FPT Education

FPT POLYTECHNIC

cdio™

Conceive Design Implement Operate



AN TOÀN THÔNG TIN & ĐẠO ĐỨC SỐ

AN TOÀN THÔNG TIN & ĐẠO ĐỨC SỐ

https://caodang.fpt.edu.vn

MỤC LỤC

- **Nội dung chính:** Giới thiệu tổng quan về
  - An toàn thông tin
  - Các tiêu chuẩn về An toàn thông tin (ISO và TCVN)
  - Vấn đề "đạo đức số"
  - Vấn đề "deepfake"
  - Một vài luật ở Việt Nam
- **Mục tiêu:**
  - Hiểu được các khái niệm cơ bản
  - Khai thác và sử dụng thông tin một cách an toàn
  - Hình thành ý thức đạo đức số và trách nhiệm số



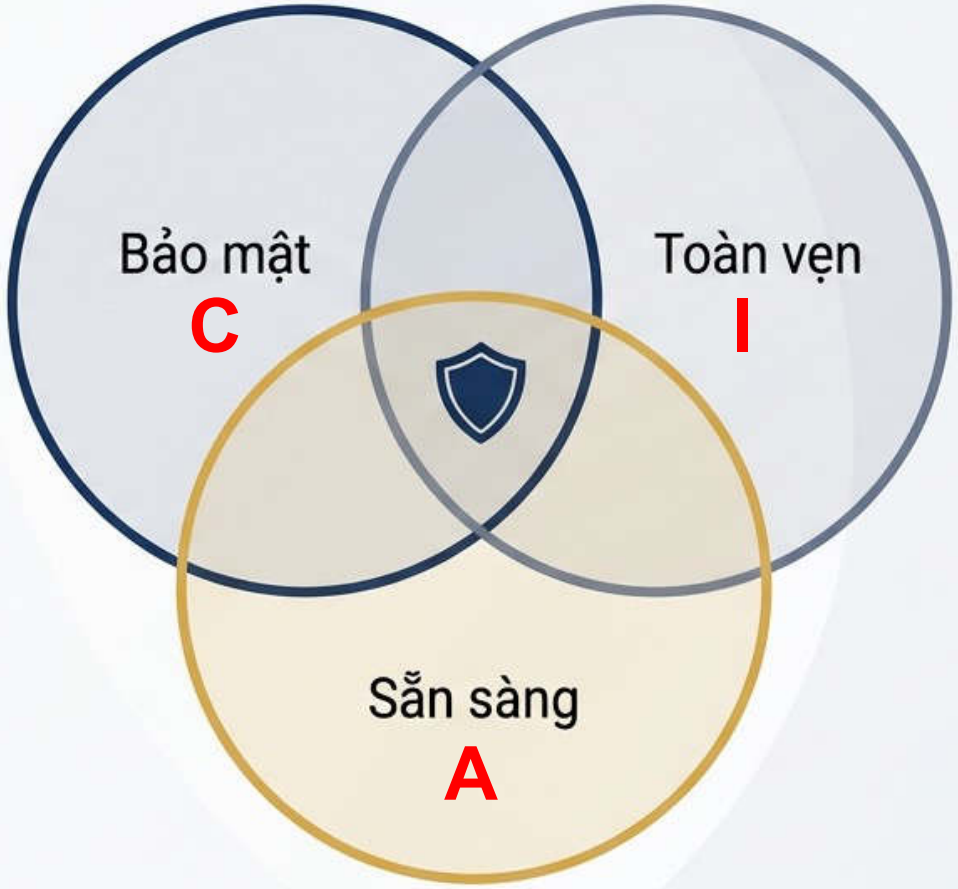


AN TOÀN THÔNG TIN

Bản Chất Của An Toàn Thông Tin

Bản chất của an toàn thông tin không chỉ là công nghệ, mà là việc bảo vệ các "tài sản thông tin" quý giá khỏi rủi ro. Trọng tâm xoay quanh 3 yếu tố cốt lõi:

- **Tính Bảo mật (Confidentiality):** Đảm bảo thông tin chỉ được tiếp cận bởi những cá nhân hoặc hệ thống được cấp phép.
- **Tính Toàn vẹn (Integrity):** Thông tin phải duy trì sự chính xác, đầy đủ và không bị sửa đổi trái phép trong suốt vòng đời.
- **Tính Sẵn sàng** (Availability): Thông tin và hệ thống luôn có thể truy cập và sử dụng được ngay khi người dùng hợp lệ cần đến.



