, no ambiente digital, frequentemente ultrapassam fronteiras geográficas e desafiam sistemas jurídicos tradicionais.



Conceito-chave: direitos digitais

Direitos digitais correspondem à aplicação e à concretização dos direitos humanos no ambiente digital. Não se trata de uma categoria completamente nova de direitos, mas da necessidade de garantir, no espaço online, direitos já reconhecidos em outros contextos.



Entre esses direitos, destacam-se:



Elaboração do Plano Orçamentário



Liberdade de Expressão no Ambiente Digital



Acesso à Internet e à Informação



Inclusão e Acessibilidade Digital



**Proteção Contra Discriminação,
Vigilância Abusiva e Violências Digitais.**

Assim, falar em direitos digitais é reconhecer que a transformação tecnológica exige atualização das formas de proteção da dignidade humana.

Saiba Mais!

Ouçá um podcast sobre o desafio das tecnologias de inteligência artificial na Educação.

Acesse aqui!

Direitos humanos e tecnologias digitais: entre potencialidades e tensões

As tecnologias digitais ampliaram significativamente as possibilidades de comunicação, produção de conhecimento, mobilização social e acesso a serviços. Bibliotecas digitais, cursos online, plataformas públicas de informação e redes de ativismo são exemplos de como o ambiente digital pode fortalecer direitos e ampliar oportunidades.

Entre suas potencialidades, podemos destacar:

- democratização do acesso ao conhecimento;
- ampliação da circulação de informações;
- fortalecimento de movimentos sociais e mobilizações coletivas;
- ampliação do acesso a serviços públicos, de saúde e de educação;
- fortalecimento de práticas de transparência e controle social.

No entanto, essas mesmas tecnologias também produzem novas formas de vulnerabilidade. O ambiente digital pode intensificar desigualdades já existentes, favorecer práticas de monitoramento e vigilância, ampliar a circulação de desinformação e expor grupos vulnerabilizados a diferentes formas de violência.

Entre os principais riscos e desafios, estão:

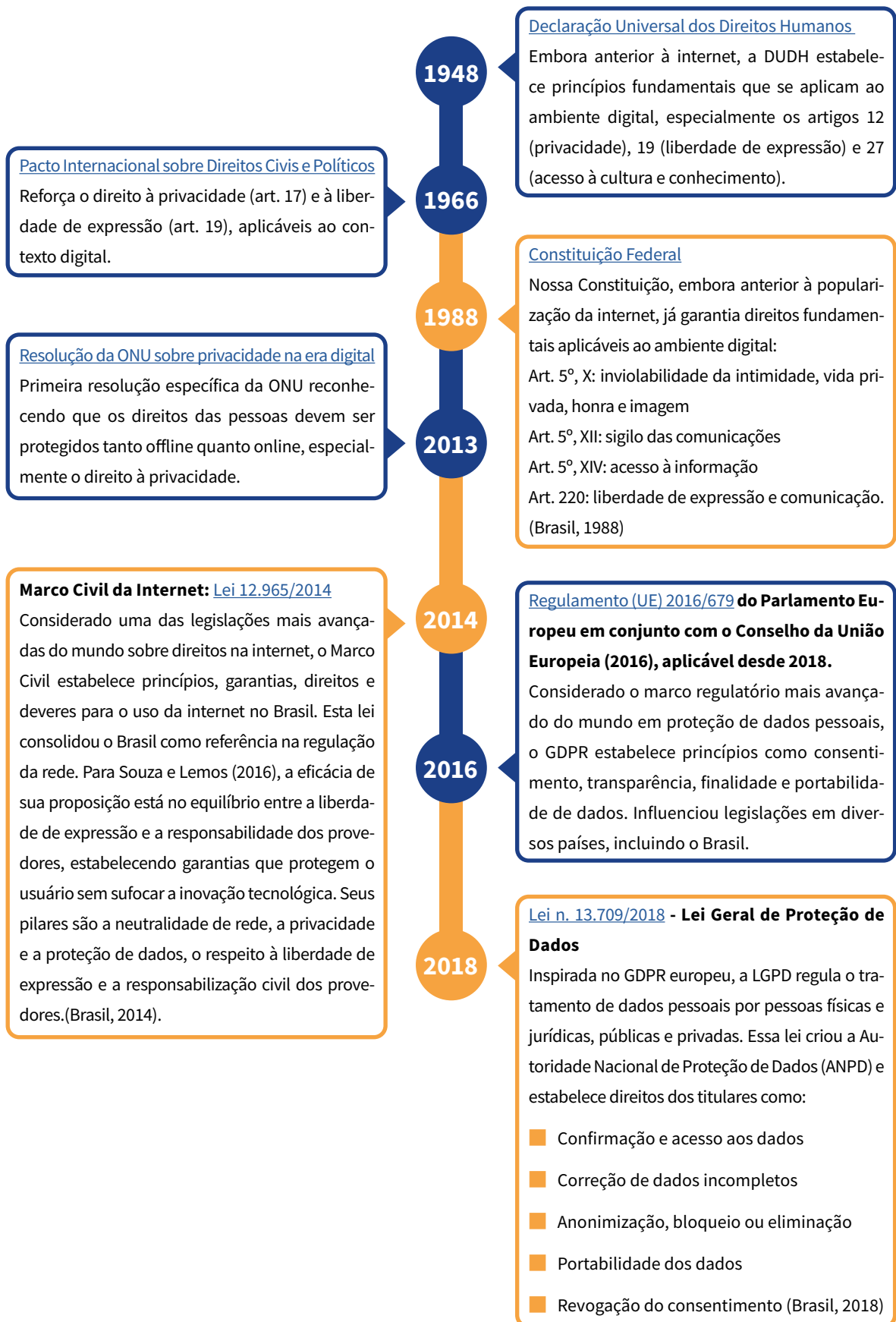
- exclusão digital;
- vigilância em massa;
- coleta abusiva de dados pessoais;
- discriminação algorítmica;
- disseminação de desinformação;
- cyberbullying, assédio e discurso de ódio.

Por isso, não basta considerar a tecnologia como instrumento neutro. As tecnologias são produzidas e utilizadas em contextos sociais marcados por relações de poder, interesses econômicos, desigualdades estruturais e disputas políticas. Seu impacto depende, em grande medida, de como são projetadas, reguladas, acessadas e apropriadas socialmente.

Marcos regulatórios: construindo uma arquitetura de direitos

A proteção dos direitos humanos na era digital depende da existência de marcos normativos capazes de orientar o uso das tecnologias e estabelecer garantias para os indivíduos e para a coletividade. No âmbito internacional, diversos instrumentos internacionais ajudam a fundamentar a proteção de direitos no ambiente digital, enquanto em âmbito nacional, o Brasil, nos últimos anos tem desenvolvido um arcabouço jurídico importante para a proteção de direitos na era digital, conforme veremos a seguir.

CONTEXTO INTERNACIONAL X CONTEXTO BRASILEIRO





Descrição: Close de um olho com reflexos de telas digitais, destacando a relação entre visão, tecnologia e informação. **Fonte:** Magnific.

É importante destacar, que no ambiente digital, as tecnologias emergentes, como a inteligência artificial (IA), os sistemas de vigilância em massa e a coleta de dados em plataformas digitais, oferecem uma nova dinâmica ao direito à privacidade.

Zuboff (2021) aponta que estamos vivendo um cenário em que as tecnologias que deveriam ampliar o acesso à informação e à liberdade também estão sujeitas a abusos no uso de dados pessoais. Uma vez que Plataformas digitais, como redes sociais, aplicativos de compras e bancos de dados online, coletam volumes massivos de informações pessoais, muitas vezes sem o consentimento explícito dos usuários, o que gera um conflito direto com o direito à privacidade.



Descrição: Pessoa de moletom com capuz diante de vários monitores. Ao fundo, um grande olho com elementos gráficos digitais sugere vigilância, cibersegurança e monitoramento de dados. **Fonte:** Maginific

Em 2018, com a implementação da Lei Geral de Proteção de Dados (LGPD), a Constituição brasileira foi complementada com regulamentações mais específicas que visam a reforçar a proteção da privacidade no ambiente digital. A LGPD garante aos cidadãos o direito de controle sobre seus dados pessoais, ao prever que eles autorizem ou revoguem o uso de suas informações pessoais e que saibam como esses dados são utilizados.

Porém, como afirmam Salgado e Campos (2023), o direito à privacidade na era digital enfrenta desafios que as legislações tradicionais não estavam preparadas para abordar. A falta de transparência, o uso indevido de dados por empresas de tecnologia e a falta de regulamentação eficaz, em muitos casos, podem levar à violação de direitos fundamentais sem a punição adequada.

Na era digital, a privacidade não é apenas uma questão de proteger a intimidade da pessoa contra invasões físicas, mas também de garantir a proteção dos dados pessoais de cada indivíduo.

A informação sobre preferências, comportamentos e histórico digital se torna um bem valioso e as tecnologias de vigilância e monitoramento podem criar um ambiente onde as pessoas não têm controle sobre seus dados. Zuboff (2021) destaca que as tecnologias de monitoramento digital podem levar à violação de direitos fundamentais como a liberdade de expressão e o direito à privacidade, criando um ciclo vicioso de vigilância e segregação.

A transição para uma “**sociedade da vigilância**” traz desafios inéditos para a dignidade humana. Segundo Rodotà (2008), a privacidade hoje não é apenas o direito de ser deixado em paz, mas um instrumento de liberdade e um pressuposto para o exercício da cidadania, pois evita que o indivíduo se torne transparente diante do poder de grandes corporações e do Estado.

É vital que a educação digital não se limite apenas ao domínio técnico das ferramentas, mas ajude os alunos a entenderem os riscos e as implicações de um mundo interconectado. A educação em direitos humanos, como Salgado e Campos (2023) sugerem, deve ser parte de um movimento mais amplo que inclua a alfabetização digital, a fim de que todos se tornem agentes ativos na defesa de seus direitos no universo digital.

A cidadania digital não é uma opção, é uma necessidade urgente.



Para refletir!

Como educadora(or) em direitos humanos, você conhece os direitos digitais garantidos pela legislação brasileira? Como pode incorporar esse conhecimento em suas práticas pedagógicas?

O direito à privacidade, como defendido pela Constituição Federal e complementado por legislações como a LGPD, precisa ser reinterpretado à luz da era digital. Em um mundo onde dados pessoais se tornaram um recurso comercial valioso, as tecnologias digitais atuam como agentes duplos:

- Garantem liberdade ao fornecer informações e facilitam a comunicação global;
- Ameaçam a privacidade, transformando dados pessoais em um bem de mercado.

Salgado e Campos (2023) sugerem que o ensino sobre privacidade digital deve ser uma prioridade das políticas educacionais, para proteger as gerações futuras de abusos tecnológicos.

O uso indiscriminado de tecnologias de monitoramento e algoritmos discriminatórios pode criar uma sociedade de vigilância, na qual a privacidade deixa de ser um direito fundamental, e torna-se uma mercadoria para empresas de tecnologia.

Nesse cenário, o direito à privacidade exige uma proteção mais robusta, que contemple os novos desafios trazidos pela era digital, como a segregação digital, a discriminação algorítmica e os abusos de dados pessoais.

Direitos humanos e tecnologias digitais: convergências e tensões

As tecnologias digitais criam um cenário paradoxal: ao mesmo tempo que ampliam possibilidades de exercício de direitos, também criam novos riscos e vulnerabilidades.

POTENCIALIDADES

Democratização do conhecimento: acesso a bibliotecas digitais, cursos online, informações científicas

Amplificação de vozes: movimentos sociais podem mobilizar milhões através das redes

Transparência governamental: dados abertos e prestação de contas online

Acesso a serviços: saúde, educação e serviços públicos digitais

RISCOS E DESAFIOS

Exclusão digital: milhões sem acesso à internet de qualidade

Vigilância em massa: monitoramento de comunicações e comportamentos

Discriminação algorítmica: sistemas que reproduzem preconceitos

Desinformação: fake news e manipulação da opinião pública

Violência digital: cyberbullying, discurso de ódio, assédio online



Descrição: Mulher em frente a telas toca um cadeado digital luminoso, representando segurança da informação, privacidade e proteção de dados.

Fonte: Magnific.



Para refletir!

Interseccionalidade digital: quem são os mais vulneráveis?

O conceito de interseccionalidade, desenvolvido pela jurista Kimberlé Crenshaw, (2002), propõe que as opressões não atuam isoladamente – raça, gênero, classe, território e outras categorias se entrelaçam, criando experiências únicas de discriminação.

Descrição : Fotografia de Kimberlé Crenshaw, mulher negra sorrindo de perfil, com dreadlocks castanhos e loiros presos no topo. Usa colar de corrente prateada e blusa preta. **Foto:** Mohamed Badarne, CC-BY-SA-4.0



No ambiente digital, essa interseccionalidade se manifesta de que forma?

Mulheres negras, por exemplo, sofrem violências digitais específicas que combinam racismo e machismo. Segundo a SaferNet Brasil, em dados de 2022 publicados no relatório de 2023 (SaferNet Brasil, 2023), mulheres negras recebem 3 vezes mais mensagens de ódio nas redes sociais do que mulheres brancas.

Ainda segundo dados do mesmo relatório pessoas LGBTQIA+ enfrentam exposição não consentida (outing), discurso de ódio e violências específicas nas plataformas digitais; populações rurais e periféricas têm acesso limitado à internet de qualidade, enfrentando exclusão digital que se soma a outras exclusões históricas; pessoas com deficiência encontram barreiras de acessibilidade em sites, aplicativos e plataformas que não foram desenvolvidos considerando suas necessidades e pessoas idosas frequentemente são excluídas por falta de letramento digital e ficam à margem de serviços cada vez mais digitalizados.

Além de todos esses grupos, também é preciso considerar que crianças e adolescentes são especialmente vulneráveis a violências digitais, à exploração e ao uso indevido de seus dados pessoais.



Dados para reflexão:

Segundo a pesquisa [TIC Domicílios 2022](#) do CETIC.br:

- Apenas 84% dos domicílios brasileiros têm acesso à internet
- Nas classes D/E, apenas 69% têm acesso
- Na área rural, 71% têm acesso (contra 90% na área urbana)
- 58% acessam a internet exclusivamente pelo celular

Esses dados revelam que a exclusão digital no Brasil tem **cor, classe social e território**.

Caso prático: educação remota e desigualdades digitais na pandemia.

Durante a pandemia de COVID-19, escolas de todo o Brasil migraram para o ensino remoto de emergência. Essa experiência evidenciou brutalmente as desigualdades digitais do país.

Vamos pensar em uma situação hipotética: Maria, 14 anos, estudante de escola pública em comunidade periférica de uma grande cidade, não tinha computador nem internet em casa. Sua família compartilhava um único celular pré-pago. Enquanto isso, João, da mesma idade, mas de escola particular, tinha computador próprio, internet de alta velocidade e apoio familiar para estudar em casa.

A partir da situação descrita, que envolve realidades muito diferentes de dois estudantes brasileiros, reflita:

- Quais direitos humanos foram violados no caso de Maria?
- Como a exclusão digital se relaciona com outras formas de exclusão social?
- Que responsabilidades têm o Estado, as escolas e a sociedade para garantir o direito à educação na era digital?
- Como educadores em direitos humanos podem atuar para reduzir essas desigualdades?



Para se questionar

O acesso à internet deveria ser reconhecido como direito humano fundamental? Por quê?

Neste contexto, o convite que fica é para olharmos para o nosso papel na educação em direitos humanos na era digital. Como educadoras e educadores em direitos humanos, ao abordar este tema temos responsabilidades específicas de:

- Compreender profundamente como tecnologias impactam direitos fundamentais;
- Desenvolver letramento digital crítico em nós mesmos e em nossos estudantes;
- Promover inclusão digital como estratégia de justiça social
- Educar para o uso ético e responsável das tecnologias;
- Denunciar e combater violações de direitos no ambiente digital;
- Empoderar grupos vulneráveis para que possam exercer plenamente seus direitos digitais;

A educação em direitos humanos na era digital não pode se limitar a ensinar sobre leis e declarações – precisa formar cidadãos e cidadãs críticos, éticos e engajados na construção de um ambiente digital mais justo, inclusivo e democrático.

Unidade 2

Direitos digitais fundamentais: liberdade, acesso e inclusão



Descrição: Mão segurando celular que exibe ícones flutuantes de redes sociais e mídia sobrepostos por feixes de luz rosa. Fundo desfocado e iluminado.

Fonte: Magnific.

Liberdade de expressão no ambiente digital

A liberdade de expressão é um dos pilares da democracia. No ambiente digital, ela ganha novas dimensões e complexidades. A internet transformou radicalmente como nos expressamos, compartilhamos ideias e participamos do debate público.

Plataformas digitais democratizaram a comunicação, permitindo que qualquer pessoa com acesso à internet possa, potencialmente, alcançar uma audiência global.

