Microsoft

책임있는 AI를 위해 고려할 MLOps와 오픈소스

최영락
마이크로소프트

왜 책임있는 AI가 중요할까요?

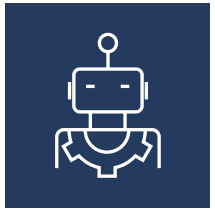
“기술에는 양심이 없다”

“The more powerful the tool, the greater the benefit or damage it can cause…Technology innovation is not going to slow down. The work to manage it needs to speed up.”

Brad Smith
President and Chief Legal Officer, Microsoft

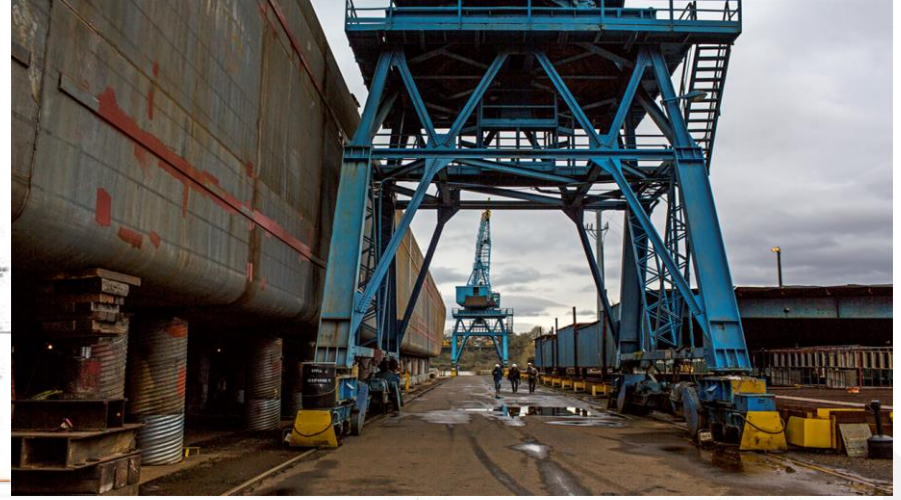
왜 책임있는 AI가 중요할까요?

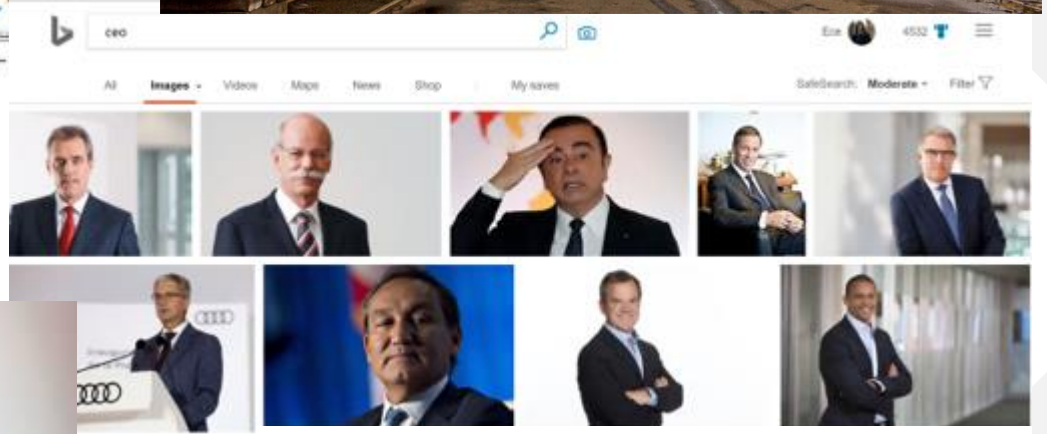
AI가 발전하면서 **혁신 속도**와 점차 **실제 사람의 지능 수준**으로 가까워지면서,
우리 개인 및 사회 전반에 영향을 미치기 때문에 다른 기술과 다릅니다.