Các Trụ Cột Trong Hệ Thống Quản Lý



Nhận diện rủi ro

Hiểu rõ tổ chức đang sở hữu dữ liệu gì, giá trị ra sao và những mối đe dọa nào (tin tặc, thiên tai, lỗi con người) có thể xảy ra.



Thiết lập kiểm soát

Áp dụng các biện pháp bảo vệ phù hợp để giảm thiểu rủi ro (đặt mật khẩu mạnh, mã hóa dữ liệu, thẻ từ ra vào).



Yếu tố con người

Công nghệ tối tân cũng vô nghĩa nếu người dùng thiếu nhận thức. Đào tạo và xây dựng văn hóa bảo mật là bắt buộc.



Cải tiến liên tục

Rủi ro luôn biến đổi. Hệ thống cần được giám sát, đánh giá và nâng cấp thường xuyên để không bị lỗi thời.

Góc Nhìn Thực Tế: Sự Khác Biệt Nằm Ở Đâu?

Tình huống: Một nhân viên để quên chiếc laptop chứa toàn bộ danh sách khách hàng và dữ liệu tài chính tại quán cà phê.



Không có hệ thống bảo vệ

Laptop không có mật khẩu đăng nhập, ổ cứng không được mã hóa. Kẻ xấu dễ dàng mở máy và sao chép toàn bộ dữ liệu. Công ty đối mặt với nguy cơ bị phạt pháp lý, rò rỉ bí mật kinh doanh, mất uy tín nghiêm trọng và khách hàng rời bỏ.



Đã áp dụng An toàn thông tin

Laptop yêu cầu xác thực sinh trắc học, toàn bộ ổ cứng được mã hóa chuẩn quốc tế. Quản trị viên ngay lập tức gửi lệnh "Xóa dữ liệu từ xa" khi nhận báo cáo mất máy. Công ty chỉ thiệt hại giá trị phần cứng; dữ liệu và uy tín kinh doanh vẫn được bảo vệ tuyệt đối.

Góc Thảo Luận: Thách Thức Trong Thực Tiễn

An toàn thông tin không phải là một đích đến tuyệt đối, mà là một quá trình cân bằng liên tục.

Bảo mật vs. Sự tiện lợi

Mật khẩu càng dài, càng phức tạp và yêu cầu xác thực nhiều bước thì hệ thống càng an toàn. Tuy nhiên, điều này lại khiến thao tác của người dùng trở nên phiền toái toái và chậm chạp. Làm sao để tìm ra điểm cân bằng hoàn hảo giữa việc bảo vệ hệ thống và duy trì hiệu suất làm việc?



Con người vs. Công nghệ

Nhiều chuyên gia nhận định: "Con người luôn là mắt xích yếu nhất trong mọi hệ thống bảo mật". Đầu tư ngân sách vào các phần mềm tường lửa đắt tiền hay tập trung đào tạo nhân viên cách nhận biết email lừa đảo (phishing) sẽ mang lại hiệu quả bảo vệ thực tế cao hơn?

Hệ thống quản lý an toàn thông tin (ISMS) bao gồm các chính sách, quy trình, hướng dẫn, nguồn lực và hoạt động liên quan, được quản lý chung bởi một tổ chức, nhằm mục đích bảo vệ tài sản thông tin của tổ chức đó.

ISMS là một phương pháp có hệ thống để thiết lập, triển khai, vận hành, giám sát, xem xét, duy trì và cải thiện an ninh thông tin của một tổ chức nhằm đạt được các mục tiêu kinh doanh. Nó dựa trên việc đánh giá rủi ro và mức độ chấp nhận rủi ro của tổ chức được thiết kế để xử lý và quản lý rủi ro một cách hiệu quả. Phân tích các yêu cầu bảo vệ tài sản thông tin và áp dụng các biện pháp kiểm soát thích hợp để đảm bảo bảo vệ các tài sản thông tin này, khi cần thiết, góp phần vào việc triển khai thành công một ISMS.

Theo ISO 27000

Các nguyên tắc cơ bản sau đây cũng góp phần vào việc triển khai thành công một ISMS:

a) nâng cao nhận thức về nhu cầu an ninh thông tin;
b) phân công trách nhiệm về an ninh thông tin;
c) kết hợp cam kết của ban quản lý và lợi ích của các bên liên quan;
d) nâng cao các giá trị xã hội;
e) đánh giá rủi ro để xác định các biện pháp kiểm soát thích hợp nhằm đạt được mức độ rủi ro chấp nhận được;
f) an ninh được tích hợp như một yếu tố thiết yếu của mạng lưới và hệ thống thông tin;
g) chủ động phòng ngừa và phát hiện các sự cố an ninh thông tin;
h) đảm bảo một cách tiếp cận toàn diện đối với quản lý an ninh thông tin;
i) Đánh giá lại liên tục về an ninh thông tin và thực hiện các điều chỉnh khi cần thiết.