Esta democratização trouxe benefícios extraordinários para a liberdade de expressão. Vozes que antes eram marginalizadas e silenciadas pelos meios de comunicação tradicionais encontraram nas plataformas digitais canais para se expressar. Movimentos sociais, ativistas de direitos humanos e cidadãos comuns podem, utilizando as redes sociais, documentar injustiças, organizar protestos e mobilizar apoio de formas que seriam impensáveis antes.

Contudo, o exercício da liberdade de expressão online também enfrenta desafios únicos. A moderação de conteúdo por plataformas privadas levanta questões sobre censura e controle editorial. Algoritmos que determinam quais conteúdos são promovidos ou suprimidos podem influenciar significativamente o debate público. A proliferação de desinformação e de discurso de ódio online cria tensões entre a proteção da liberdade de expressão e a necessidade de proteger outros direitos fundamentais.

Potencialidades da liberdade de expressão online

A internet democratizou a produção e circulação de informações. Qualquer pessoa com acesso à rede pode:

- Criar e compartilhar conteúdo
- Expressar opiniões e ideias
- Mobilizar-se politicamente
- Denunciar injustiças
- Participar de debates públicos

Exemplo: As Jornadas de Junho de 2013 foram amplamente organizadas por meio das redes sociais, demonstrando o poder mobilizador da internet.



Limites da liberdade de expressão

A liberdade de expressão não é absoluta. Seu limite é a violação de direitos fundamentais.



Discurso de ódio

Manifestações que incitam violência, discriminação ou preconceito contra grupos vulneráveis (por raça, gênero, orientação sexual, religião, etc.)



Fake news com potencial lesivo

Desinformação deliberada que pode causar danos à saúde pública, à democracia ou aos direitos individuais.



Violação de privacidade

Exposição não consentida de dados pessoais, imagens íntimas, etc.



Calúnia, difamação e injúria

Ataques à honra e à reputação de pessoas.

Moderação de conteúdo: entre censura e proteção

Um dos grandes dilemas contemporâneos é: **quem deve decidir o que pode ou não ser publicado na internet?**

As plataformas digitais enfrentam o desafio de moderar bilhões de posts, comentários e vídeos diariamente. Esta moderação envolve decisões sobre o que constitui conteúdo aceitável, com vistas a equilibrar a liberdade de expressão com a proteção contra danos. Os critérios utilizados nessas decisões podem variar significativamente entre plataformas e culturas.



Descrição: Ilustração surrealista de garoto olhando o celular, cercado por mãos fantasmagóricas, cadeados, um grande olho vigilante e telas sobre privacidade.

Fonte: Magnific.

A moderação automatizada, baseada em algoritmos de inteligência artificial, é relevante devido ao volume de conteúdo, mas apresenta limitações significativas. Algoritmos podem não compreender contexto, ironia, sarcasmo ou nuances culturais, o que pode resultar em decisões de moderação inadequadas. A moderação humana, embora mais precisa, é limitada e pode expor moderadores a conteúdo traumático.

As plataformas digitais (Facebook, X/Twitter, Instagram, YouTube, etc.) têm seus próprios **“termos de uso”** e **políticas de moderação de conteúdo**.

No entanto, essa moderação faz surgir outros questionamentos, como por exemplo:



Atenção!

- Empresas privadas devem ter poder de censurar conteúdos?
- Como garantir transparência e accountability nessas decisões?
- Como evitar que a moderação seja usada para silenciar vozes dissidentes?
- Como equilibrar liberdade de expressão e proteção contra discursos nocivos?

O Marco Civil da Internet estabelece que provedores de aplicações só podem ser responsabilizados por conteúdos de terceiros após ordem judicial específica (exceto em casos de imagens de nudez ou atos sexuais sem consentimento).

Discurso de ódio online: um desafio urgente

O discurso de ódio online tem crescido de forma alarmante. Segundo relatório da [SaferNet Brasil](#), em 2022 foram registradas mais de 50 mil denúncias de crimes contra direitos humanos na internet. Observe o infográfico abaixo com os principais crimes e suas características.





ESTRATÉGIA PEDAGÓGICA!

Como trabalhar a liberdade de expressão e seus limites com estudantes?

Atividade sugerida: apresente casos reais (anonimizados) de postagens em redes sociais e peça que analisem:

- Trata-se de exercício legítimo de liberdade de expressão ou discurso de ódio?
- Quais direitos estão em tensão?
- Como deveria ser a resposta adequada (educativa, judicial, moderação da plataforma)?

Direito ao acesso à informação

O acesso à informação é fundamental para o exercício da cidadania. Na era digital, esse direito ganha novas configurações. A internet criou o maior repositório de informações da história humana, tornando acessível conhecimento que antes estava restrito a bibliotecas especializadas ou arquivos governamentais.

O acesso à informação digital também enfrenta obstáculos significativos. A “divisão digital” - a lacuna entre aqueles que têm acesso efetivo às tecnologias digitais e aqueles que não têm - cria novas formas de desigualdade informacional. Fatores como infraestrutura inadequada, custos elevados de conectividade, falta de habilidades digitais e barreiras linguísticas podem limitar o acesso à informação.

Transparência e dados abertos

A Lei de Acesso à Informação ([LAI – Lei 12.527/2011](#)) garante o direito de qualquer cidadão solicitar informações públicas aos órgãos governamentais. Muitos desses dados estão disponíveis em portais de transparência e dados abertos.

- Dados abertos governamentais permitem:
- Controle social sobre gastos públicos
- Desenvolvimento de aplicações de interesse público
- Pesquisas acadêmicas
- Jornalismo investigativo

Desinformação e fake news

No contexto contemporâneo, marcado pela intensificação do uso das tecnologias digitais, observa-se uma ampliação significativa no acesso à informação. No entanto, esse mesmo ambiente que democratiza conteúdos também favorece a circulação de informações falsas ou distorcidas. A desinformação, nesse cenário, passa a ocupar um papel central nos debates sociais, uma vez que impacta diretamente a forma como os indivíduos compreendem a realidade e tomam decisões em diferentes esferas da vida cotidiana.

Tipos de desinformação:

- **Misinformation:** informação falsa compartilhada sem intenção de enganar
- **Disinformation:** informação falsa criada e compartilhada deliberadamente para enganar
- **Malinformation:** informação verdadeira usada para causar dano (como vazamento de dados privados)

Diante desse cenário, torna-se fundamental o desenvolvimento do letramento midiático e informacional, entendido como um conjunto de competências que possibilita ao indivíduo não apenas acessar informações, mas também avaliá-las de forma crítica.

Esse letramento envolve a capacidade de identificar conteúdos enganosos, utilizar informações de maneira ética e responsável, além de produzir e compartilhar conteúdos de qualidade. Trata-se, portanto, de uma habilidade essencial para a participação consciente na sociedade contemporânea.

Entre as habilidades que compõem esse conjunto de competências, destacam-se algumas práticas fundamentais, como a verificação da fonte da informação e a checagem da data de publicação, aspectos que ajudam a contextualizar o conteúdo.

Também é importante distinguir entre textos informativos e opinativos, bem como buscar múltiplas fontes que confirmem determinada informação. A atenção a títulos sensacionalistas e a análise da autenticidade de imagens — considerando possíveis manipulações ou retiradas de contexto — são igualmente estratégias relevantes no enfrentamento à desinformação.

Por fim, cabe mencionar o papel das iniciativas de checagem de fatos, que atuam como aliadas nesse processo. No Brasil, destacam-se agências como **Aos Fatos**, **Agência Lupa**, **Comprova** e **Fato ou Fake**, que se dedicam à verificação de informações que circulam no ambiente digital.

Ferramentas de fact-checking

Agências brasileiras de checagem de fatos:

- Aos Fatos (www.aosfatos.org)
- Agência Lupa (www.agencialupa.org)
- Comprova (www.projeto comprova.com.br)
- Fato ou Fake (www.g1.globo.com/fato-ou-fake)

Embora não substituam o desenvolvimento do pensamento crítico individual, essas ferramentas contribuem significativamente para a construção de um ecossistema informacional mais confiável.

Rumo à inclusão digital

A exclusão digital pode ser compreendida como a ausência de acesso às tecnologias digitais de informação e comunicação (TDICs) e/ou a incapacidade de utilizá-las de maneira significativa. Trata-se de um fenômeno multifacetado, que não se limita à simples disponibilidade de conexão à internet. Envolve, por um lado, o acesso físico, relacionado à existência de infraestrutura e dispositivos adequados, e, por outro, o acesso econômico, que diz respeito à possibilidade de custear serviços e equipamentos. Soma-se a isso a dimensão das competências digitais, ou seja, as habilidades necessárias para operar essas tecnologias, bem como a qualidade do acesso, que inclui aspectos como velocidade e estabilidade da conexão. Por fim, destaca-se o uso significativo das tecnologias, entendido como a capacidade de mobilizá-las de forma efetiva para ampliar oportunidades e melhorar as condições de vida.

Nesse contexto, a inclusão digital emerge como um direito fundamental, uma vez que o acesso efetivo às tecnologias digitais tornou-se condição indispensável para a participação plena na vida social, econômica e política. Mais do que garantir conexão, a inclusão digital pressupõe o desenvolvimento de habilidades, o acesso a conteúdos relevantes e a oferta de tecnologias acessíveis e adequadas às diferentes realidades. Assim, trata-se de um processo que articula infraestrutura, formação e uso crítico das tecnologias, permitindo que os indivíduos produzam conhecimento e exerçam sua cidadania de forma ativa.

A ausência dessa inclusão tende a perpetuar e até intensificar desigualdades já existentes. Indivíduos que não dispõem de acesso adequado às tecnologias digitais ficam à margem de oportunidades educacionais, de inserção no mercado de trabalho e de acesso a serviços públicos cada vez mais digitalizados. Além disso, sua participação em debates públicos e espaços de decisão torna-se limitada. Durante a pandemia de COVID-19, a exclusão digital tornou-se ainda mais evidente, com estudantes sem acesso à internet en-

frentando desvantagens educacionais significativas

Dimensões da inclusão digital

A inclusão digital possui múltiplas dimensões que devem ser consideradas de forma integrada:

Acesso Físico



Disponibilidade de infraestrutura de telecomunicações e dispositivos de acesso à internet. Isso inclui cobertura de banda larga, disponibilidade de dispositivos acessíveis e espaços públicos com acesso à internet.



Acesso Econômico

Capacidade financeira para custear serviços de internet e dispositivos digitais. Os custos de conectividade podem representar uma barreira significativa, especialmente para populações de baixa renda.

Habilidades Digitais



Competências necessárias para utilizar efetivamente as tecnologias digitais. Isso inclui desde habilidades básicas de navegação até competências avançadas de programação e análise de dados.



Conteúdo Relevante

Disponibilidade de informações e serviços digitais em idiomas locais e culturalmente apropriados. O conteúdo deve ser relevante para as necessidades e contextos específicos dos usuários.

Acessibilidade



Garantia de que as tecnologias digitais sejam acessíveis a pessoas com deficiências. Isso inclui design universal, tecnologias assistivas e interfaces adaptáveis.

Políticas públicas para inclusão digital

Governos ao redor do mundo têm desenvolvido políticas públicas para promover a inclusão digital. O Brasil, por meio do Programa Nacional de Banda Larga e outras iniciativas, busca expandir o acesso à internet e desenvolver habilidades digitais. Programas como o “Computador para todos” e iniciativas que garantem wi-fi público em espaços urbanos representam esforços para reduzir a exclusão digital.

A Lei Geral de Proteção de Dados (LGPD) brasileira também contribui para a inclusão di-

gital ao estabelecer direitos dos titulares de dados e promover transparência no tratamento de informações pessoais. Esta legislação ajuda a construir confiança no ambiente digital, incentivando maior participação online.

Educação digital e letramento informacional

A educação digital tornou-se fundamental para garantir que os indivíduos possam participar efetivamente da sociedade digital. Isso vai além do ensino de habilidades técnicas, incluindo também letramento informacional - a capacidade de encontrar, avaliar e utilizar informações de forma crítica e efetiva.

O letramento informacional é especialmente importante na era da desinformação, na qual a capacidade de distinguir entre fontes confiáveis e não confiáveis de informação torna-se uma necessidade para o exercício amplo da cidadania. Programas educacionais devem ensinar como navegar criticamente no ambiente informacional digital.

Estratégias para a promoção dos direitos digitais

Para promover efetivamente os direitos digitais, é necessária uma abordagem multifacetada que envolva:

- **Regulação equilibrada:** desenvolvimento de marcos regulatórios que protejam direitos fundamentais sem sufocar inovação tecnológica.
- **Investimento em infraestrutura:** expansão de redes de banda larga e melhoria da qualidade de conectividade, especialmente em áreas rurais e comunidades marginalizadas.
- **Educação e capacitação:** programas abrangentes de educação digital que desenvolvam tanto habilidades técnicas quanto pensamento crítico.
- **Transparência:** exige que plataformas digitais sejam transparentes sobre suas políticas de moderação de conteúdo e algoritmos.
- **Participação democrática:** envolvimento da sociedade civil e dos cidadãos em discussões sobre políticas digitais e governança da internet.

A realização plena dos direitos digitais requer reconhecer que a tecnologia não é neutra. As escolhas sobre como as tecnologias são projetadas, implementadas e regulamentadas refletem valores sociais e podem promover ou prejudicar direitos humanos. É essencial que essas escolhas sejam feitas por meio de processos democráticos que priorizem o bem-estar humano e a justiça social.



ESTRATÉGIA PEDAGÓGICA!

Proposta 1:

Atividade prática de verificação

- Apresente uma notícia suspeita aos estudantes;
- Ensine o passo a passo da verificação;
- Peça que busquem em agências de checagem;
- Discutam os resultados e aprendizados.

Proposta 2:

Caso prático - Desenvolvendo um projeto de inclusão digital

- **Contexto:** Você é educadora(or) em uma escola de comunidade periférica. Identificou que 40% dos estudantes não têm acesso adequado à internet e muitos nunca usaram um computador. A escola tem um pequeno laboratório de informática com 15 computadores antigos.



Figura 1: Pilares dos direitos digitais - síntese visual do módulo

Considerações finais

Chegamos ao final do primeiro módulo de nossa jornada com a compreensão de que os direitos humanos não apenas permanecem válidos no ambiente digital, como também assumem novas dimensões e urgências. Ao longo deste percurso, refletimos sobre como esses direitos se manifestam na contemporaneidade, marcada pela intensa presença das tecnologias digitais em todas as esferas da vida social.

Nesse contexto, reconhecemos a importância dos marcos regulatórios — desde a Declaração Universal dos Direitos Humanos até legislações específicas como o Marco Civil da Internet e a Lei Geral de Proteção de Dados — como instrumentos fundamentais para a proteção de direitos, ainda que demandem constante atualização diante da velocidade das transformações tecnológicas.

Também avançamos na compreensão da interseccionalidade digital, percebendo que os impactos das tecnologias não se distribuem de forma homogênea. Grupos historicamente vulnerabilizados — como mulheres negras, pessoas LGBTQIA+, populações periféricas, pessoas com deficiência, idosos e crianças — enfrentam desafios específicos no ambiente digital, o que exige uma análise crítica sensível às desigualdades estruturais.

Nesse sentido, aprofundamos três direitos digitais fundamentais:

- a liberdade de expressão online, que amplia vozes, mas encontra limites quando se converte em discurso de ódio ou desinformação;
- o acesso à informação, potencializado pelas tecnologias, mas ameaçado pelas fake news, o que demanda o fortalecimento do letramento midiático e informacional;
- e a inclusão e acessibilidade digital, que permanecem como desafios estruturais e requerem tanto políticas públicas quanto ações educativas.

Os fundamentos construídos neste módulo servirão de base para os próximos passos da nossa formação. No Módulo 2, abordaremos as implicações éticas da inteligência artificial, investigando como algoritmos podem reproduzir desigualdades e como podem ser orientados por princípios de justiça e direitos humanos. Já no Módulo 3, aprofundaremos temas relacionados à privacidade, à proteção de dados e à segurança digital, cada vez mais centrais em um cenário de vigilância e circulação massiva de informações.

Por fim, reafirmamos o papel essencial de educadoras e educadores na construção de uma sociedade digital mais justa, inclusiva e democrática.

Mais do que conhecer os direitos, é necessário promover práticas educativas que incentivem seu exercício, denunciar violações e fomentar espaços de respeito e participação.

Isso implica incorporar discussões sobre direitos digitais em contextos formativos, promover o letramento digital crítico, apoiar iniciativas de inclusão, exigir acessibilidade e engajar-se em redes e movimentos que defendam esses direitos.

Em um mundo em constante transformação, somos chamados a assumir uma postura ativa: não como meros espectadores, mas como protagonistas na construção do futuro digital que desejamos.

Até o próximo módulo!

Referências

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: <https://link.ufms.br/ewn3o>. Acesso em: 8 jan. 2026.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Brasília, DF: Presidência da República, 2011. Disponível em: <https://link.ufms.br/pviD3>. Acesso em: 8 jan. 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: <https://link.ufms.br/EWpqC>. Acesso em: 8 jan. 2026.