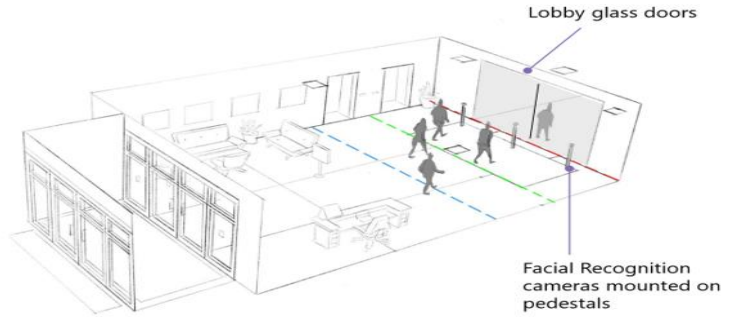
Vision	Speech Recognition	Reading	Translation	Speech Synthesis	Language Understanding
					
2016	**2017**	**2018**	**2018**	**2018**	**2019**
Object recognition human parity	Speech recognition human parity	Reading comprehension human parity	Machine translation human parity	Speech synthesis near-human parity	General Language Understanding human parity

오늘날 토론/논쟁이 이루어지는 부분

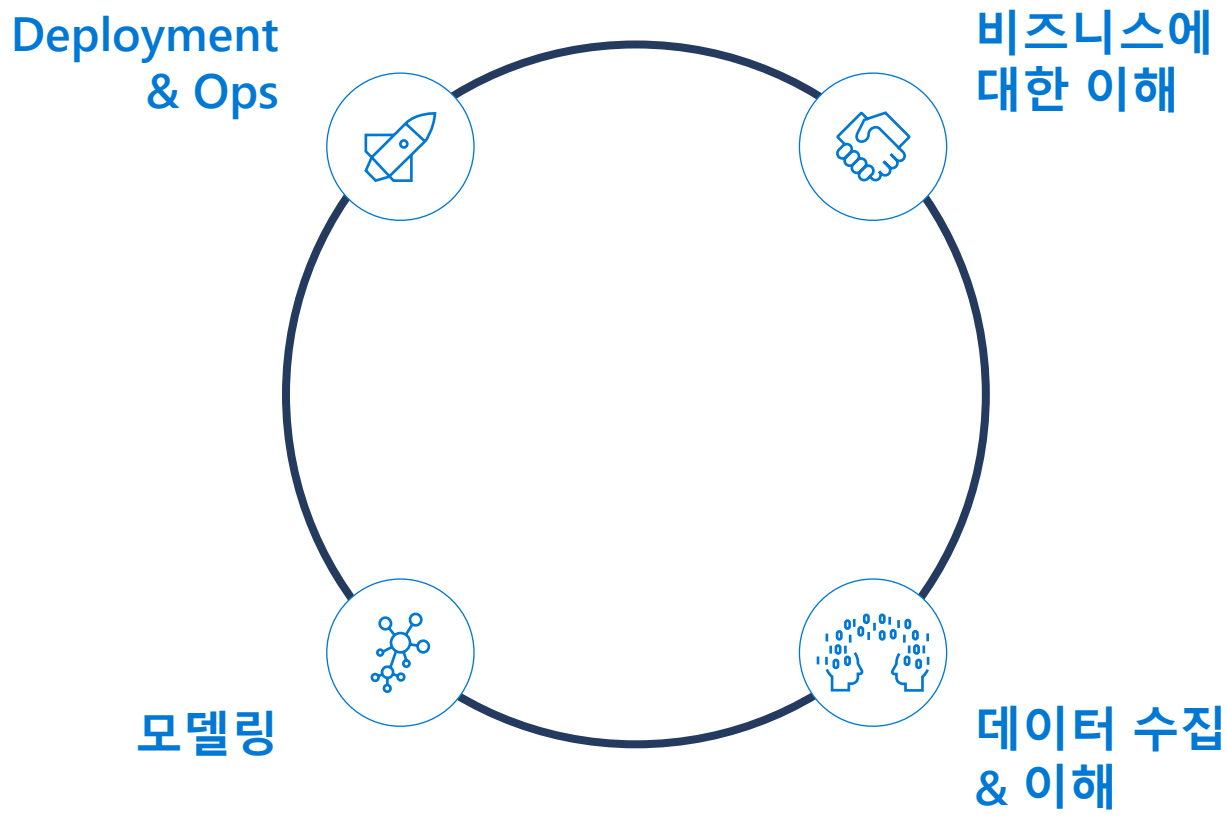
- Facial Recognition
- Fairness
- Corporate responsibility
- Deepfakes
- Human rights
- Meaningful human control
- Contact tracing
- Consent
- Unintended consequences
- Disproportionate impact
- Model Fragility
- Socio-technical issues
- Algorithmic auditing
- Platform accountability
- Regulation