Theo ISO 27000



ĐẠO ĐỨC SỐ

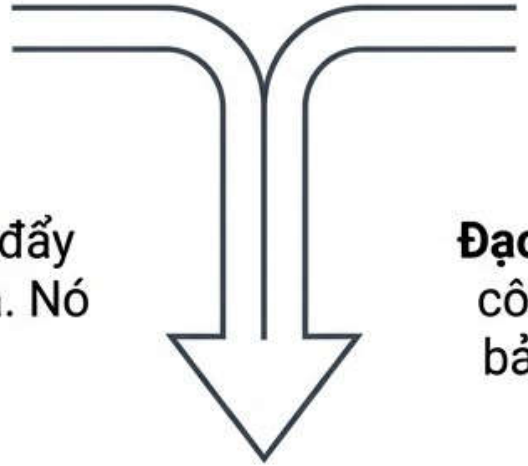
Hiểu về "ĐẠO ĐỨC SỐ" thông qua lăng kính của 4 tổ chức hàng đầu

Tại sao máy móc cần có đạo đức?

Trí tuệ nhân tạo (AI) mang lại sức mạnh vô hạn, nhưng sức mạnh thiếu định hướng sẽ trở thành mối nguy.



Công nghệ là Động cơ. Nó thúc đẩy tốc độ, hiệu suất và tự động hóa. Nó giúp chúng ta đi nhanh hơn.





Đạo đức số là Vô lăng. Nó đảm bảo công nghệ không đi chệch hướng, bảo vệ con người khỏi sự thiên vị, rủi ro và mất kiểm soát.

Đạo đức số không phải là rào cản cản trở sự phát triển, mà là bộ quy tắc đảm bảo công nghệ phục vụ lợi ích tốt nhất của nhân loại.

Bốn cách tiếp cận, một mục tiêu chung

Cách thế giới kiểm soát AI đang được định hình bởi sự kết hợp giữa các chính phủ toàn cầu và những gã khổng lồ công nghệ.

UNESCO

Nền tảng toàn cầu. Đặt con người và thiên thiên nhiên làm trung tâm.

Microsoft

Tấm khiên doanh nghiệp. Nguyên tắc thực tế cho phần mềm hàng ngày.

Google

Cán cân đổi mới. Cân bằng giữa đột phá khoa học và sự an toàn.

OpenAI

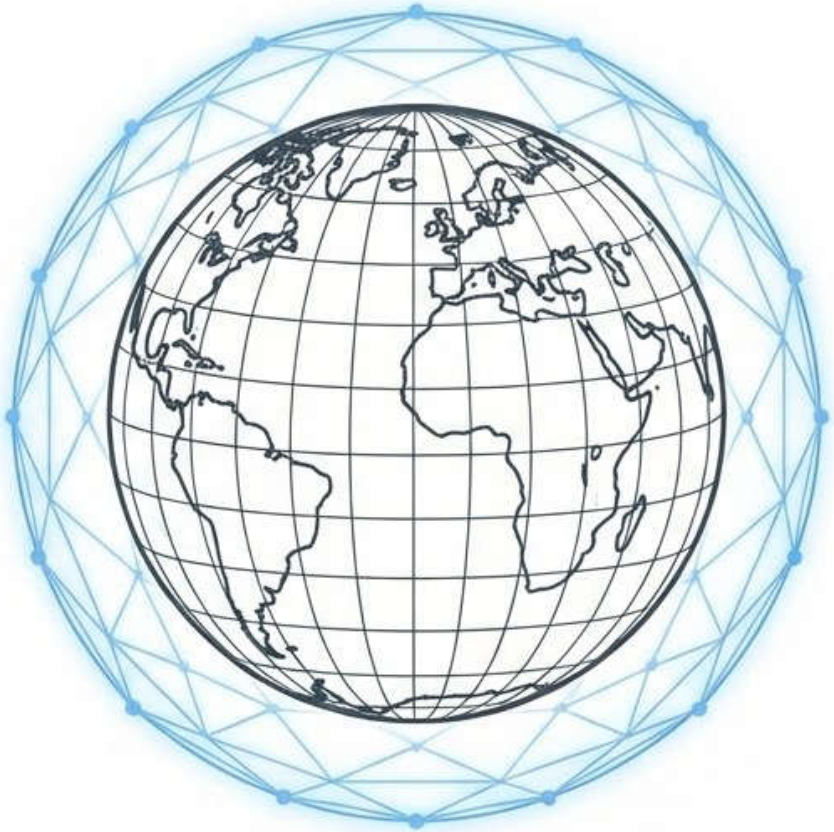
La bàn tương lai. Tầm nhìn dài hạn hướng tới Siêu trí tuệ (AGI).