BRASIL. **Lei n. 13.146, de 6 de julho de 2015**. Institui a Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência). Brasília, DF: Presidência da República, 2015. Disponível em: <https://link.ufms.br/XiEEq>. Acesso em: 8 jan. 2026.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: <https://link.ufms.br/WkeVA>. Acesso em: 8 jan. 2026.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (CETIC.BR). **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2022**. São Paulo: Comitê Gestor da Internet no Brasil, 2023. Disponível em: <https://link.ufms.br/1FD62>. Acesso em: 8 jan. 2026.

CRENSHAW, Kimberlé. **Documento para o encontro de especialistas em aspectos da discriminação racial relativos ao gênero**. Revista Estudos Feministas, Florianópolis, v. 10, n. 1, p. 171-188, jan. 2002. Disponível em: <https://link.ufms.br/EgX33>. Acesso em: 8 jan. 2026.

KAUFMAN, Dora. **Desmistificando a inteligência artificial**. Belo Horizonte: Autêntica, 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Assembleia Geral. **Resolução 68/167**. The right to privacy in the digital age. Nova York: ONU, 2013. Disponível em: <https://link.ufms.br/RfcqJ>. Acesso em: 8 jan. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Declaração Universal dos Direitos Humanos**. Paris: ONU, 1948. Disponível em: <https://link.ufms.br/a9rRL>. Acesso em: 8 jan. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **International Covenant on Civil and Political Rights**. Nova York: ONU, 1966. United Nations Treaty Series, v. 999, p. 171. Disponível em: <https://link.ufms.br/FS19f>. Acesso em: 8 jan. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Resolução A/HRC/RES/20/8: The promotion, protection and enjoyment of human rights on the Internet**. Genebra: Conselho de Direitos Humanos da ONU, 2012. Disponível em: <https://link.ufms.br/rfEIs>. Acesso em: 8 jan. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA (UNESCO). **Alfabetização midiática e informacional: currículo para formação de professores**. Brasília: UNESCO, 2013. Disponível em: <https://link.ufms.br/o8ANT>. Acesso em: 8 jan. 2026.

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. **Regulamento (UE) 2016/679: Regulamento Geral sobre a Proteção de Dados (RGPD)**. Bruxelas: União Europeia, 2016. Disponível em: <https://link.ufms.br/yWooT>. Acesso em: 8 jan. 2026.

PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional**. 19. ed. São Paulo: Saraiva Jur, 2021.

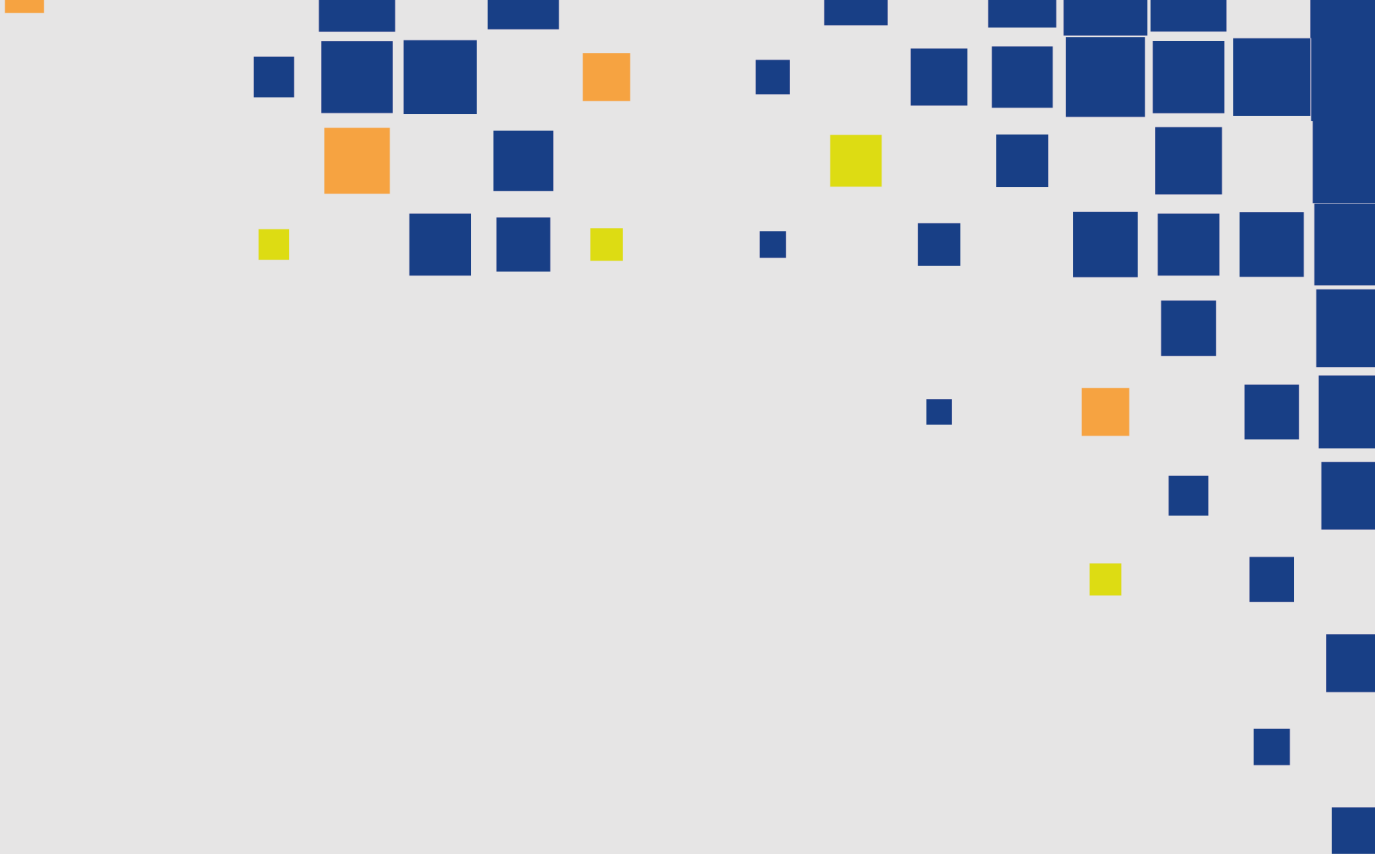
RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

SAFERNET BRASIL. **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos**. Salvador: SaferNet Brasil, 2023. Disponível em: <https://link.ufms.br/kgPlq>. Acesso em: 8 jan. 2026.

SALGADO, Karine; CAMPOS, Gabriel Afonso. **Educação, tecnologia e direitos humanos**. Revista de Ciências do Estado, Belo Horizonte, v. 8, n. 2, p. 1–15, 2023. Disponível em: <https://link.ufms.br/mVnXi>. Acesso em: 08 jan. 2026.

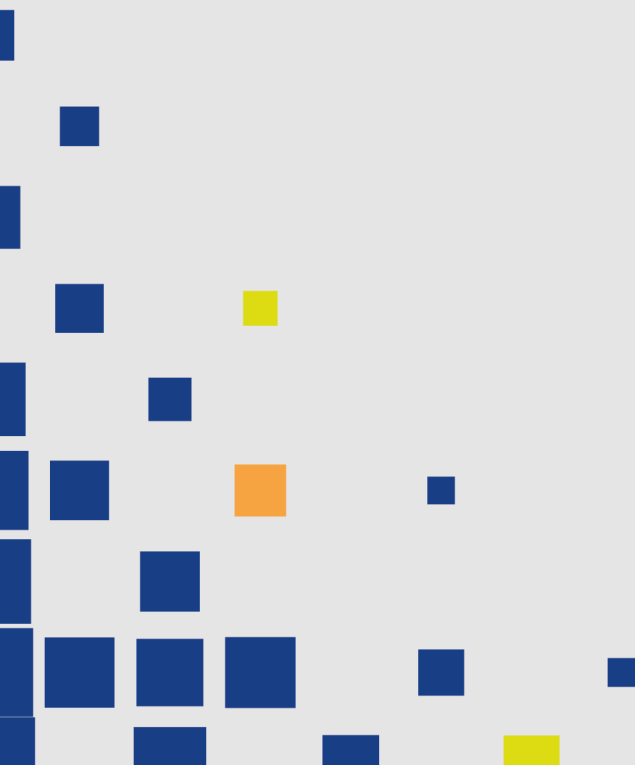
SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco Civil da Internet: construção e aplicação**. Juiz de Fora: Editar, 2016. Disponível em: <https://link.ufms.br/9Rjl6>. Acesso em: 8 jan. 2026.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Rio de Janeiro: Intrínseca, 2021.



Módulo 2

Ética, Direitos Humanos e Inteligência Artificial



Apresentação

Bem-vinda(o) ao segundo módulo de nossa disciplina!

Imagine as seguintes situações: um sistema de inteligência artificial (IA) usado por um banco nega automaticamente empréstimos para pessoas de determinados bairros periféricos. Uma ferramenta de reconhecimento facial identifica erroneamente uma pessoa negra como suspeita de crime. Um algoritmo de recrutamento descarta currículos de mulheres para vagas de tecnologia.

Essas situações não são ficção científica – são casos reais que evidenciam como a inteligência artificial, uma das tecnologias mais transformadoras de nosso tempo, pode reproduzir e até amplificar discriminações, preconceitos e violações de direitos humanos.

A IA está presente em nosso cotidiano de formas que nem sempre percebemos: nos feeds de redes sociais que decidem o que vemos, nos sistemas de GPS que escolhem nossas rotas, nos assistentes virtuais que respondem nossas perguntas, nos algoritmos que recomendam filmes, músicas e produtos. Cada vez mais, sistemas de IA tomam ou influenciam decisões que afetam profundamente nossas vidas: aprovação de crédito, diagnósticos médicos, seleção de candidatos a empregos, concessão de liberdade condicional, e, até mesmo, decisões sobre quem recebe benefícios sociais.

Como educadoras e educadores em direitos humanos, precisamos compreender essa tecnologia: suas potencialidades, seus riscos, seus impactos sociais e, principalmente, como garantir que seja desenvolvida e utilizada de forma ética, justa e alinhada aos direitos humanos.

A IA pode ser uma aliada na promoção da justiça social – ajudando a identificar violações de direitos, democratizando acesso a serviços, personalizando a educação, auxiliando diagnósticos médicos. Mas também pode ser uma ferramenta de opressão – perpetuando discriminações, invadindo privacidade, concentrando poder, substituindo trabalho humano sem proteção social adequada.

Neste módulo, vamos mergulhar no universo da inteligência artificial com um olhar crítico e humanista. Não se trata de demonizar a tecnologia, mas de compreendê-la para que possamos orientá-la em direção a um futuro mais justo e inclusivo.

Ao final deste módulo, você será capaz de compreender os fundamentos básicos da inteligência artificial, reconhecendo conceitos centrais como algoritmos, *machine learning* e o papel dos dados em seu funcionamento. Também será possível identificar e discutir princípios éticos essenciais para o desenvolvimento e uso dessas tecnologias, tais como

transparência, justiça e privacidade, articulando-os com práticas concretas.

Ao longo do percurso, você desenvolverá a capacidade de analisar criticamente como vieses algorítmicos podem reproduzir e até ampliar desigualdades sociais já existentes, além de avaliar, de forma contextualizada, os riscos e as oportunidades que a IA apresenta para os direitos humanos em diferentes cenários. O módulo também permitirá reconhecer marcos regulatórios emergentes e compreender seus impactos, bem como aplicar ferramentas e metodologias de inteligência artificial de maneira ética no campo da educação em direitos humanos.

Por fim, você irá iniciar o desenvolvimento do seu letramento em IA, tanto em sua própria prática quanto na formação de seus estudantes, ampliando repertórios e promovendo uma atuação mais consciente e crítica.

Para alcançar esses objetivos, o módulo está estruturado em duas unidades complementares. Na **Unidade 1**, intitulada “**Princípios éticos e desafios da IA para os Direitos Humanos**”, serão explorados os conceitos fundamentais da inteligência artificial, seu funcionamento e os princípios éticos que devem orientá-la. Além disso, serão discutidos os impactos dos vieses algorítmicos, os riscos associados à vigilância digital e os principais marcos regulatórios que vêm sendo construídos nesse campo.

Já na **Unidade 2**, “**IA na Educação em Direitos Humanos – oportunidades, riscos e práticas pedagógica**”, o foco recai sobre as possibilidades de uso da IA para a promoção dos direitos humanos, suas aplicações no contexto educacional e os desafios específicos que emergem nesse cenário. Também serão abordadas estratégias para o desenvolvimento do letramento em IA e para a construção de práticas pedagógicas críticas e transformadoras.

Prepare-se para questionar, refletir e construir uma visão crítica sobre uma das tecnologias mais impactantes do nosso tempo, compreendendo não apenas seu potencial, mas também suas implicações éticas, sociais e educacionais.

Unidade 1

Princípios éticos e desafios da IA para os direitos humanos



Descrição: Ilustração de mulher frente a frente com robô virtual em perfil, iluminados em tons de azul e laranja. **Fonte:** Magnific.

Inteligência Artificial (IA) é um campo da ciência da computação dedicado a criar sistemas capazes de realizar tarefas que normalmente exigiriam inteligência humana: reconhecer padrões, tomar decisões, compreender linguagem, resolver problemas complexos.

Diferentemente de programas tradicionais que seguem instruções fixas, sistemas de IA podem aprender com dados e melhorar seu desempenho ao longo do tempo.



Descrição: capa do livro Desmistificando a inteligência artificial, KAUFMAN, Dora. São Paulo: Autêntica, 2022

No livro “**Desmistificando a inteligência artificial**” de Dora Kaufman, a autora ressalta a importância de compreendermos que a IA não é uma tecnologia neutra, mas incorpora os valores, preconceitos e limitações de seus criadores e dos dados utilizados em seu treinamento.

Como observa Dora Kaufman em “Desmistificando a inteligência artificial”, é importante compreender que a IA não é uma tecnologia neutra, mas incorpora os valores, preconceitos e limitações de seus criadores e dos dados utilizados em seu treinamento.



A ética da IA não é apenas uma questão técnica, mas uma questão sobre valores humanos e sociais. As decisões sobre como projetar, treinar e implementar sistemas de IA refletem escolhas sobre que tipo de sociedade queremos construir. Essas escolhas podem promover justiça, igualdade e bem-estar humano, ou podem perpetuar e amplificar discriminações, desigualdades e injustiças existentes.



CONCEITOS-CHAVE

Algoritmo: conjunto de instruções passo a passo para resolver um problema ou realizar uma tarefa. É a “receita” que o computador segue.

Machine learning (aprendizado de máquina): subcampo da IA em que sistemas aprendem padrões a partir de dados, sem serem explicitamente programados para cada situação.

Dados de treinamento: conjunto de informações usado para “ensinar” um sistema de IA. A qualidade e representatividade desses dados são de extrema relevância.

Modelo: sistema de IA treinado que pode fazer previsões ou tomar decisões com base em novos dados.

A Inteligência Artificial (IA) no cotidiano

Nos últimos anos a Inteligência Artificial deixou de ser um conceito futurista e distante da população e hoje é uma ferramenta ativa em nosso cotidiano, transformando a forma como navegamos, consumimos conteúdos e até nos comunicamos.

Para compreendermos melhor o seu impacto, a ciências da computação categoriza essa tecnologia em dois grandes grupos: a IA Estreita (Narrow AI), que engloba todas as soluções especializadas que utilizamos hoje, e a IA Geral (AGI), que representa um modelo teórico de capacidade humana integral, ou seja, uma IA hipotética com capacidade cognitiva humana completa, mas vale ressaltar que atualmente não há registros de que alguma IA tenha conseguido atingir esse nível tecnológico. A seguir observe alguns tipos de IA Estreita e os exemplos práticos de sua aplicação no dia a dia.

Tipos de IA Estreita (Narrow AI) Especializada em tarefas específicas!		
 Recurso/Tecnologia:	 O que faz no cotidiano:	 Exemplo de aplicações:
 Assistentes virtuais	Resgata informações e executa comandos por escrito ou por voz ...	Siri, Alexa, Google Assistant ...
 Sistemas de navegação	Calcula rotas e analisa o trânsito em tempo real	Waze e Google Maps ...
 Sistemas de recomendações	Sugere conteúdos com base no histórico do usuário.	Netflix, Spotify, Instagram, TikTok, Youtube e e-commerces...
 Filtros inteligentes	Organiza dados e bloqueia conteúdos indesejáveis.	Filtros de Spam em e-mails, bloqueadores de propagandas ...
 Reconhecimento facial	Identifica rostos para segurança, organização e melhoria de qualidade.	Acesso a portarias eletrônicas e organização automática de fotos...
 Processamento de linguagem	Traduz e simula conversas humanas.	Tradução automática e Chatbots de atendimento ao cliente ...

fonte: Gerada por IA - ChatGPT.