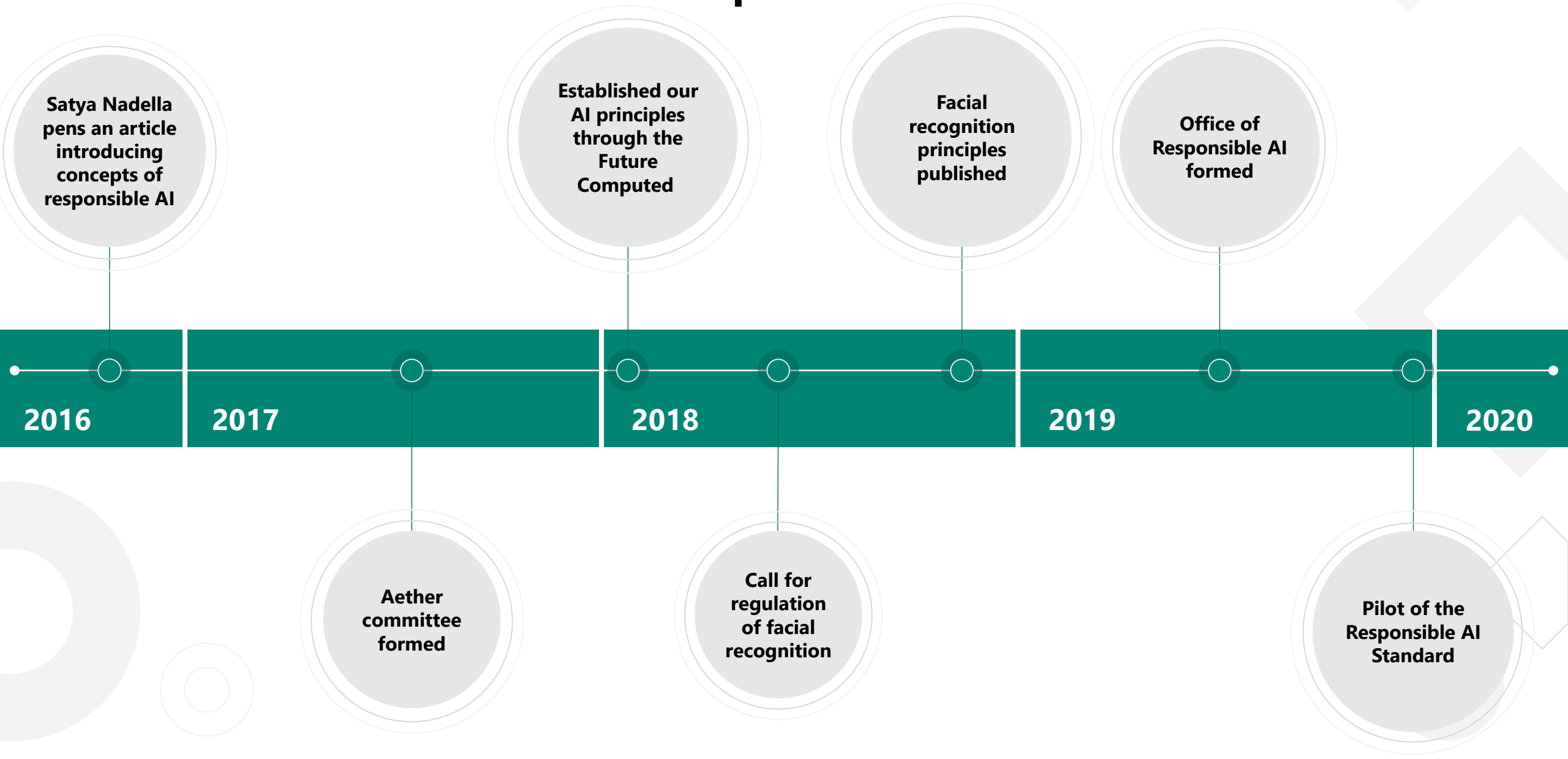




책임감있는 AI (Responsible AI) : 복잡하고 광범위한 주제



마이크로소프트 여정: Responsible AI



책임감있는 AI를 위한 마이크로소프트 Approach

Principles (원칙)

Fairness (공정성)

Inclusiveness (포괄적)

Transparency (투명성)

Accountability (책임)