01 / UNESCO

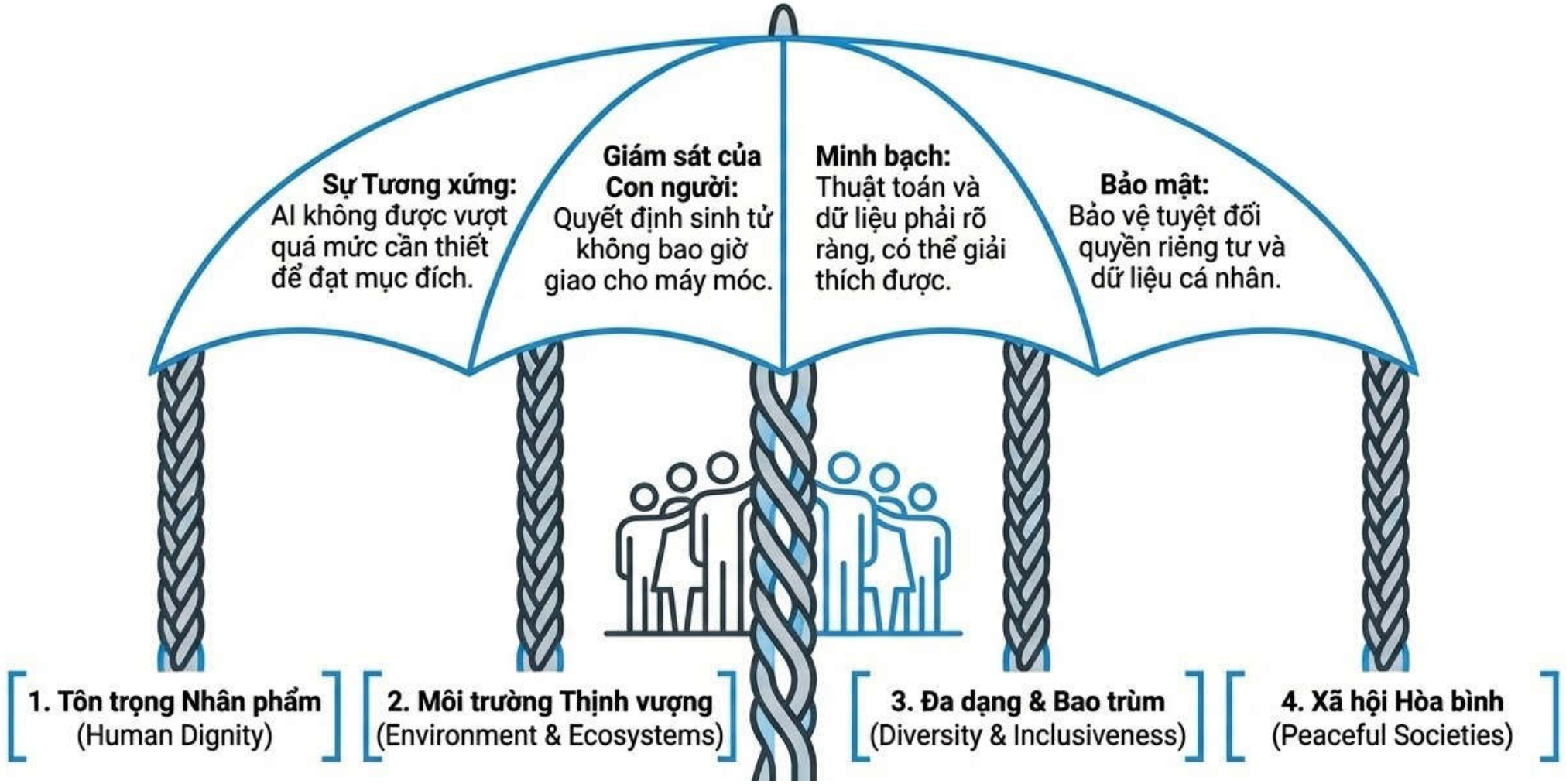
Tiêu chuẩn của Nhân loại & Trái đất

Khác với các công ty công nghệ, bộ quy tắc của UNESCO không nhằm tạo ra sản phẩm. Đây là một hiệp ước toàn cầu nhằm định hướng cho luật pháp của các quốc gia.