Para Refletir

Se a IA aprende com dados do passado, e o passado está repleto de discriminações e desigualdades, o que acontece quando usamos esses dados para treinar sistemas que tomarão decisões sobre o futuro? Como alerta Kaufman, a IA se estrutura a partir de dados e escolhas humanas, o que pode reproduzir padrões e desigualdades (Kaufman, 2022).

A ética aplicada à inteligência artificial baseia-se em tradições filosóficas milenares, adaptadas aos desafios únicos das tecnologias contemporâneas. Três abordagens éticas principais são particularmente relevantes:

Ética deontológica: baseada na filosofia de Immanuel Kant, esta abordagem enfatiza que certas ações são intrinsecamente certas ou erradas, independentemente de suas consequências. No contexto da IA, isso implica que alguns usos de tecnologia são inaceitáveis mesmo que produzam benefícios, como sistemas de vigilância que violam a dignidade humana.

Ética consequencialista: focada nos resultados das ações, esta abordagem avalia a moralidade com base nas consequências produzidas. Para a IA, isso significa avaliar se os benefícios de um sistema superam seus riscos e custos sociais.

Ética da virtude: centrada no caráter moral dos agentes, esta abordagem pergunta que virtudes devem orientar o desenvolvimento de IA. Virtudes como honestidade, justiça,

compaixão e prudência devem guiar cientistas, engenheiros e formuladores de políticas.



VÍDEO RECOMENDADO

“Inteligência Artificial: O que é e como funciona?” - Canal Código Fonte TV

Duração: 51,25 minutos

O vídeo apresenta uma explicação didática sobre conceitos básicos de IA, machine learning e redes neurais

[Clique aqui para acessar o vídeo!](#)



Descrição: Uma pessoa usa notebook com gráficos holográficos e ícone de Inteligência Artificial (IA) na tela. **Fonte:** Magnific.

Princípios éticos aplicados à inteligência artificial

Sistemas de inteligência artificial não são neutros: eles incorporam valores, escolhas e contextos sociais. Ao serem desenvolvidos, carregam os princípios e visões de mundo de quem os programa, além de reproduzirem os vieses presentes nos dados utilizados em seu treinamento.

Também refletem decisões de design e implementação que, muitas vezes, passam despercebidas, mas que têm impactos diretos na forma como esses sistemas operam. Nesse sentido, a IA está profundamente conectada às estruturas de poder existentes na sociedade, podendo reforçar desigualdades já estabelecidas.

Diante disso, a presença de princípios éticos claros torna-se indispensável. Sem essa orientação, sistemas de IA podem perpetuar e até ampliar discriminações, violar direitos fundamentais como a privacidade e a dignidade humana, além de concentrar poder em grandes corporações ou instituições.

Outro risco significativo está na tomada de decisões automatizadas sem transparência ou possibilidade de explicação, o que compromete a responsabilização. Além disso, a substituição do trabalho humano por sistemas automatizados, quando não acompanhada de políticas de proteção social, pode aprofundar desigualdades e gerar novos desafios econômicos e sociais.

Com base nessas tradições filosóficas e nas necessidades específicas da era digital, emergiram princípios éticos fundamentais para a inteligência artificial:

1. Transparência e explicabilidade

A transparência exige que sistemas de IA sejam compreensíveis para seus usuários e para aqueles afetados por suas decisões. Este princípio é fundamental para permitir que indivíduos contestem decisões automatizadas que os afetem.

A explicabilidade vai além da transparência, exigindo que sistemas de IA possam fornecer explicações claras e compreensíveis sobre como chegaram a determinadas decisões. Isso é particularmente importante em áreas como diagnóstico médico, decisões judiciais e aprovação de crédito, nas quais as consequências das decisões podem ser significativas para a vida das pessoas.

Contudo, a explicabilidade enfrenta desafios técnicos significativos. Sistemas de aprendizado profundo (deep learning) podem ser tão complexos que mesmo seus criadores não compreendem completamente como eles chegam a determinadas conclusões.

2. Justiça e não-discriminação

O princípio da justiça exige que sistemas de IA não discriminem injustamente indivíduos ou grupos. Isso é particularmente desafiador porque algoritmos de IA aprendem a partir de dados históricos que podem refletir discriminações passadas e presentes.

A justiça algorítmica não é um conceito simples, pois envolve diferentes definições de equidade que podem ser matematicamente incompatíveis. Isso requer escolhas éticas explícitas sobre que tipo de justiça priorizar em diferentes contextos.

Exemplos de discriminação algorítmica incluem:

- Sistemas de recrutamento que discriminam contra mulheres
- Algoritmos de aprovação de crédito que desfavorecem minorias étnicas
- Sistemas de reconhecimento facial que funcionam mal para pessoas de pele escura
- Algoritmos de justiça criminal que reproduzem vieses raciais

Desafio: Como garantir justiça quando os dados históricos refletem discriminações?

3. Privacidade e proteção de dados

A privacidade é um direito fundamental que contribui para a dignidade humana e a autonomia individual. Sistemas de IA frequentemente requerem grandes quantidades de dados pessoais para funcionar efetivamente, criando tensões entre utilidade tecnológica e proteção da privacidade.

Os princípios de proteção de dados orientam o uso responsável das informações pessoais e incluem a minimização de dados, que consiste em coletar apenas o estritamente necessário para finalidades específicas; a finalidade específica, que determina que os dados sejam utilizados exclusivamente para os propósitos previamente informados; o consentimento informado, garantindo que os indivíduos compreendam de forma clara como seus dados serão coletados e utilizados; e o direito ao esquecimento, que assegura às pessoas a possibilidade de solicitar a remoção de suas informações quando desejarem.

A Lei Geral de Proteção de Dados (LGPD) brasileira estabelece esses princípios como direitos fundamentais, criando obrigações legais para organizações que processam dados pessoais.

4. Autonomia e controle humano

O princípio da autonomia humana exige que sistemas de IA preservem a capacidade humana de tomar decisões significativas sobre suas próprias vidas. Isso implica que as pessoas devem manter controle final sobre decisões importantes, especialmente aquelas que afetam direitos fundamentais.

Este princípio levanta questões sobre automação e substituição humana. Embora a automação possa trazer eficiência e precisão, ela também pode reduzir a agência e criar dependência excessiva de sistemas tecnológicos.

5. Responsabilidade

Sistemas de IA devem ser desenvolvidos e implementados de forma que seja possível identificar responsabilidades quando algo dá errado. Isso requer estruturas claras de governança e mecanismos que permitam identificar e remediar danos.

A responsabilidade em IA é complexa porque envolve múltiplos atores: desenvolvedores, operadores, usuários e reguladores. Cada um desses atores tem responsabilidades específicas, mas também compartilha responsabilidade coletiva pelo impacto social dos sistemas de IA.

Desafios Éticos Específicos

Viés algorítmico e discriminação: Algoritmos podem reproduzir e amplificar discriminações existentes na sociedade, criando novas formas de injustiça digital. Esses vieses podem surgir de várias fontes:

Viés nos dados: dados de treinamento que não representam adequadamente a diversidade populacional ou que refletem discriminações históricas.

Viés no design: escolhas de design que inadvertidamente favorecem certos grupos e não outros.

Viés na implementação: uso inadequado de sistemas de IA em contextos para os quais não foram projetados.

Casos Reais de Discriminação Algorítmica

CASO 1: Reconhecimento Facial Racialmente Enviesado

Pesquisa do MIT e Stanford (2018) revelou que sistemas comerciais de reconhecimento facial tinham:

- Taxa de erro de 0,8% para homens brancos
- Taxa de erro de 34,7% para mulheres negras

Impacto: Pessoas negras sendo erroneamente identificadas como suspeitas de crimes.

CASO 2: Sistema de Recrutamento da Amazon

A Amazon desenvolveu (e depois descartou) um sistema de IA para triagem de currículos que sistematicamente desfavorecia mulheres, porque foi treinado com dados de contratações passadas em uma indústria dominada por homens.

Veja na íntegra: DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. Reuters, San Francisco, 10 out. 2018.

[Acesse aqui!](#)



Casos Reais de Discriminação Algorítmica

CASO 3: COMPAS - Predição de Reincidência Criminal (EUA)

Sistema usado para prever probabilidade de reincidência criminal apresentava viés racial:

- Superestimava risco de reincidência para réus negros
- Subestimava risco para réus brancos

Impacto: Pessoas negras recebendo sentenças mais duras e sendo negadas liberdade condicional injustamente.

CASO 4: Algoritmos de Crédito

Sistemas de análise de crédito usando dados de redes sociais, histórico de navegação e localização podem discriminar pessoas de bairros periféricos, mesmo quando têm boa capacidade de pagamento.

Acima conhecemos alguns casos recentes que envolvem questões éticas no uso da IA. O caso 2, que ocorreu com o sistema de recrutamento da Amazon, é um dos mais conhecidos e divulgados que mostra como a IA não é neutra e que sua tomada de decisão depende do banco de dados que alimenta a ferramenta.



Descrição: Logotipo internacional da Amazon.

Fonte: Wikimedia.

No caso da Amazon, o sistema aprendeu a discriminar mulheres, com base nos históricos de contratações que favoreciam candidatos do sexo masculino, e assim foi definindo as novas contratações demonstrando como vieses históricos podem ser perpetuados por algoritmos.

O caso da Amazon também nos ajuda a compreender um pouco mais do que os pesquisadores brasileiros denominam de ‘racismo e sexismo algorítmico’. Segundo Silva (2022), a automação de processos seletivos baseada em dados históricos tende a excluir grupos que foram sistematicamente marginalizados no passado, transformando o código em um espelho das desigualdades sociais.

A automação baseada em IA levanta questões éticas fundamentais sobre o futuro do trabalho e da distribuição de renda. Embora a automação possa aumentar a produtividade e reduzir custos, ela também pode deslocar trabalhadores e aumentar desigualdades econômicas.

As considerações éticas relacionadas aos impactos da inteligência artificial no mundo do trabalho envolvem, a responsabilidade social das empresas diante dos trabalhadores potencialmente deslocados por processos de automação.

Nesse contexto, torna-se fundamental a implementação de programas de requalificação profissional e de educação continuada, capazes de preparar esses indivíduos para novas demandas do mercado. Além disso, discute-se a possibilidade de adoção de políticas como a renda básica universal, como forma de mitigar os efeitos do desemprego tecnológico. Por fim, destaca-se a importância de preservar e valorizar atividades que envolvem o cuidado humano e a criatividade, dimensões que permanecem centrais e dificilmente substituíveis por sistemas automatizados.



VÍDEO RECOMENDADO

“Dez princípios para utilizar a inteligência artificial com ética” - Canal USP

Duração: 5 minutos.

Podcast sobre os princípios da Declaração de Montreal para uso ético da IA

[Clique aqui para acessar o vídeo!](#)

Para Refletir!

A ética da IA não busca apenas prevenir danos, mas promover ativamente o bem-estar e a justiça social. Isso requer que vejamos a IA não apenas como uma ferramenta técnica, mas como uma força social que pode moldar o futuro da humanidade.

O desenvolvimento de sistemas cada vez mais autônomos - como veículos, robôs militares e sistemas de trading financeiro - levanta questões sobre responsabilidade moral.

Quem é responsável quando um sistema autônomo causa danos? Como atribuir responsabilidade a sistemas que aprendem independentemente de seus criadores?

A implementação de princípios éticos em sistemas de IA requer abordagens práticas e sistemáticas:

- Avaliação de impacto ético: processos estruturados para avaliar potenciais impactos éticos de sistemas de IA antes de sua implementação.
- Auditoria algorítmica: exame regular de sistemas de IA para identificar vieses, er-

ros ou impactos não intencionais.

- Comitês de ética: estabelecimento de comitês multidisciplinares para orientar decisões éticas em desenvolvimento de IA.
- Treinamento em ética: educação de desenvolvedores, gerentes e usuários sobre considerações éticas em IA.

Você sabia!

Que organizações internacionais têm desenvolvido frameworks éticos para orientar o desenvolvimento responsável de IA?

Veja alguns exemplos:

UNESCO: A Recomendação sobre Ética da IA da UNESCO estabelece princípios globais para desenvolvimento ético de IA, enfatizando direitos humanos, diversidade cultural e sustentabilidade **ambiental**.

União Europeia: O Regulamento de IA da UE estabelece requisitos legais para sistemas de IA de alto risco, priorizando transparência, accountability e proteção de direitos fundamentais.

OCDE: Os Princípios de IA da OCDE promovem IA inovadora e confiável que respeite direitos humanos e valores democráticos.



ESTRATÉGIA PEDAGÓGICA!

Atividade: Detectando Vieses

Apresente aos estudantes cenários de uso de IA e peça que identifiquem:

- Que dados estão sendo usados?
- Que grupos podem estar sub-representados?
- Que vieses históricos podem estar nos dados?
- Quem pode ser prejudicado?
- Como corrigir ou mitigar esses vieses?



Para Refletir!

Até que ponto devemos aceitar vigilância em nome de segurança, eficiência ou conveniência? Onde está o limite entre proteção e opressão?



VÍDEO RECOMENDADO

“Coded Bias” (Viés Codificado) - trailer e discussão

Duração: 3 minutos.

Documentário sobre discriminação algorítmica, especialmente em reconhecimento facial (Buolamwini; Gebru, 2018). Apresenta pesquisa de Joy Buolamwini sobre vieses raciais em IA.

[Clique aqui para acessar o vídeo!](#)

Unidade 2

O Uso da Inteligência Artificial na Promoção e Proteção dos Direitos Humanos



Descrição: Homem interagindo com telas virtuais holográficas de gráficos e mapa-múndi sobre mesa de trabalho. **Fonte:** Maginific.

Embora muito da discussão sobre inteligência artificial e direitos humanos foque nos riscos e desafios, é igualmente importante reconhecer o potencial transformador da IA para promover e proteger direitos humanos.

Quando desenvolvida e implementada de forma ética e responsável, a IA pode ser uma ferramenta poderosa para avançar a justiça social, ampliar o acesso a serviços essenciais e empoderar comunidades marginalizadas.

A capacidade da IA de processar grandes volumes de dados, identificar padrões complexos e automatizar tarefas repetitivas pode ser direcionada para resolver alguns dos desafios mais persistentes da humanidade. Desde melhorar o acesso à educação e saúde até combater a pobreza e promover a igualdade, a IA oferece oportunidades sem precedentes para acelerar o progresso em direitos humanos.

Monitoramento de Violações de Direitos Humanos

Análise de grandes volumes de dados:

- Identificação de padrões de violência
- Mapeamento de conflitos e deslocamentos forçados
- Detecção de trabalho escravo em cadeias produtivas
- Monitoramento de desmatamento e crimes ambientais



Exemplo: Organizações de direitos humanos usam IA para analisar imagens de satélite e identificar destruição de vilarejos em zonas de conflito.

Acesso à Justiça

IA pode democratizar acesso a informações e serviços jurídicos:

- Chatbots jurídicos que orientam sobre direitos
- Sistemas de busca inteligente em legislação
- Análise de jurisprudência para identificar precedentes
- Assistência na elaboração de petições simples
- Tradução de documentos jurídicos

Exemplo: No Brasil, projetos como “Robô Laura” (TJ-RO) e “Elis” (TJ-PE) auxiliam cidadãos a obter informações sobre processos.

Fontes: TRIBUNAL DE JUSTIÇA DE RONDÔNIA. Justiça de Rondônia lança “Laura”, a primeira inteligência artificial do Judiciário estadual. Porto Velho: TJRO, 2021

TRIBUNAL DE JUSTIÇA DE PERNAMBUCO. Elis: Inteligência Artificial do TJPE agiliza a tramitação de processos de execução fiscal. Recife: TJPE, 2020

Combate ao Tráfico Humano e Trabalho Escravo

IA pode analisar:

- Anúncios online suspeitos
- Padrões de movimentação financeira
- Imagens e vídeos para identificar vítimas
- Cadeias de suprimento para detectar trabalho forçado

Exemplo: Organização Thorn usa IA para identificar e resgatar crianças vítimas de exploração sexual. O Thorn é uma organização internacional fundada pelos atores Ashton Kutcher e Demi Moore, focada na proteção infantil online.

[Para conhecer mais sobre a organização acesse aqui!](#)

Tradução e Acessibilidade

IA quebrando barreiras linguísticas e de acessibilidade:

- Tradução automática em tempo real
- Legendas automáticas para vídeos
- Conversão de texto em fala (text-to-speech)

- Conversão de fala em texto (speech-to-text)
- Descrição automática de imagens para pessoas cegas
- Tradução para língua de sinais

Impacto: Pessoas com deficiência e falantes de idiomas minoritários tendo maior acesso a informações e serviços.

Fonte: No Brasil, a fonte principal é o Hand Talk, que utiliza um avatar 3D para traduzir sites e vídeos para a Língua Brasileira de Sinais. HAND TALK. Tecnologia e acessibilidade digital para a comunidade surda. Maceió, 2023.