Reliability & Safety (신뢰 & 안전성)

Privacy & Security (보안 & 개인정보)

실천 사례 (Practices)

Ethics Committees (윤리 위원회)

Governance (거버넌스)

Methodology (방법론)

Documentation (문서화)

Tools (도구)

Homomorphic Encryption

Differential Privacy

Interpret ML

Data Drift

책임감있는 AI를 위한 마이크로소프트 Approach

Principles (원칙)

Fairness (공정성)

Inclusiveness (포괄적)

Transparency (투명성)

Accountability (책임)

Reliability & Safety (신뢰 & 안전성)

Privacy & Security (보안 & 개인정보)

실천 사례 (Practices)

Ethics Committees (윤리 위원회)

Governance (거버넌스)

Methodology (방법론)

Documentation (문서화)

Tools (도구)

Homomorphic Encryption

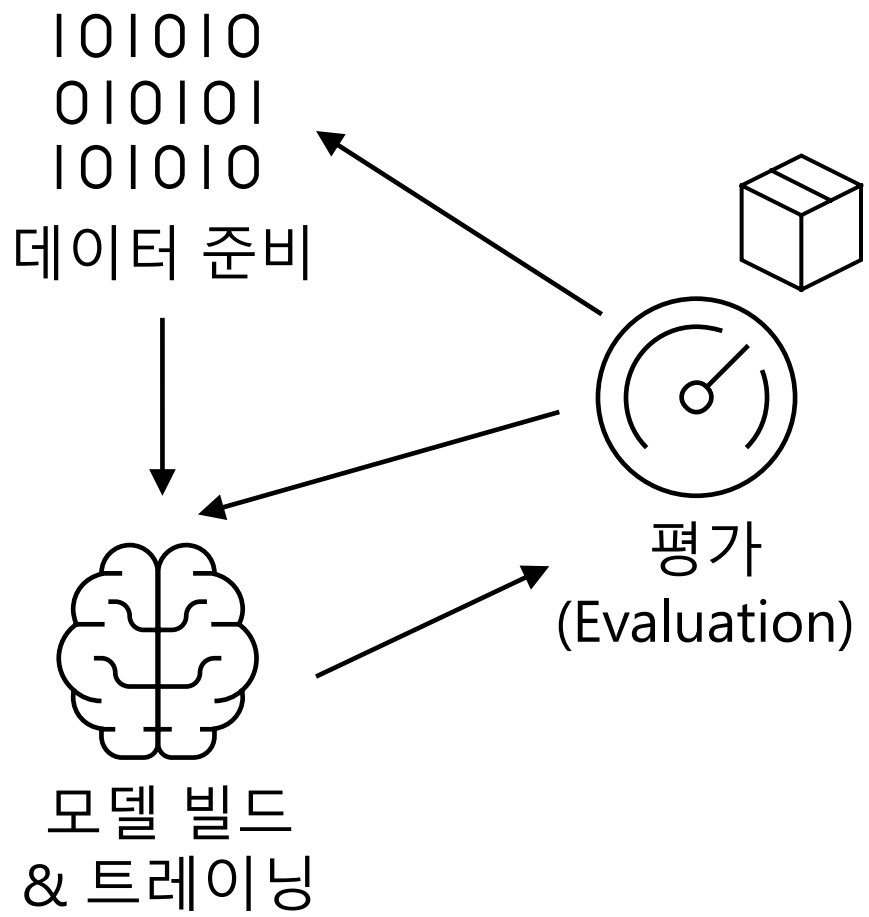
Differential Privacy

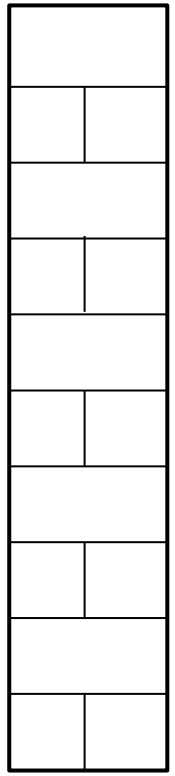
Interpret ML

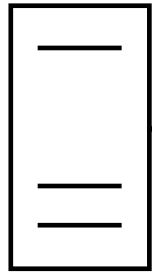
Data Drift

1. MLOps: 운영 관점에서 머신러닝 도구

머신 러닝 프로세스







프로덕션

DEVOPS	MLOPS