Trọng tâm của UNESCO là **bảo vệ Quyền con người** và **Sự phát triển của Hệ sinh thái.** Công nghệ phải phục vụ sự đa dạng văn hóa và không để ai bị bỏ lại phía sau, đặc biệt là các quốc gia đang phát triển.



Mô hình "Chiếc Ô Toàn Cầu" của UNESCO



02 / MICROSOFT



Tích hợp Đạo đức vào Phần mềm

Microsoft là người khổng lồ cung cấp công cụ cho các doanh nghiệp toàn cầu (như Office, Azure). Do đó, cách tiếp cận đạo đức của họ mang tính thực tiễn cao: làm sao để biến lý thuyết thành các tính năng và bộ lọc an toàn ngay trong mã nguồn.

Xây dựng niềm tin thông qua hệ thống có thể kiểm chứng, đánh giá rủi ro và các công cụ thực thi trực tiếp trên phần mềm hàng ngày.

6 Trụ cột Đạo đức của Microsoft



Công bằng (Fairness)
AI phải đối xử bình đẳng, không thiên vị hay phân biệt đối xử với bất kỳ nhóm người nào.

Đáng tin & An toàn (Reliability & Safety)
Hệ thống phải hoạt động chuẩn xác ngay cả trong các tình huống bất ngờ.

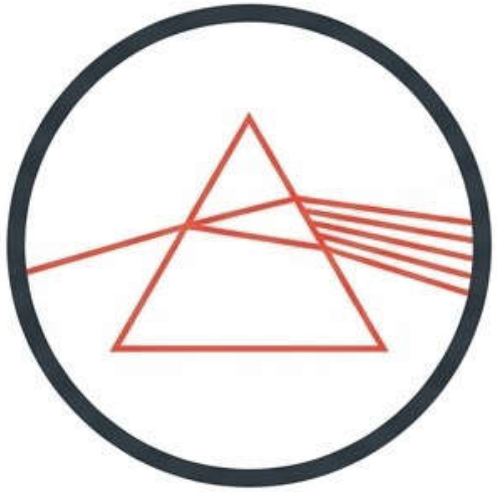
Bảo mật (Privacy & Security)
Tôn trọng và bảo vệ nghiêm ngặt dữ liệu của người dùng.

Hòa nhập (Inclusiveness)
Thiết kế để mọi người, mọi nền tảng và mọi khiếm khuyết đều có thể sử dụng.

Minh bạch (Transparency)
Người dùng phải hiểu được hệ thống AI đang làm gì và khả năng của nó đến đâu.

Trách nhiệm (Accountive (Accountability)
Con người luôn là người chịu trách nhiệm pháp lý và đạo đức cuối cùng, không phải máy móc.

03 / GOOGLE



Nghệ thuật Cân bằng

Sứ mệnh của Google là tổ chức thông tin của thế giới. Triết lý đạo đức của họ phản ánh một sự giằng co liên tục: làm thế nào để thúc đẩy ranh giới của khoa học (Y tế, Khí hậu, Lượng tử) mà không giải phóng những công cụ gây hại cho xã hội.

Đổi mới táo bạo (Bold Innovation) nhưng phải đi kèm với Phát triển có trách nhiệm (Responsible Development).

Cán cân Đổi mới và Trách nhiệm



Đổi mới Táo bạo (Bold Innovation)

- Tạo ra bước đột phá trong sinh học, y học, vật lý học.
- Giải quyết các vấn đề vĩ mô của nhân loại (ví dụ: dự báo biến đổi khí hậu).
- Chia sẻ khám phá để thúc đẩy kinh tế và sáng tạo.