[Para saber mais sobre a Hand Talk clique aqui!](#)

Saúde e Bem-Estar

IA na promoção do direito à saúde:

- Diagnóstico auxiliar de doenças
- Triagem em emergências
- Identificação de surtos epidêmicos
- Personalização de tratamentos
- Telemedicina em áreas remotas
- Análise de imagens médicas

Exemplo: Sistemas de IA detectando câncer de pele, retinopatia diabética e tuberculose com precisão comparável a especialistas.



VÍDEO RECOMENDADO

“Como a IA pode ajudar os direitos humanos” - TED Talk

Palestrante: Fei-Fei Li

Duração: 18 minutos.

Cientista da computação discute potencial da IA para o bem social

[Clique aqui para acessar o vídeo!](#)

Conheças alguns Casos de Estudo: IA para o Bem Social

CASO 1: Microsoft AI for Good

A Microsoft desenvolveu várias iniciativas utilizando IA para abordar desafios globais, incluindo conservação ambiental, acessibilidade, resposta humanitária e direitos humanos. Seus projetos demonstram como grandes corporações tecnológicas podem direcionar recursos para o bem social.

CASO 2: Projeto Thorn

A organização Thorn utiliza IA para combater exploração sexual infantil online, desenvolvendo ferramentas que ajudam autoridades policiais a identificar e resgatar vítimas mais rapidamente.

Caso 3: Crisis Text Line

Esta organização utiliza IA para analisar conversas de texto e identificar pessoas em risco de suicídio, permitindo intervenções mais rápidas e efetivas.

IA na Educação: Potencialidades

O direito à educação, consagrado no artigo 26 da Declaração Universal dos Direitos Humanos, pode ser significativamente avançado através de tecnologias de IA. Sistemas inteligentes podem personalizar a aprendizagem, tornando a educação mais efetiva e acessível para estudantes com diferentes necessidades e estilos de aprendizagem.



Ferramentas de Apoio Pedagógico



Planos de aula e avaliações



Correção automatizada



Análise de desempenho



Sugestões de recursos



Para Estudantes



Tutores virtuais 24/7



Escrita assistida



Resumos e traduções



Auxílio em pesquisas



Inclusão de Estudantes com Deficiência



Leitura de textos e legendas automáticas



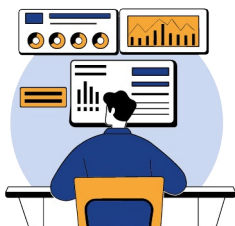
Fala para texto e interfaces adaptativas



Simplificação de textos



Tecnologia assistiva para todos



Análise de Dados Educacionais

Identificar risco de evasão



Detectar dificuldades de aprendizagem



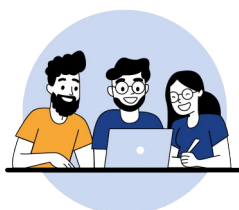
Avaliar eficácia de metodologias



Otimizar recursos



Potencial: Intervenções precoces para prevenir evasão e apoiar estudantes em dificuldade.



Democratização do Conhecimento



Plataformas adaptativas online



Tradução de cursos



Chatbots educacionais



Recomendação personalizada de recursos

Personalização da Aprendizagem

Algoritmos de IA podem analisar o progresso individual de estudantes, identificando lacunas de conhecimento e adaptando conteúdos e métodos de ensino às necessidades específicas de cada aluno. Isso é particularmente valioso para estudantes com dificuldades de aprendizagem ou aqueles que precisam de apoio adicional.

Democratização do Acesso

Plataformas educacionais baseadas em IA podem tornar educação de qualidade acessível em regiões onde recursos educacionais são escassos. Sistemas de tutoria inteligente podem fornecer instrução personalizada mesmo na ausência de professores qualificados.

Tradução e Localização

Tecnologias de IA podem traduzir conteúdos educacionais para idiomas locais e adaptar materiais a contextos culturais específicos, removendo barreiras linguísticas e culturais ao acesso à educação.

Um exemplo inspirador é o uso de IA pela organização não governamental Pratham na Índia, que desenvolveu sistemas adaptativos para ensinar matemática e leitura a crianças em comunidades rurais, ajudando milhões de estudantes a melhorar suas habilidades básicas.

Vigilância Algorítmica de Estudantes



Proctoring (Supervisão Algorítmica em Provas)

Sistemas que monitoram estudantes durante provas online através de:

- Câmera (movimentos faciais e corporais)
- Microfone (sons no ambiente)
- Tela (navegação e tentativas de “colar”)
- Análise de padrões de digitação

Problemas:

- Invasão severa de privacidade
- Estudantes sendo filmados em suas casas
- Falsos positivos (sistema acusando cola incorretamente)
- Discriminação contra estudantes com deficiência ou neurodivergentes
- Estresse e ansiedade exacerbados
- Normalização da vigilância

Caso real: Durante a pandemia, universidades adotaram sistemas de proctoring que geraram denúncias de violação de privacidade e discriminação.



Decisões Automatizadas sobre Trajetórias Escolares

Riscos de sistemas de IA decidirem:

- Aprovação/reprovação
- Direcionamento para turmas ou trilhas
- Previsão de “potencial” acadêmico
- Recomendações de carreira

Problemas:

- Vieses reproduzindo desigualdades
- Profecia autorrealizável (estudantes rotulados como “baixo potencial” recebendo menos investimento)
- Perda de nuances e contexto
- Redução de estudantes a métricas

Perda de Autonomia Docente



Preocupações:

- Professores se tornando meros executores de scripts gerados por IA
- Desvalorização do conhecimento pedagógico
- Padronização excessiva do ensino
- Perda da dimensão relacional e afetiva da educação
- Substituição de professores por sistemas automatizados



Aprofundamento de Desigualdades

- Risco de “apartheid educacional digital”:
- Escolas ricas com IA de ponta, escolas pobres sem recursos básicos
- Estudantes com acesso a tutores de IA em casa vs. estudantes sem internet
- Concentração de desenvolvimento de IA educacional em países ricos
- Conteúdos de IA não adaptados a realidades locais.



Para Refletir!

Como garantir que IA na educação reduza, em vez de ampliar, desigualdades educacionais?

Para educadoras e educadores que atuam com Direitos Humanos, o letramento em IA (AI Literacy) organiza-se em quatro dimensões complementares:

- **Compreensão Conceitual:** envolve o conhecimento sobre algoritmos, machine learning e como esses sistemas aprendem a partir de dados, reconhecendo suas limitações técnicas.
- **Pensamento Crítico:** voltado a identificar vieses e discriminações, questionar a suposta neutralidade tecnológica e avaliar impactos concretos sobre a igualdade e a liberdade.
- **Competências Práticas:** abrangem o uso ético de ferramentas, a proteção da privacidade e a capacidade de desenvolver estratégias para ensinar sobre IA no contexto escolar.
- **Dimensão Ética e Social:** exige compreender os princípios de justiça e inclusão, participando de debates sobre regulação e promovendo o uso responsável da tecnologia.



Descrição: Criança usando óculos de realidade virtual em sala de aula, cercada por ícones de aprendizagem.
Fonte: Magnific.

As competências essenciais para educadores em Direitos Humanos começam pela compreensão conceitual, que envolve saber o que é inteligência artificial, o que são algoritmos e machine learning, como os sistemas de IA aprendem a partir de dados e quais são suas principais limitações.

Essa base é necessária para evitar explicações simplistas, identificar usos inadequados da tecnologia no contexto educacional e sustentar práticas pedagógicas alinhadas à formação crítica e cidadã.

A partir desse fundamento, entram o pensamento crítico, as competências práticas e a dimensão ética e social, que se articulam diretamente com a proteção e a promoção de direitos. Isso inclui identificar vieses e discriminações, questionar a suposta neutralidade da tecnologia, avaliar impactos concretos sobre Direitos Humanos e reconhecer interesses econômicos e políticos por trás de soluções tecnológicas, além de usar ferramentas de IA de forma ética, avaliar sua qualidade, proteger a privacidade e desenvolver estratégias para ensinar sobre IA.

Por fim, exige compreender princípios éticos aplicáveis, reconhecer efeitos desiguais em diferentes grupos, participar de debates sobre regulação e promover um uso responsável da IA, com foco em justiça, inclusão e responsabilização.



VÍDEO RECOMENDADO

“Inteligência Artificial na Educação: limites, Oportunidades e Desafios para educadores e estudantes” - Instituto Claro

Duração: 44 minutos.

[Clique aqui para acessar o vídeo!](#)

Ensinar sobre inteligência artificial na Educação em Direitos Humanos significa trabalhar a tecnologia como objeto de estudo, com objetivos claros de desmistificar seu funcionamento, desenvolver pensamento crítico, compreender impactos sociais e promover um uso ético.

Nessa abordagem, a IA é apresentada como uma construção sociotécnica, atravessada por escolhas humanas, interesses institucionais e efeitos concretos sobre igualdade, privacidade, liberdade e não discriminação, o que permite ao estudante enxergar a relação entre tecnologia, poder e direitos.

Para alcançar esses objetivos, metodologias ativas e contextualizadas funcionam melhor: análise de casos de discriminação algorítmica para discutir dilemas éticos, identificar direitos violados e propor soluções; experimentos com IA para comparar respostas de chatbots, identificar vieses e analisar reconhecimento facial; debates sobre regulação, vigilância, substituição de professores e responsabilidade por erros; produção de princípios éticos, checklists de direitos e campanhas em vídeos, podcasts e infográficos; e investigação com mapeamento do uso de IA na comunidade, entrevistas, análise de políticas de privacidade e estudo da legislação sobre IA.



Descrição: Crianças em sala de aula focadas em atividades de robótica e computação, em plano detalhado.

Fonte: Magnific.

PRINCÍPIOS ORIENTADORES:



Transparência: Sempre informar quando usar IA



Complementaridade: IA como apoio, não substituição



Privacidade: Proteger dados de estudantes



Inclusão: Garantir acessibilidade



Criticidade: Sempre questionar e avaliar



Autonomia: Desenvolver independência, não dependência



ESTRATÉGIA PEDAGÓGICA!

ATIVIDADE 1: “Desafio do Viés”

Objetivo: Identificar vieses em sistemas de IA

Procedimento: Apresente imagens de pessoas de diferentes raças, gêneros e idades. Use uma ferramenta de reconhecimento de emoções (ex: Microsoft Azure, Google Vision). Compare resultados.

Discuta: Há diferenças? Por quê? Que impactos isso pode ter?

ATIVIDADE 2: “Júri Simulado sobre IA”

Tema: “Sistemas de IA devem ser usados para decisões de justiça criminal?”

Papéis:

- Promotoria (a favor)
- Defesa (contra)
- Juízes (estudantes)
- Especialistas (direitos humanos, tecnologia, vítimas)

ATIVIDADE 3: “Criando Princípios Éticos”

Desafio: Sua escola vai adotar uma ferramenta de IA. Crie um documento de “Princípios Éticos para Uso de IA na Escola”.

Incluir:

- Valores fundamentais
- Direitos de estudantes
- Responsabilidades da escola
- Critérios de avaliação de ferramentas
- Mecanismos de contestação



ESTRATÉGIA PEDAGÓGICA!

ATIVIDADE 4: “Auditoria de Privacidade”

Tarefa: Analisar políticas de privacidade de aplicativos educacionais

- Perguntas:
- Que dados coletam?
- Como usam?
- Compartilham com terceiros?
- É possível excluir dados?
- Linguagem é clara?
- Cumpre LGPD?

ATIVIDADE 5: “Chatbot de Direitos Humanos”

Projeto: Criar um chatbot simples sobre direitos digitais usando plataforma no-code (ex: Chatfuel, ManyChat)

- Aprendizados:
- Como IA é treinada
- Importância de dados de qualidade
- Desafios de linguagem natural
- Limitações da IA

Considerações finais

Chegamos ao final de nossa jornada pelo universo da inteligência artificial e direitos humanos! Neste módulo, desmistificamos a inteligência artificial, compreendendo que não se trata de “mágica” nem de entidade autônoma, mas de sistemas criados por humanos, treinados com dados humanos, refletindo valores, escolhas e vieses humanos.

Exploramos princípios éticos fundamentais que devem orientar o desenvolvimento e uso de IA: transparência, accountability, justiça, privacidade, autonomia humana e supervisão. Esses princípios não são abstrações filosóficas – são necessidades urgentes para proteger direitos fundamentais.

Analizamos como vieses algorítmicos reproduzem e amplificam discriminações históricas, afetando desproporcionalmente grupos já marginalizados. Reconhecemos que a IA não é neutra – ela pode ser ferramenta de opressão ou de libertação, dependendo de como é desenvolvida, regulada e utilizada.

Discutimos os riscos da vigilância algorítmica – do reconhecimento facial em espaços públicos ao monitoramento de estudantes em escolas – reconhecendo que a normalização da vigilância constante representa ameaça à liberdade, privacidade e dignidade humana.

Conhecemos marcos regulatórios emergentes, especialmente o AI Act europeu (COMISSÃO EUROPEIA, 2021) e projetos de lei brasileiros, compreendendo que a regulação é essencial mas insuficiente – precisamos também de educação, conscientização e mobilização social.

Na segunda unidade, exploramos o potencial transformador da IA para promoção de direitos humanos: monitoramento de violações, democratização do acesso à justiça, combate ao tráfico humano, tradução e acessibilidade. A IA pode ser aliada poderosa quando orientada por valores humanistas.

Estudamos especificamente a IA na educação, reconhecendo potencialidades (personalização, inclusão, apoio pedagógico) mas também riscos graves (vigilância de estudantes, perda de autonomia docente, aprofundamento de desigualdades, violação de privacidade de crianças).

O letramento em IA é essencial para educadores em direitos humanos que precisam não apenas usá-la, mas compreendê-la criticamente, avaliá-la eticamente e ensinar sobre ela de forma responsável.

Finalmente, demonstramos algumas metodologias pedagógicas para ensinar sobre IA e usar IA na educação em direitos humanos, sempre orientadas por princípios de transparência, complementaridade, privacidade, inclusão, criticidade e autonomia.

Conexões com o Próximo Módulo

Os conhecimentos construídos aqui serão fundamentais para o Módulo 3, onde aprofundaremos questões de privacidade, proteção de dados e segurança digital.

Compreender IA é essencial para entender:

- Como nossos dados são coletados e analisados
- Que riscos enfrentamos em um mundo de vigilância digital
- Como proteger nossa privacidade e a de nossos estudantes
- Como combater desinformação amplificada por algoritmos
- Como educar para segurança e responsabilidade digital
- Convite à Ação Transformadora
- Como educadoras e educadores em direitos humanos, temos papel crucial na construção de um futuro em que a IA sirva à humanidade, não o contrário.

Ações concretas que você pode desenvolver:



Eduque-se continuamente sobre IA

– a tecnologia evolui rapidamente



Desenvolva letramento em IA

em si mesmo e em seus estudantes



Questione sistemas de IA

– exija transparência e accountability



Denuncie discriminações algorítmicas

quando identificá-las



Proteja privacidade

– sua e de seus estudantes



Participe de debates

sobre regulação de IA



Use IA de forma ética

– sempre com supervisão humana



Ensine sobre IA

– forme cidadãos críticos e conscientes



Promova diversidade em tecnologia

– incentive grupos sub-representados



Exija que instituições adotem princípios éticos de IA

Reflexão Final

A Inteligência Artificial não é inevitável em sua forma atual. Não precisamos aceitar sistemas opacos, discriminatórios, invasivos. Podemos e devemos exigir outra IA – transparente, justa, inclusiva, respeitosa de direitos humanos.

A IA que teremos amanhã depende das escolhas que fazemos hoje. Façamos escolhas corajosas, éticas e humanistas.

Até o próximo módulo!

Referências

ALGORITMOS da **desigualdade: como as ferramentas digitais reforçam a injustiça**. Vox, 2018. Disponível em: <https://link.ufms.br/DajlC>. Acesso em: 8 jan. 2026.

BRASIL. **Projeto de Lei nº 2.338/2023: dispõe sobre o uso da Inteligência Artificial**. Brasília, DF: Câmara dos Deputados, 2023. Disponível em: <https://link.ufms.br/7dl5w>. Acesso em: 8 jan. 2026.

BUOLAMWINI, Joy; GEBRU, Timnit. **Gender shades: intersectional accuracy disparities in commercial gender classification**. Proceedings of Machine Learning Research, [s. l.], v. 81, p. 1-15, 2018. Disponível em: <https://link.ufms.br/cTfRP>. Acesso em: 8 jan. 2026.

COMISSÃO EUROPEIA. **Proposta de regulamento sobre Inteligência Artificial (AI Act)**. Bruxelas: União Europeia, 2021. Disponível em: <https://link.ufms.br/1udbE>. Acesso em: 8 jan. 2026.