코드 관리 (소스 파일)	코드 관리 (소스 파일) 데이터 파일, 노트북, README 등 문서 관리
인프라 관리 (as code)	인프라 관리 (as code) 환경 관리 (as code)
소스 코드/버전 제어	소스 코드 제어 실험 결과 추적 데이터셋 관리
실행 파일 빌드 빌드: 짧으면 수 분, 길게는 몇 시간 소요 (대부분) 상용 컴퓨팅 자원 또는 PaaS	모델 트레이닝 모델 트레이닝: 때로는 며칠/몇 주 소요 GPU 컴퓨팅
빌드 버전 관리	모델 버전 관리 재현 가능한 환경 관리
테스트 (deterministic) 코드 버그 수정	테스트 (probabilistic) 코드 버그 수정 and/or 데이터 모델 변경 / 모델 재트레이닝 등

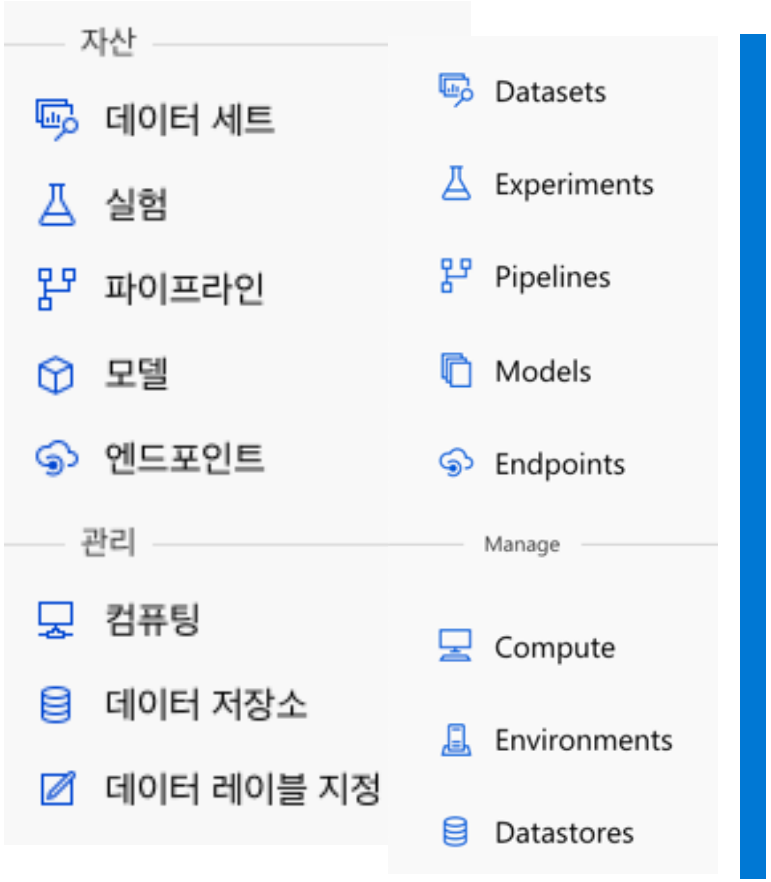
Azure Machine Learning 서비스 & GitHub Actions 를 적용하면서 "책임감있는 AI" 고려하기

Set of Azure Cloud Services + **Python & R SDKs** + **GitHub Actions**

That enables you to:

- ✓ Prepare Data
- ✓ Build Models
- ✓ Train Models
- ✓ Manage Models
- ✓ Track Experiments
- ✓ Deploy Models
- ✓ Manage Code
- ✓ Collaborate
- ✓ Continuous Integration

Azure Machine Learning과 MLOps



Datasets – registered, known data sets

Experiments – 트레이닝 실행

Pipelines – 트레이닝 워크플로우

Models – 등록된 모델 (버전 관리)