Phát triển Có trách nhiệm (Responsible Development)

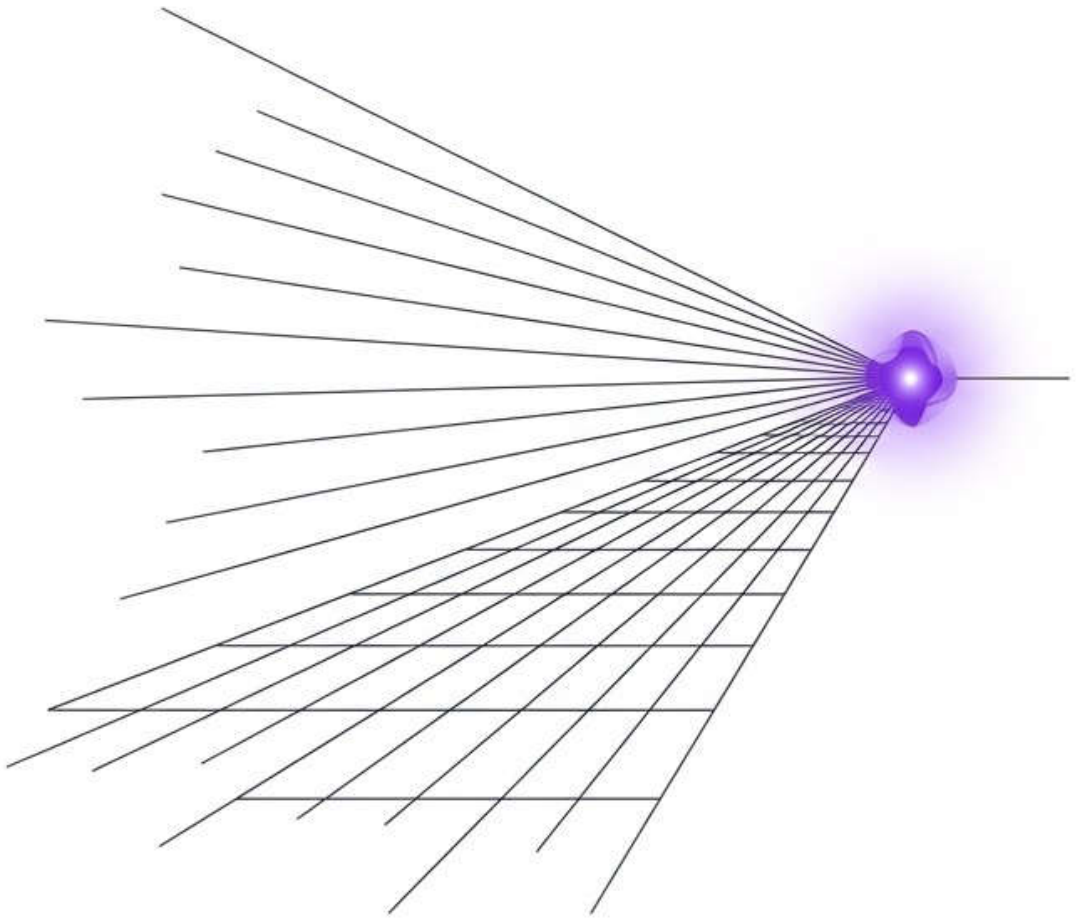
- Lợi ích mang lại phải vượt trội hoàn toàn so với rủi ro có thể thấy trước.
- Tránh tạo ra hoặc củng cố những thành kiến bất công trong xã hội.
- Áp dụng các bài kiểm tra an toàn nghiêm ngặt trước khi ra mắt công chúng.

04 / OPENAI

Tầm nhìn về Siêu Trí Tuệ (AGI)

Khác với các tổ chức khác tập trung vào công nghệ hiện tại, hiến chương của OpenAI hoàn toàn hướng về tương lai. Mục tiêu duy nhất của họ là **AGI** (**Artificial General Intelligence**) – hệ thống máy móc có thể vượt trội hơn con người trong hầu hết mọi công việc kinh tế.