GRUPO DE ESPECIALISTAS DE ALTO NÍVEL SOBRE IA DA COMISSÃO EUROPEIA. **Diretrizes éticas para uma IA de confiança**. Bruxelas: Comissão Europeia, 2019. Disponível em: <https://link.ufms.br/7Bw5X>. Acesso em: 8 jan. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA (UNESCO). **Recomendação sobre a ética da Inteligência Artificial**. Paris: UNESCO, 2021. Disponível em: <https://link.ufms.br/j78a3>. Acesso em: 8 jan. 2026.

REDE DE PESQUISA SOLIDÁRIA. **Inteligência artificial e desigualdades no Brasil: mapeamento de riscos e oportunidades**. Rio de Janeiro: Rede de Pesquisa Solidária, 2022. Disponível em: <https://redepesquisasolidaria.org/>. Acesso em: 8 jan. 2026.

SILVA, Tarcízio. **Racismo algorítmico: inteligência artificial e discriminação nas redes digitais**. São Paulo: Edições Sesc, 2022. Disponível em: <https://www.sescsp.org.br/racismoalgoritmico/>. Acesso em: 8 jan. 2026.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Rio de Janeiro: Intrínseca, 2021.

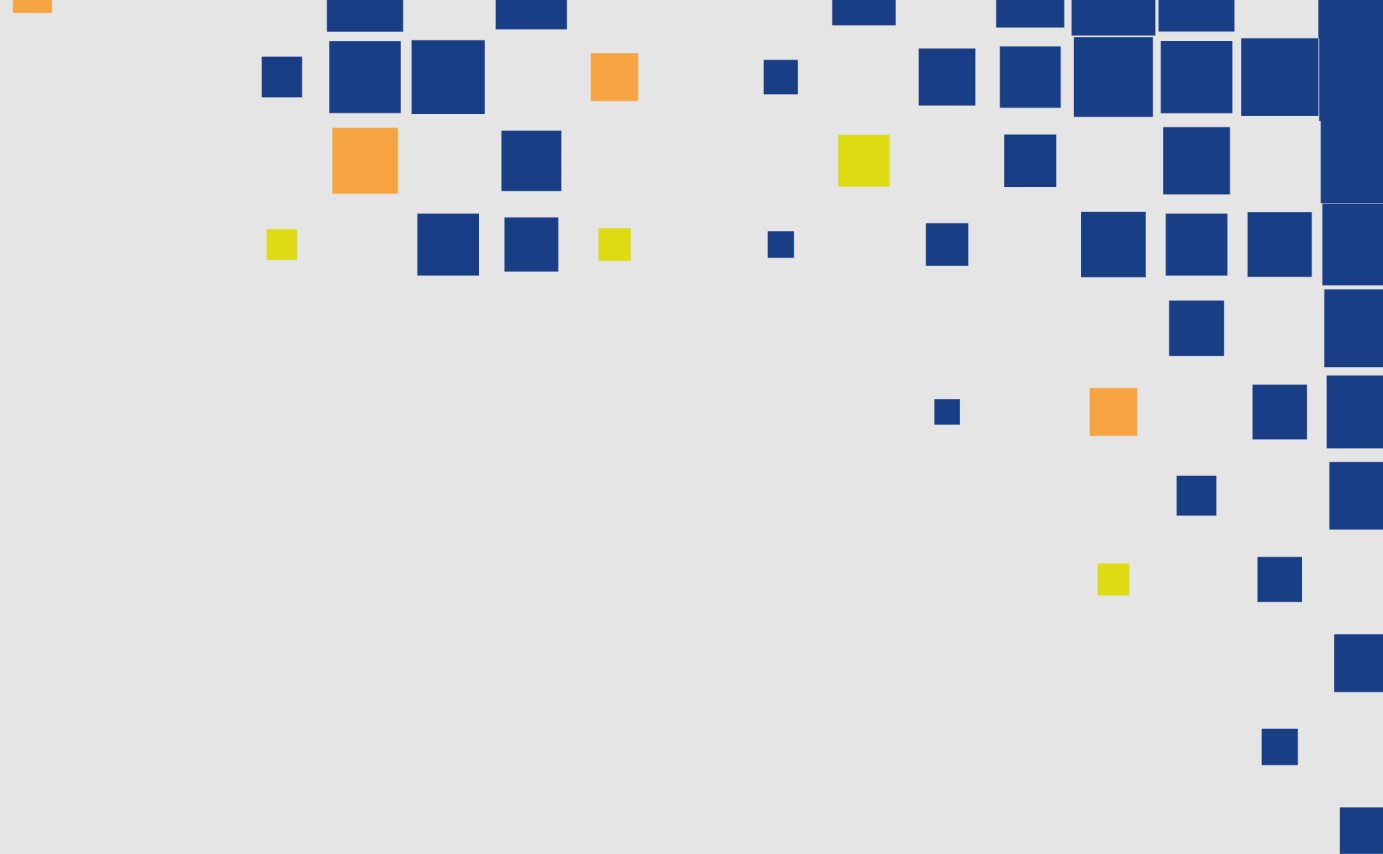
Vídeos recomendados (recursos complementares)

KANTAYYA, Shalini. **CODED Bias**. Netflix, 2020. Documentário (90 min). Disponível em: <https://www.netflix.com/title/81328723>.

ORLOWSKI, Jeff. **O dilema das redes (The Social Dilemma)**. Netflix, 2020. Documentário (94 min). Disponível em: <https://www.netflix.com/title/81254224>.

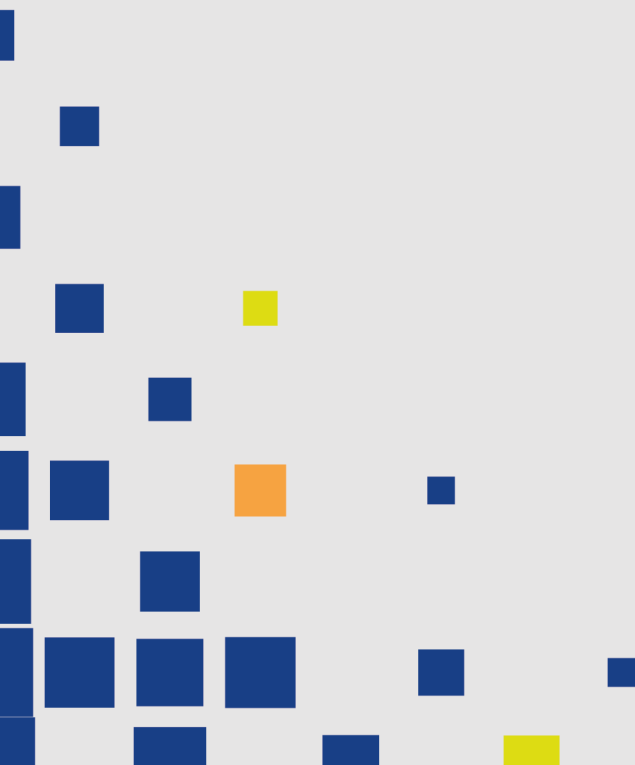
KOHS, Greg. **ALPHAGO**. YouTube, 2017. Documentário (90 min). Disponível em: <https://www.youtube.com/watch?v=WXuK6gekU1Y>.

INTELIGÊNCIA Artificial: uma visão brasileira. **Canal USP**, 2022. Série de vídeos. Disponível em: <https://www.youtube.com/playlist?list=PLAudUnJeNg4vWJhSvV6FpeFJ1YL4FQVJ>.



Módulo 3

Segurança Digital, Privacidade e Proteção de Dados



Apresentação

Bem-vinda(o) ao terceiro e último módulo de nossa disciplina!

Imagine estas situações: uma professora descobre que fotos íntimas suas foram vazadas online por um ex-parceiro. Um estudante tem sua conta de redes sociais invadida e usada para espalhar fake news. Uma escola sofre um ataque de ransomware e perde todos os dados dos estudantes. Milhões de brasileiros têm CPF, endereço e dados bancários expostos em vazamentos massivos de empresas.

Essas situações, infelizmente, são cada vez mais comuns. Vivemos em uma era de vulnerabilidade digital permanente, onde nossa privacidade, segurança e até nossa integridade física podem ser ameaçadas através do ambiente digital.

Ao mesmo tempo, enfrentamos uma epidemia de desinformação que ameaça a democracia, a saúde pública e os direitos humanos. Fake news se espalham mais rápido que a verdade, algoritmos amplificam polarização, e discursos de ódio encontram terreno fértil nas redes sociais, vitimando especialmente grupos vulneráveis.

Como educadoras e educadores em direitos humanos, precisamos compreender profundamente essas ameaças e, mais importante, saber como nos proteger e proteger nossos estudantes. Privacidade não é luxo – é direito fundamental. Segurança digital não é paranoia – é necessidade. Letramento midiático não é opcional – é urgente.

Neste módulo final, vamos mergulhar em três dimensões interconectadas:



Privacidade e proteção de dados como direitos humanos fundamentais



Cibersegurança como prática de autocuidado e proteção coletiva



Combate à desinformação e ao discurso de ódio como defesa da democracia e dos direitos humanos

Você aprenderá não apenas conceitos teóricos, mas estratégias práticas que poderá aplicar imediatamente em sua vida e em sua prática educativa.

Objetivos de Aprendizagem

Ao final deste módulo, você será capaz de:

- Compreender a privacidade como direito humano fundamental e sua importância na era digital;
- Aplicar os princípios e direitos da LGPD no contexto educacional, especialmente em relação a dados de crianças e adolescentes;
- Implementar práticas de cibersegurança para proteger-se e proteger estudantes de ameaças digitais;
- Identificar e combater desinformação, fake news e discursos de ódio online;
- Desenvolver estratégias pedagógicas para educar sobre privacidade, segurança e letramento midiático;
- Criar ambientes educacionais digitalmente seguros e respeitosos de direitos;
- Empoderar estudantes para que sejam cidadãos digitais críticos, seguros e responsáveis.

Estrutura do Módulo

Este módulo está organizado em duas unidades complementares:

Unidade 1: Privacidade e Proteção de Dados como Direitos Humanos

Exploraremos a privacidade na era digital, a LGPD e seus impactos na educação, a proteção de dados de crianças e adolescentes, e estratégias pedagógicas para educar sobre proteção de dados.

Unidade 2: Cibersegurança, Desinformação e Combate ao Discurso de Ódio

Aprenderemos práticas de cibersegurança, como identificar e combater desinformação, desenvolver letramento midiático, enfrentar o discurso de ódio online e criar projetos educativos integrados.

Prepare-se para uma jornada prática e transformadora que o(a) capacitará a navegar com segurança e consciência crítica no mundo digital!

Unidade 1

Privacidade como Direito Humano: Educação e Proteção de Dados na Era Digital



Descrição: Estudantes concentrados usando tablets e notebooks em uma biblioteca escolar iluminada. **Fonte:** Magnific.

O conceito de privacidade mudou com as transformações sociais e tecnológicas: no século XIX, ganhou forma como o “direito de ser deixado em paz”, formulado por Samuel Warren e Louis Brandeis em 1890, no século XX, passou a enfatizar a proteção contra intrusões físicas, como no domicílio e na correspondência, e no século XXI, tornou-se inseparável da proteção de dados pessoais, do controle sobre informações e da privacidade digital.

Essa trajetória já encontra amparo na Declaração Universal dos Direitos Humanos, que no Artigo 12 afirma que ninguém deve sofrer interferências arbitrárias na vida privada, na família, no lar ou na correspondência, nem ataques à honra e reputação, assegurando proteção legal contra tais violações.

Na era da vigilância digital, a privacidade enfrenta pressões inéditas, inseridas no que Shoshana Zuboff denomina “capitalismo de vigilância”, um modelo econômico baseado em coletar e transformar dados pessoais em valor. Em termos práticos, empresas capturam massivamente informações sobre navegação, localização, compras e comunicações, analisam esses registros para construir perfis detalhados, usam esses perfis para prever e influenciar comportamentos e, por fim, monetizam tais previsões por meio de publicidade direcionada e outros mercados de dados, o que amplia riscos de manipulação, assimetrias de poder e violações de direitos.

A assimetria de poder entre indivíduos e grandes corporações tecnológicas é significativa. Enquanto empresas possuem recursos técnicos e legais sofisticados para coletar e analisar dados, indivíduos frequentemente carecem de conhecimento, ferramentas e poder de barganha para proteger sua privacidade efetivamente. Esta assimetria torna essencial a regulação legal e a educação digital.





Descrição: Shoshana Zuboff, mulher de cabelos volumosos e óculos, segurando microfone com jaqueta bordada em evento. **Fonte:** Wikimedia.

SHOSHANA ZUBOFF

Autora do livro “The Age of Surveillance Capitalism: The Struggle for a Human Future on Power’s New Frontier”. Traduzido por George Schlesinger. Rio de Janeiro: Editora Intrínseca, 2021.

[Clique aqui para acessar o vídeo!](#)

O Dilema da Privacidade

Quando falamos de privacidade muitas questões podem ser levantadas. A privacidade importa porque é ela que sustenta dimensões centrais da vida em sociedade, e não porque alguém “tem algo a esconder”. Ela protege a autonomia, permitindo tomar decisões livres sem manipulação, a dignidade, ao garantir controle sobre informações pessoais, e a segurança, reduzindo riscos de fraude, perseguição e discriminação.

Também é condição para a liberdade, já que possibilita se expressar, explorar ideias e aprender com erros sem vigilância constante, e para a democracia, pois espaços privados são essenciais para dissidência, organização política e participação cidadã sem intimidação.

Na esfera digital, essa proteção é pressionada por ameaças recorrentes e complementares: a vigilância corporativa, marcada por coleta massiva de dados, perfilamento comportamental e publicidade invasiva, a vigilância governamental, com monitoramento de comunicações, reconhecimento facial em espaços públicos e coleta de metadados, os vazamentos de dados, que expõem informações por falhas de segurança, alimentam mercados ilegais e facilitam uso indevido por terceiros, e as violências digitais, como exposição não consentida de imagens íntimas, doxxing e stalking digital, que transformam dados e rastros online em instrumentos de coerção e dano.

Reconhecendo os riscos crescentes para a privacidade digital, jurisdições ao redor do mundo têm desenvolvido marcos regulatórios abrangentes para proteção de dados pessoais.

O Regulamento Geral de Proteção de Dados (GDPR)

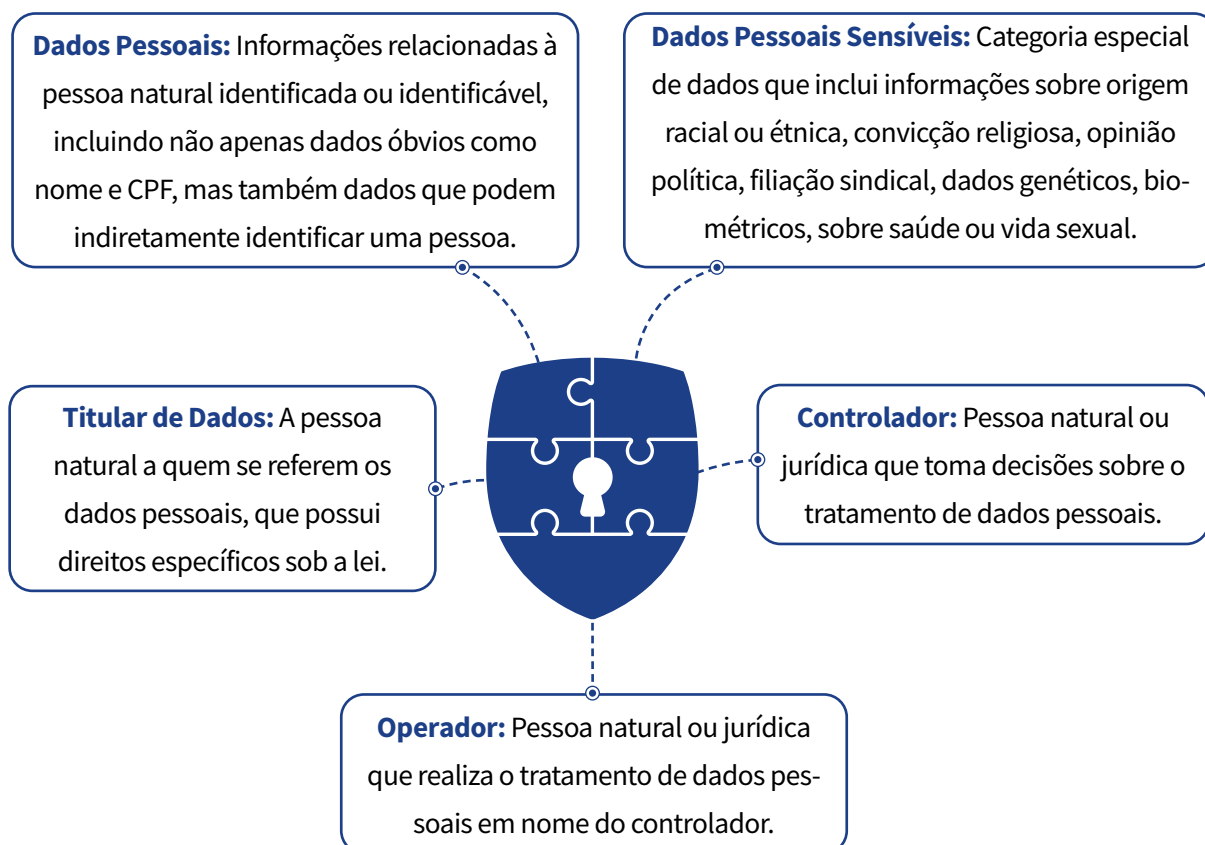
O [GDPR europeu](#), implementado em 2018, estabeleceu um novo padrão global para proteção de dados pessoais. Esta regulação introduziu princípios fundamentais como consentimento explícito, minimização de dados, transparência e accountability, além de direitos robustos para indivíduos, incluindo o direito de acesso, retificação, portabilidade e esquecimento.