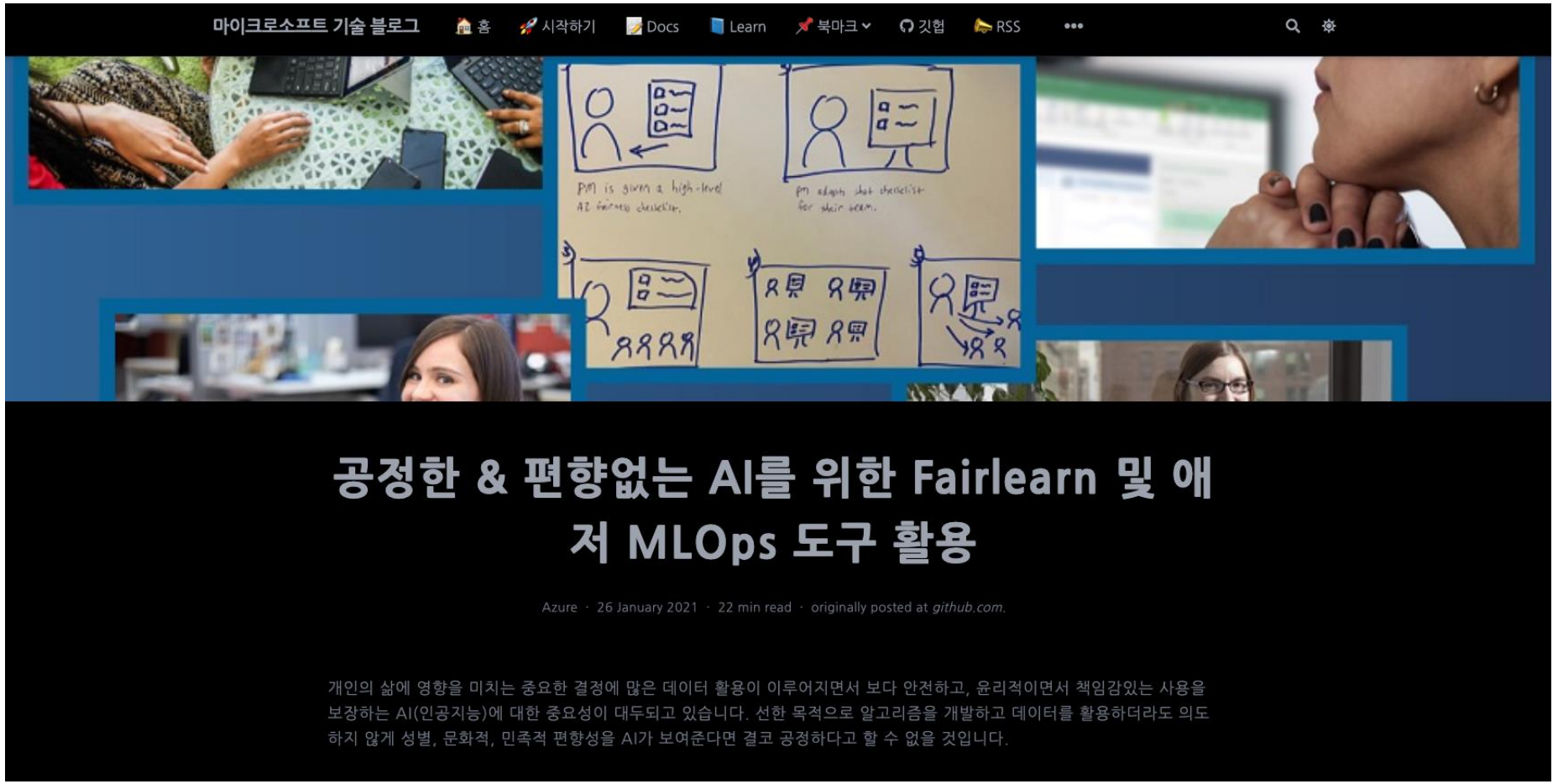
Endpoints – 배포가 이루어진 모델 엔드포인트

Compute – (CPU/GPU) 컴퓨팅 자원 관리

Environments – 트레이닝 및 추론 환경 관리

Datastores – 데이터저장소와 연결

Quick Demo: Fairlearn 오픈소스와 MLOps



블로그 글: **https://aka.ms/fairlearn-and-mlops**

AI, 윤리적인 고민 또한 중요합니다 "감사합니다"

- Enable people
- Inclusive
- Fair and Transparent

질문 있으신 분?

- 온라인 라이브 질의응답 일시
  : 2021년 3월 29일(월요일) 오후 4시~5시

뉴스레터에 가입하세요!

커뮤니티 전문가로부터 정기적인 업데이트 및 커뮤니티 이벤트, 워크샵에 대한 안내를 Microsoft.Source 뉴스레터 형태로 받으실 수 있습니다.

https://aka.ms/devKR

Microsoft