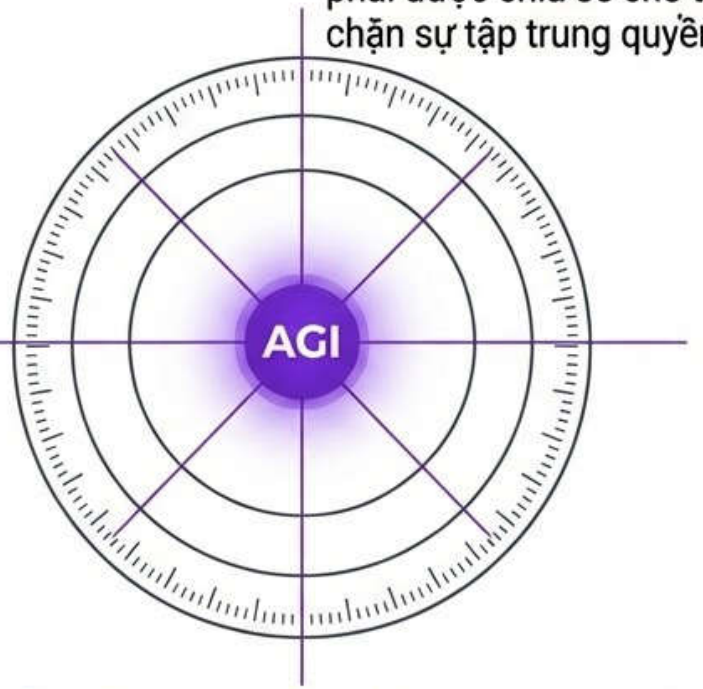
Tránh một cuộc chạy đua vũ trang AI và đảm bảo rằng khi AGI xuất hiện, nó sẽ mang lại lợi ích cho toàn bộ nhân loại, chứ không phải một nhóm nhỏ.



La Bàn Hướng Tới AGI

Phân phối Lợi ích (Distributed Benefits).
Nếu AGI thành công, ảnh hưởng và nguồn lực phải được chia sẻ cho tất cả mọi người, ngăn chặn sự tập trung quyền lực độc hại.

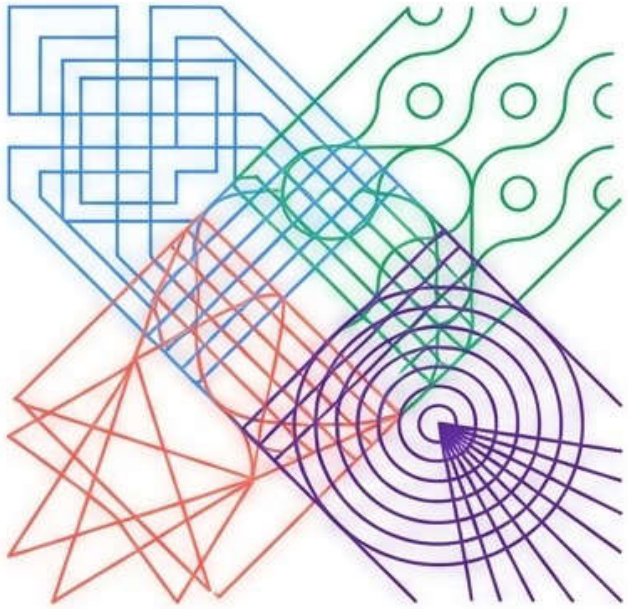
Hợp tác Toàn cầu (Cooperative Orientation).
Xây dựng cộng đồng toàn cầu, chia sẻ nghiên cứu (trừ khi có rủi ro an ninh nghiêm trọng).



An toàn Dài hạn (Long-term Safety).
Nghiên cứu sâu về an toàn. Sẵn sàng ngừng cạnh tranh và hợp tác với dự án khác nếu họ sắp đạt được AGI an toàn trước.

Dẫn đầu Công nghệ (Technical Leadership).
Phải là người giỏi nhất về công nghệ mới có đủ tiếng nói và năng lực để định hướng chính sách an toàn của thế giới.