O GDPR também estabeleceu penalidades significativas para violações, com multas que podem chegar a 4% do faturamento global anual de uma empresa. Esta abordagem de “regulação com dentes” influenciou legislações de proteção de dados ao redor do mundo e forçou empresas globais a repensar suas práticas de tratamento de dados.

A Lei Geral de Proteção de Dados (LGPD) Brasileira

O Brasil seguiu o exemplo europeu com a aprovação da LGPD em 2018, que entrou em vigor em 2020. A LGPD estabelece princípios similares ao GDPR, adaptados ao contexto jurídico e social brasileiro. A lei aplica-se a qualquer operação de tratamento de dados pessoais realizada no território brasileiro ou que envolva dados de indivíduos localizados no Brasil.

Conceitos importantes introduzidos pela LGPD



Princípios Fundamentais da Proteção de Dados

A LGPD estabelece dez princípios fundamentais que devem orientar todo tratamento de dados pessoais:

1

Finalidade

Dados devem ser tratados para propósitos legítimos, específicos, explícitos e informados ao titular.

2

Adequação

O tratamento deve ser compatível com as finalidades informadas ao titular.

3

Necessidade

Limitação do tratamento ao mínimo necessário para a realização de suas finalidades.

4

Livre Acesso

Garantia aos titulares de consulta facilitada e gratuita sobre a forma e duração do tratamento.

5

Qualidade dos Dados

Garantia de exatidão, clareza, relevância e atualização dos dados.

6

Transparência

Informações claras, precisas e facilmente acessíveis sobre a realização do tratamento.

7

Segurança

Medidas técnicas e administrativas para proteger dados de acessos não autorizados.

8

Prevenção

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados.

9

Não Discriminação

Impossibilidade de realizar tratamento para fins discriminatórios ilícitos ou abusivos.

10

Responsabilização e Prestação de Contas

Demonstração da adoção de medidas eficazes e capazes de comprovar a observância das normas.

Direitos dos Titulares de Dados

A LGPD estabelece direitos robustos para os titulares de dados, empoderando indivíduos com controle sobre suas informações pessoais:



Descrição: Ilustração de martelo da justiça batendo no botão Enter, com fundo branco e estética digital.

Fonte: gerada pelo Chat GPT.

■ **Direito de Confirmação e Acesso:** Obter confirmação sobre a existência de tratamento e acessar seus dados pessoais.

■ **Direito de Retificação:** Solicitar correção de dados incompletos, inexatos ou desatualizados.

■ **Direito de Anonimização, Bloqueio ou Eliminação:** Solicitar que dados desnecessários, excessivos ou tratados em desconformidade sejam anonimizados, bloqueados ou eliminados.

■ **Direito de Portabilidade:** Solicitar a portabilidade de dados a outro fornecedor de serviço ou produto.

■ **Direito de Informação:** Obter informações sobre entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.

■ **Direito de Oposição:** Opor-se ao tratamento realizado com fundamento em legítimo interesse.

■ **Direito de Revisão:** Solicitar revisão de decisões automatizadas que afetem seus interesses.

Desafios da Implementação da LGPD

A implementação efetiva da LGPD enfrenta desafios significativos que refletem a complexidade da proteção de dados na era digital:

■ **Conscientização e Educação:** Muitas organizações e indivíduos ainda não compreendem completamente suas obrigações e direitos sob a LGPD. É necessário investimento contínuo em educação e capacitação.

■ **Recursos Técnicos e Financeiros:** Implementar medidas adequadas de proteção de dados requer investimentos em tecnologia, processos e pessoal qualificado, o que pode ser desafiador para organizações menores.

■ **Complexidade Técnica:** A natureza técnica da proteção de dados pode tornar difícil para não especialistas compreender e implementar medidas adequadas.

■ **Enforcement:** A Autoridade Nacional de Proteção de Dados (ANPD) enfrenta o desafio de fiscalizar milhares de organizações com recursos limitados.

Privacidade by Design

O conceito de “Privacy by Design”(Privacidade desde a Concepção), desenvolvido por Ann Cavoukian, propõe que a proteção da privacidade deve ser incorporada desde o início do desenvolvimento de sistemas e processos. Pesquisas recentes, como as de Lopes (2024), demonstram que esta abordagem é hoje o padrão ouro para a conformidade com a LGPD, permitindo que a proteção de dados não seja apenas uma camada burocrática, mas uma característica intrínseca da arquitetura tecnológica.

Os sete princípios fundamentais do Privacy by Design são:

1. Proativo, não Reativo: Antecipar e prevenir invasões de privacidade antes que ocorram.
2. Privacidade como Padrão: Garantir máxima proteção de privacidade sem exigir ação do indivíduo.
3. Privacidade Incorporada no Design: Incorporar considerações de privacidade desde o início do design de sistemas.
4. Funcionalidade Completa: Acomodar todos os interesses legítimos sem compromissos desnecessários.

5. Segurança de Ponta a Ponta: Garantir que dados sejam seguros durante todo seu ciclo de vida.
6. Visibilidade e Transparência: Garantir que práticas de dados sejam visíveis e verificáveis.
7. Respeito pela Privacidade do Usuário: Manter os interesses do usuário como prioridade máxima.

Tecnologias de Preservação da Privacidade

O desenvolvimento de tecnologias que preservam a privacidade (Privacy-Preserving Technologies - PPTs) é essencial para equilibrar os benefícios da análise de dados com a proteção da privacidade individual.



Criptografia

Técnicas criptográficas podem proteger dados em trânsito e em repouso, garantindo que apenas partes autorizadas possam acessar informações sensíveis.



Anonimização e Pseudonimização

Técnicas para remover ou mascarar identificadores pessoais, permitindo análise de dados sem comprometer a privacidade individual.



Computação Segura Multipartidária

Permite que múltiplas partes computem funções sobre seus dados privados sem revelar os dados uns aos outros.



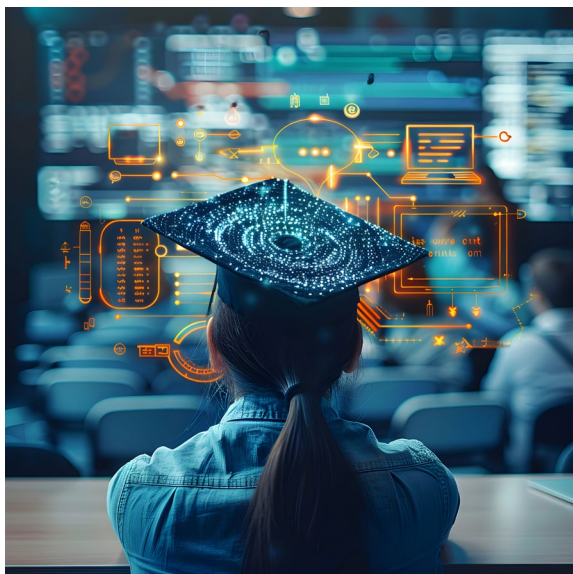
Aprendizado Federado

Permite treinar modelos de machine learning sem centralizar dados, mantendo informações pessoais nos dispositivos dos usuários.



Privacidade Diferencial

Técnica matemática que adiciona ruído controlado aos dados para proteger a privacidade individual enquanto preserva utilidade estatística.



Descrição: Estudante de costas com capelo brilhante olhando para telas virtuais e gráficos de dados. **Fonte:** Magnific.

Olhando para os dados educacionais!

Dados educacionais são especialmente sensíveis porque escolas e universidades lidam com informações que revelam muito mais do que identificação básica. Além de nome, CPF, endereço e contatos, o cotidiano escolar produz dados sobre desempenho, frequência, comportamento, dificuldades de aprendizagem e avaliações psicopedagógicas, que podem impactar oportunidades e gerar estigmas.

Soma-se a isso o tratamento de dados sensíveis, como saúde, deficiência, origem racial e étnica associada a políticas afirmativas, e situação socioeconômica vinculada a programas de apoio, além de dados biométricos, como impressão digital, voz e reconhecimento facial, cujo uso indevido pode produzir riscos graves e duradouros.

Por isso, a LGPD impõe proteção reforçada para crianças e adolescentes: como regra geral, o tratamento deve ocorrer no melhor interesse do menor e depende de consentimento específico de pelo menos um dos pais ou responsável legal. Há exceções em situações como contato com pais ou responsáveis, medidas de proteção da criança e cumprimento de obrigação legal, mas existem vedações importantes, como exigir dados além do necessário para permitir a participação em jogos ou aplicações, e realizar contato direto com a criança sem intermediação dos pais, salvo hipóteses excepcionais previstas em lei.



Para Refletir!

A proteção da privacidade na era digital não é apenas uma questão técnica ou legal, mas fundamentalmente uma questão sobre que tipo de sociedade queremos construir. As escolhas que fazemos sobre como coletar, usar e proteger dados pessoais refletem nossos valores sobre autonomia individual, poder corporativo e responsabilidade social.

Educação para a privacidade digital?

Educação para privacidade digital é essencial porque empodera pessoas a compreenderem como seus dados circulam, e a tomarem decisões informadas em ambientes conectados. Quando a escola e a universidade tratam a privacidade como tema formativo, elas fortalecem autonomia, segurança e cidadania, ajudando estudantes a reconhecerem práticas de coleta e uso de dados, e a exigirem transparência e responsabilidade de plataformas e serviços digitais.



Descrição: Mulher com óculos tocando em tela virtual futurista de segurança digital e proteção de dados.

Fonte: Magnific.

Programas de educação digital voltados à privacidade devem incluir, de modo prático e contextualizado, consciência sobre coleta de dados, para entender como, quando e por quem dados pessoais são capturados, leitura de políticas de privacidade, para desenvolver habilidade de interpretar termos, finalidades e riscos, configurações de privacidade, para ajustar permissões em dispositivos e aplicativos, reconhecimento de riscos, para identificar situações que expõem dados e aumentam vulnerabilidades, e ferramentas de proteção, com conhecimento de recursos e técnicas que reduzem rastreamento, vazamentos e usos indevidos de informações online.

Responsabilidades das Instituições Educacionais

Escolas e universidades devem:



Mapear dados

Identificar quais dados coletam e como tratam



Definir bases legais

Justificar por que coletam cada dado



Obter consentimento

Quando necessário, de forma clara e específica



Garantir segurança

Proteger dados contra vazamentos



Treinar equipe

Educar funcionários sobre LGPD



Elaborar políticas

Política de privacidade, termos de uso



Designar responsável

Encarregado de proteção de dados (DPO)



Atender direitos

Responder solicitações de titulares



Notificar incidentes

Comunicar ANPD - (Autoridade Nacional de Proteção de Dados) e titulares em caso de vazamento

Plataformas Educacionais e LGPD

Perguntas a fazer antes de adotar uma plataforma:



Onde os dados são armazenados?



A empresa cumpre a LGPD?



Dados são compartilhados com terceiros?



Como solicitar exclusão de dados?



É possível exportar dados (portabilidade)?



Crianças estão protegidas?



Há criptografia?



Como notificam vazamentos?



A LGPD transparência, segurança e respeito aos direitos das pessoas.

Educação e proteção de dados caminham juntas!



Você sabia?

A ANPD (Autoridade Nacional de Proteção de Dados) é o órgão do governo federal brasileiro responsável por implementar, fiscalizar e zelar pela Lei Geral de Proteção de Dados (LGPD) no país, com o objetivo de proteger os dados pessoais dos cidadãos, aplicando sanções em caso de descumprimento e educando sobre o tema. Ela atua com autonomia para criar diretrizes, receber reclamações e promover o conhecimento sobre privacidade e proteção de dados no Brasil.

[Clique aqui para acessar a ANPD!](#)

Unidade 2

Educação para a Cibersegurança e o Combate à Desinformação e ao Discurso de Ódio



Descrição: Mulher utilizando notebook em casa, com tela exibindo sistema de segurança e acesso autorizado.

Fonte: Magnific.

A segurança digital emergiu como uma dimensão fundamental dos direitos humanos na era digital. Assim como temos direito à segurança física, também devemos ter direito à segurança no ambiente digital. A cibersegurança não é apenas sobre proteger sistemas tecnológicos, mas sobre proteger pessoas, suas informações, sua privacidade e sua capacidade de participar seguramente da sociedade digital.

A vulnerabilidade digital pode ter consequências devastadoras para indivíduos e comunidades. Ataques cibernéticos podem resultar em roubo de identidade, fraude financeira, chantagem, assédio e até mesmo ameaças à segurança física. Para grupos vulneráveis - incluindo mulheres, minorias étnicas, ativistas de direitos humanos e jornalistas - os riscos digitais podem ser particularmente severos.

Cibersegurança é o conjunto de práticas, tecnologias e processos voltados a proteger sistemas, redes, dispositivos e dados contra ataques, danos e acessos não autorizados. Ela não se limita a especialistas, porque boa parte dos incidentes acontece por falhas cotidianas, por isso a higiene digital básica é uma responsabilidade compartilhada, especialmente em ambientes educacionais, onde circulam dados pessoais e acadêmicos sensíveis.

Entre as principais ameaças digitais, destacam-se o **phishing**, que usa e-mails e mensagens falsas com tom de urgência e links para sites clonados. Essa ameaça pode ser percebida por erros de escrita, remetentes suspeitos e URLs estranhas.

Esse tipo de ameaça pode criptografar arquivos e exigir resgate, sem garantir a recuperação dos dados. A prevenção envolve downloads seguros, antivírus atualizado, backups regulares e cautela com anexos. Outra ameaça é a engenharia social, que manipula psicologicamente as pessoas ao explorar urgência, autoridade e confiança. Nesse caso, é importante verificar identidades e recusar pedidos incomuns.

A proteção envolve não clicar por impulso, conferir endereços, usar canais oficiais e ativar a autenticação de dois fatores. Também se destaca o malware, como vírus, trojans, spyware e ransomware.





Descrição: Pessoa de costas em frente a monitores com códigos, em ambiente escuro de segurança cibernética. **Fonte:** Magnific.

Há ainda os ataques de força bruta, que tentam adivinhar senhas automaticamente. Eles podem ser mitigados com senhas fortes, autenticação de dois fatores e bloqueio após tentativas falhas. Por fim, o roubo de identidade frequentemente está ligado a vazamentos, phishing e perda de documentos. Esse risco pode ser reduzido com monitoramento de CPF, compartilhamento mínimo de documentos e proteção ativa de dados pessoais.

Em ambientes educacionais, cibersegurança é parte da garantia do direito à educação com proteção à privacidade, à integridade e à segurança de estudantes e trabalhadores. Isso exige uma governança clara, na qual a instituição assume deveres estruturais e organizacionais, enquanto educadores e estudantes incorporam práticas cotidianas que reduzem riscos e fortalecem uma cultura de cuidado com dados e sistemas.

A educação para a cibersegurança é, portanto, uma questão de justiça social e direitos humanos. Todos os indivíduos, independentemente de sua formação técnica ou recursos econômicos, devem ter acesso ao conhecimento e ferramentas necessárias para se proteger no ambiente digital.

Do lado institucional, as responsabilidades incluem manter infraestrutura segura, com firewall, antivírus e criptografia, definir políticas claras de uso aceitável, treinar equipes, proteger dados de estudantes, estabelecer plano de resposta a incidentes, realizar backup regular, e aplicar controle de acesso.

Para educadores, é essencial proteger credenciais, não compartilhar senhas, usar apenas dispositivos e redes seguras, orientar estudantes sobre segurança, reportar incidentes imediatamente e seguir as políticas institucionais.

Já com os estudantes, a formação deve começar cedo, ensinando práticas básicas, ampliando consciência sobre riscos, promovendo cultura de segurança e incentivando o reporte de situações suspeitas.

Garantir a cibersegurança também implica a qualidade e propagação de informações. Assim, a desinformação - informação falsa ou enganosa deliberadamente criada e disseminada - representa uma das maiores ameaças à democracia e aos direitos humanos na era digital. Diferentemente da simples informação incorreta (misinformação), a desinformação é caracterizada pela intenção maliciosa de enganar.

A desinformação pode ter consequências devastadoras:

- Minar confiança em instituições democráticas
- Influenciar eleições e processos políticos
- Promover discriminação e violência contra grupos minoritários
- Prejudicar saúde pública através de informações médicas falsas
- Causar pânico e instabilidade social

Mecanismos de Propagação da Desinformação

- 1. Algoritmos de Recomendação:** Plataformas digitais utilizam algoritmos que podem amplificar conteúdo sensacionalista ou polarizador, incluindo desinformação, porque tal conteúdo gera maior engajamento.
- 2. Câmaras de Eco:** Ambientes digitais onde indivíduos são expostos apenas a informações que confirmam suas crenças existentes, tornando-os mais suscetíveis a desinformação alinhada com seus preconceitos.
- 3. Bots e Contas Falsas:** Contas automatizadas ou falsas utilizadas para amplificar artificialmente a disseminação de desinformação.
- 4. Deepfakes:** Tecnologias de IA utilizadas para criar vídeos ou áudios falsos convincentes de pessoas reais, representando uma nova fronteira na desinformação.

Estratégias de Combate à Desinformação

O letramento informacional - a capacidade de encontrar, avaliar e utilizar informações de forma crítica - é fundamental para combater a desinformação.

- **Verificação de Fontes:** Ensinar indivíduos a verificar a credibilidade de fontes de informação, incluindo verificação de autoria, data de publicação e reputação da fonte.
- **Checagem de Fatos:** Utilizar serviços de fact-checking e ensinar técnicas básicas de verificação de informações.
- **Pensamento Crítico:** Desenvolver habilidades de análise crítica que permitam questionar informações e identificar possíveis vieses ou motivações.
- **Diversidade de Fontes:** Incentivar o consumo de informações de múltiplas fontes com diferentes perspectivas.



ESTRATÉGIA PEDAGÓGICA!

ATIVIDADE 1: “Detetive de Notícias”

Objetivo: Desenvolver habilidades de verificação

Procedimento: Apresente 5 notícias (3 verdadeiras, 2 falsas); Estudantes aplicam checklist de verificação; Identificam verdadeiras e falsas; Justificam suas conclusões e Discussão coletiva

ATIVIDADE 2: “Criando Fake News”

Objetivo: Compreender técnicas de manipulação

Procedimento: Grupos criam notícia falsa (sem divulgar!); Usam técnicas de desinformação; Apresentam para turma; Turma tenta identificar como é falsa.

Discussão: como criaram? Como poderiam ser mais convincentes? Por que é antiético?

ATIVIDADE 3: “Fact-Checking na Prática”

Objetivo: Aplicar verificação em contexto real

Procedimento:

- Estudantes coletam conteúdos suspeitos circulando online
- Aplicam metodologia de fact-checking
- Documentam processo de verificação
- Criam posts desmentindo ou confirmando
- Compartilham resultados

ATIVIDADE 4: “Linha do Tempo da Desinformação”

Objetivo: Compreender impactos históricos

Procedimento:

- Pesquisar casos históricos de desinformação
- Analisar consequências
- Criar linha do tempo visual
- Discutir padrões e lições

Discurso de Ódio Digital

O discurso de ódio digital constitui uma ameaça relevante aos direitos humanos, sobretudo para grupos historicamente marginalizados, porque o ambiente online combina alcance elevado, velocidade de circulação e barreiras reduzidas para a agressão. A dinâmica das plataformas pode ampliar a exposição das vítimas e intensificar a disseminação de mensagens discriminatórias, tornando o dano mais amplo e mais difícil de reparar, inclusive quando o conteúdo é replicado, arquivado e redistribuído.



Descrição: Jovem preocupada diante de notebook, enquanto duas pessoas conversam ao fundo em ambiente escolar.

Fonte: Magnific.

Entre suas características centrais estão o anonimato, que pode encorajar condutas que muitas pessoas não assumiriam presencialmente, a amplificação, pela capacidade de viralização e recomendação algorítmica para grandes audiências, a persistência, já que conteúdos podem permanecer disponíveis por tempo indeterminado, e a coordenação, que facilita campanhas organizadas de assédio. Seus impactos incluem trauma psicológico, autocensura e retirada de espaços digitais, normalização de atitudes discriminatórias, risco de incitação à violência fora da internet e erosão da coesão social.

No ambiente online, o discurso de ódio tende a ganhar potência por características próprias das plataformas, como amplificação, com alcance massivo, rapidez e efeito viral, anonimato, que aumenta a sensação de impunidade e desinibição, permanência, já que o conteúdo é difícil de apagar totalmente e pode gerar trauma duradouro, e organização, com grupos coordenando ataques e campanhas de assédio.



Descrição: Ilustração de jovem alvo de cyberbullying, com ofensas e gestos hostis saindo de um celular.
Fonte: Magnific.

A liberdade de expressão não é um direito absoluto, e encontra limites quando passa a violar direitos de outras pessoas e grupos, especialmente quando envolve incitação à violência, ameaças, difamação e discursos que desumanizam coletividades. Um critério pedagógico útil para perceber a gravidade é testar a frase substituindo o grupo-alvo por outro, se a formulação soar absurda ou claramente inaceitável, há forte indicação de discurso de ódio, porque o conteúdo costuma operar por desumanização, estigmatização e incentivo à exclusão.

Os alvos preferenciais incluem mulheres, que sofrem ameaças de violência sexual e exposição não consentida; pessoas negras, atingidas por racismo explícito e velado, injúria racial e desumanização; pessoas LGBTQIA+, com manifestações de LGBTfobia, patologização e incitação à violência; pessoas com deficiência, afetadas pelo capacitismo, pela ridicularização e pela negação de direitos; migrantes e refugiados, expostos à xenofobia, à criminalização e à desumanização; e grupos religiosos, que podem ser alvo de intolerância, associação indevida ao terrorismo e desrespeito a símbolos. Essas violências geram impactos individuais, como trauma, ansiedade, depressão, autocensura e abandono de espaços digitais, além de impactos coletivos, como silenciamento, normalização da intolerância, polarização social e aumento de violências offline.



Fonte: Gerado por ChatGPT

Reflexão Final

A segurança digital não é apenas uma questão técnica, mas uma questão de justiça social e direitos humanos. Nossa capacidade de participar plenamente da sociedade digital depende de nossa capacidade de fazê-lo com segurança. Isso requer não apenas ferramentas e conhecimento técnico, mas também valores compartilhados de respeito, dignidade e inclusão.

Considerações finais

Chegamos ao final de nossa jornada pela disciplina Direitos Humanos, Tecnologias e Inteligência Artificial!

Neste terceiro módulo, exploramos três dimensões fundamentais e interconectadas da vida digital contemporânea.

Compreendemos que privacidade é direito humano fundamental, não privilégio de quem “tem algo a esconder”. Na era do capitalismo de vigilância, onde nossos dados são constantemente coletados, analisados e monetizados, defender a privacidade é defender autonomia, dignidade e liberdade.

Estudamos a Lei Geral de Proteção de Dados (LGPD), reconhecendo-a como marco civilizatório que estabelece direitos dos titulares e responsabilidades de quem trata dados. Aprendemos que crianças e adolescentes merecem proteção especial, e que instituições educacionais têm responsabilidades específicas no tratamento de dados sensíveis de estudantes.

O letramento em IA é essencial para educadores em direitos humanos que precisam não apenas usá-la, mas compreendê-la criticamente, avaliá-la eticamente e ensinar sobre ela de forma responsável.

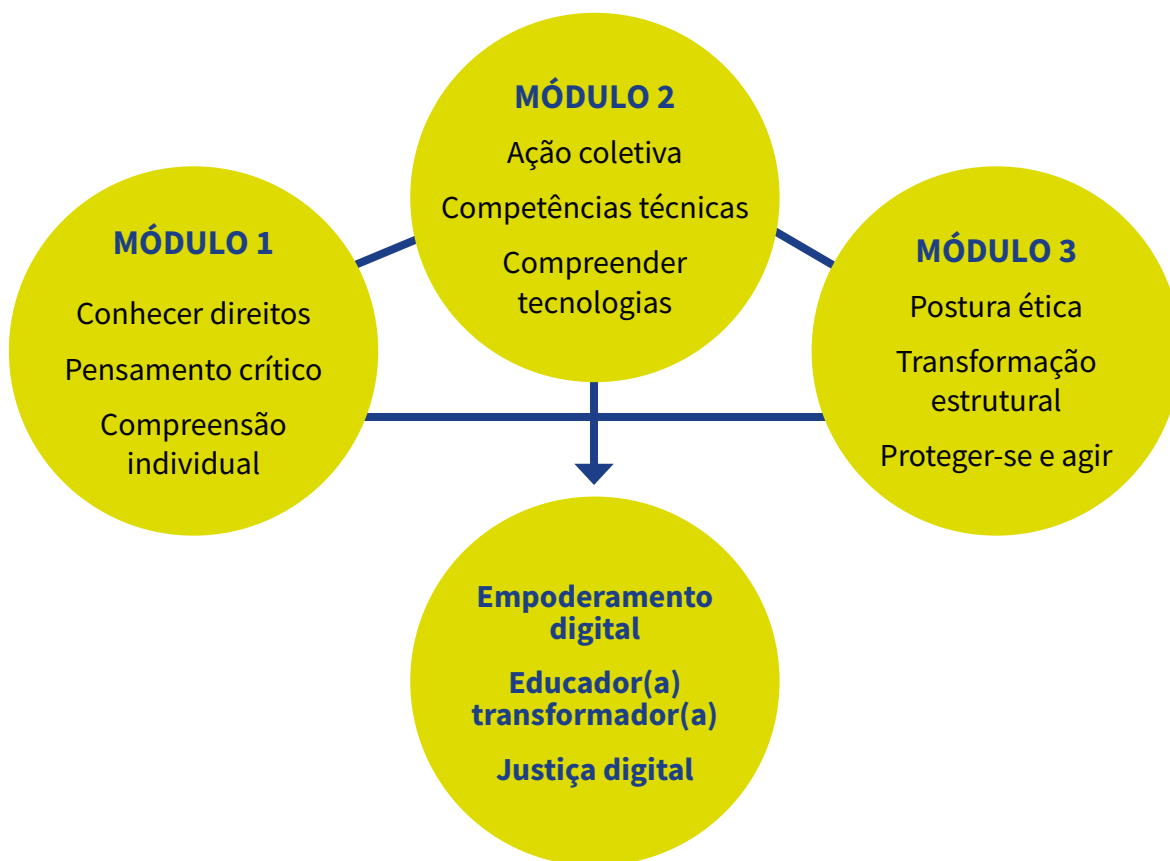
Aprendemos a identificar ameaças (phishing, malware, engenharia social), implementar práticas de higiene digital (senhas fortes, 2FA, backup, atualizações) e proteger-nos e proteger nossos estudantes de violências digitais.

Enfrentamos o desafio urgente da desinformação, reconhecendo que as fake news não são fenômeno novo, mas ganharam escala e velocidade sem precedentes na era digital. Desenvolvemos competências de letramento midiático e informacional, aprendendo metodologias de verificação e fact-checking que nos capacitam a navegar criticamente no mar de informações (e desinformações) que nos cerca.

Finalmente, confrontamos o discurso de ódio online, reconhecendo-o como uma ameaça grave aos direitos humanos e à democracia. Aprendemos a identificá-lo, compreender seus impactos devastadores em grupos vulneráveis, e desenvolver estratégias de combate – desde denúncias até contra-narrativas, desde educação antidiscriminação até apoio solidário às vítimas.

Integração: Cidadania Digital Crítica e Transformadora

Os três módulos se integram em uma visão holística de cidadania digital crítica e transformadora:



O Papel do Educador em Direitos Humanos na Era Digital

Como educadoras e educadores em direitos humanos, temos responsabilidades específicas e urgentes:

- 1. COMPREENDER PROFUNDAMENTE:** Não basta saber usar tecnologias – precisamos compreender como funcionam, que interesses servem, que impactos causam.
- 2. DESENVOLVER PENSAMENTO CRÍTICO:** Em nós mesmos e em nossos estudantes. Questionar, investigar, não aceitar passivamente.
- 3. PROTEGER OS VULNERÁVEIS:** Especialmente crianças e adolescentes, que são alvos de coleta massiva de dados, violências digitais e manipulação.
- 4. EDUCAR PARA AUTONOMIA:** Não formar usuários passivos, mas cidadãos digitais ativos, críticos, conscientes de direitos e responsabilidades.
- 5. COMBATER INJUSTIÇAS:** Denunciar violações, enfrentar discriminações, desmentir desinformações, combater discursos de ódio.
- 6. PROMOVER INCLUSÃO:** Lutar para que tecnologias sejam acessíveis, inclusivas, democráticas – não instrumentos de exclusão e opressão.

7. CONSTRUIR ALTERNATIVAS: Não apenas criticar, mas propor e construir usos éticos, justos e emancipatórios das tecnologias.

Convite à Ação Permanente

A disciplina termina, mas o trabalho continua. Tecnologias evoluem rapidamente, novos desafios surgem constantemente. Precisamos de:

- Formação permanente – Manter-se atualizado(a)
- Vigilância crítica – Questionar constantemente
- Ação coletiva – Organizar-se com outros educadores
- Incidência política – Participar de debates sobre regulação
- Experimentação pedagógica – Testar metodologias, compartilhar experiências
- Cuidado coletivo – Apoiar-se mutuamente, proteger uns aos outros

Vivemos um momento histórico de profunda transformação. As tecnologias digitais estão reconfigurando nossa sociedade, nossa economia, nossa política, nossas relações, nossa subjetividade. Podemos ser passageiros ou pilotos dessa transformação.

Como educadores em direitos humanos, não temos o luxo da neutralidade. Precisamos tomar partido – pelo lado da justiça, da dignidade, da liberdade, da igualdade, da solidariedade.

As tecnologias não são neutras. Elas podem libertar ou oprimir, incluir ou excluir, empoderar ou subjugar. Depende de nós.

Você, que chegou até aqui, está agora equipado(a) com conhecimentos, competências e ferramentas para fazer a diferença. Para proteger-se e proteger seus estudantes. Para educar cidadãos digitais críticos e conscientes. Para lutar por um mundo digital mais justo.

O futuro digital não está escrito. Está sendo escrito agora. E você tem caneta na mão.

Use-a com sabedoria, coragem e amor pela humanidade.

Grata por esta jornada! Sigamos na luta por direitos humanos na era digital.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Lei Geral de Proteção de Dados: guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-agentes-de-tratamento_final.pdf. Acesso em: 8 jan. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: <https://link.ufms.br/WkeVA>. Acesso em: 8 jan. 2026.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro. Brasília, DF: Presidência da República, 2018. Disponível em: <https://link.ufms.br/Ffx1F>. Acesso em: 8 jan. 2026.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (CETIC.BR). **Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2022**. São Paulo: Comitê Gestor da Internet no Brasil, 2023. Disponível em: <https://link.ufms.br/UV1EK>. Acesso em: 8 jan. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA (UNESCO). **Alfabetização midiática e informacional: diretrizes para a formulação de políticas e estratégias**. Brasília: UNESCO, 2016. Disponível em: <https://link.ufms.br/7kwmt>. Acesso em: 8 jan. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA (UNESCO). **Jornalismo, fake news e desinformação: manual para educação e treinamento em jornalismo**. Brasília: UNESCO, 2019. Disponível em: <https://link.ufms.br/mFMqi>. Acesso em: 8 jan. 2026.

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. **Regulamento (UE) 2016/679: Regulamento Geral sobre a Proteção de Dados (RGPD)**. Bruxelas: União Europeia, 2016. Disponível em: <https://link.ufms.br/yWooT>. Acesso em: 8 jan. 2026.

SAFERNET BRASIL. **Cartilha de segurança para internet**. Salvador: SaferNet Brasil, 2022. Disponível em: <https://link.ufms.br/zxmj2>. Acesso em: 8 jan. 2026.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Rio de Janeiro: Intrínseca, 2021.

Vídeos recomendados (recursos complementares)

PRIVACIDADE hackeada (The Great Hack). Direção: Karim Amer; Jehane Noujaim. **Netflix**, 2019. Documentário (114 min). Disponível em: <https://www.netflix.com/title/80117542>.

O DILEMA DAS REDES (The Social Dilemma). Direção: Jeff Orlowski. **Netflix**, 2020. Documentário (94 min). Disponível em: <https://www.netflix.com/title/81254224>.

NADA a esconder (Nothing to Hide). Direção: Marc Meillassoux. **YouTube**, 2017. Documentário (97 min). Disponível em: <https://www.youtube.com/watch?v=djbwzElv7gE>.

SÉRIE explicando – vigilância de dados (Explained – The Surveillance Economy). **Netflix**, 2019. Episódio de série documental (18 min). Disponível em: <https://www.netflix.com/title/80216752>.



AGEAD

Agência de Educação
Digital e a Distância