Từ Nguyên tắc đến Toàn cảnh



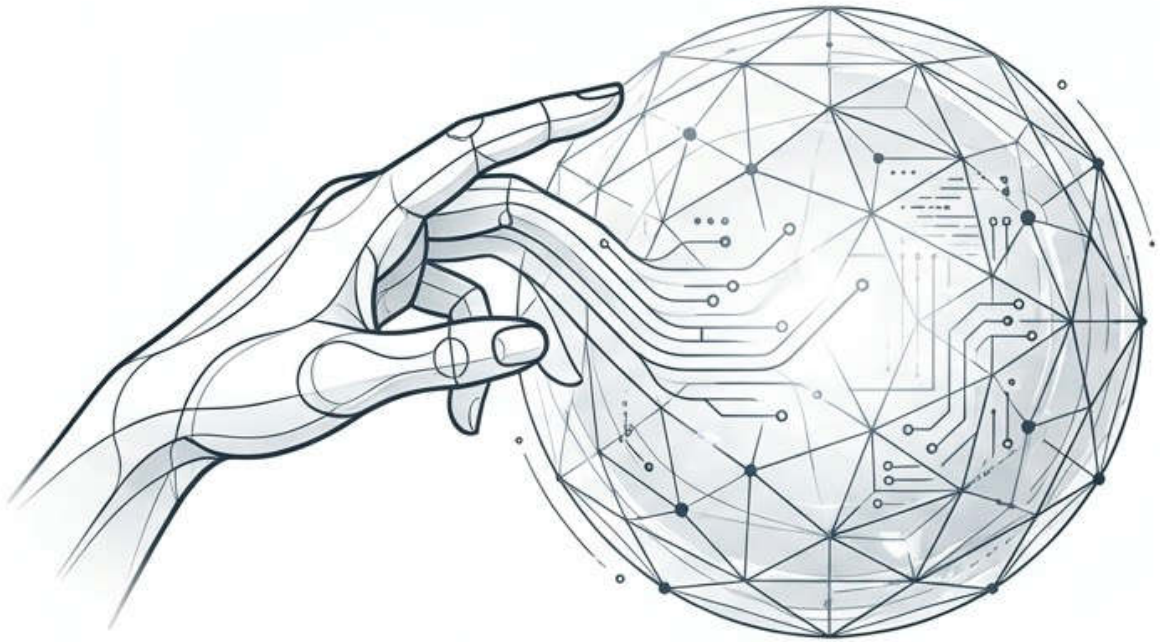
Bốn tổ chức, bốn lăng kính khác biệt. UNESCO nhìn từ góc độ luật pháp quốc tế.
Microsoft nhìn từ góc độ phần mềm doanh nghiệp. Google cân bằng giữa khoa học và thương mại.
OpenAI hướng ánh nhìn về một tương lai viễn tưởng.

Khi đặt cạnh nhau, họ tạo thành một mạng lưới bảo vệ đa tầng cho Đạo đức số toàn cầu.
Hãy cùng so sánh sự khác biệt cốt lõi.

Ma trận Đạo đức Số (The Alignment Matrix)

	UNESCO	Microsoft	Google	OpenAI
Bản chất (Core Nature)	Hiệp ước Toàn cầu	Khung thực hành Doanh nghiệp	Cán cân Đổi mới	Hiến chương Tương lai
Mục tiêu Tối thượng (Ultimate Goal)	Bảo vệ Quyền con người & Trái đất	Xây dựng công cụ AI đáng tin cậy	Giải quyết vấn đề lớn của nhân loại	Tạo ra AGI an toàn và có lợi
Ưu tiên Hàng đầu (Top Priority)	Đa dạng văn hóa & Bao trùm	Bảo mật & Trách nhiệm giải trình	Đột phá khoa học + An toàn	An toàn dài hạn & Hợp tác
Điểm Khác biệt (Unique Trait)	Góc nhìn vĩ mô (chính phủ, luật pháp)	Tích hợp trực tiếp vào phần mềm	Kiểm tra nghiêm ngặt trước khi ra mắt	Sẵn sàng ngừng cạnh tranh vì mục đích chung

Tương lai được viết bằng Cốt lõi Nhân bản



Dù được viết dưới dạng luật lệ toàn cầu, bộ lọc phần mềm hay hiến chương tương lai, thông điệp cốt lõi của Đạo đức số đều giống nhau: Công nghệ phục vụ con người.

Bản thiết kế của tương lai không chỉ cần những dòng code thông minh, mà còn cần những giới hạn mang tính nhân văn. Máy móc học từ dữ liệu, nhưng đạo đức của chúng học từ chính chúng ta.



MỘT VÀI LUẬT CỦA VIỆT NAM

Một vài luật của Việt Nam



LUẬT AN NINH MẠNG

24/2018/QH14
HIỆU LỰC NGÀY 01-01-2019

Luật này quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan

An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân

Tham khảo toàn văn tại link này

Một vài luật của Việt Nam



LUẬT TRÍ TUỆ NHÂN TẠO

134/2025/QH15

HIỆU LỰC NGÀY 01-03-2026

1. Luật này quy định về nghiên cứu, phát triển, cung cấp, triển khai và sử dụng hệ thống trí tuệ nhân tạo (sau đây gọi là hoạt động trí tuệ nhân tạo); quyền, nghĩa vụ của tổ chức, cá nhân có liên quan và quản lý nhà nước đối với hoạt động trí tuệ nhân tạo tại Việt Nam.
2. Hoạt động trí tuệ nhân tạo chỉ phục vụ cho mục đích quốc phòng, an ninh, cơ yếu không thuộc phạm vi điều chỉnh của Luật này.

Tham khảo toàn văn tại link này

Một vài luật của Việt Nam



LUẬT BẢO VỆ DỮ LIỆU CÁ NHÂN

91/2025/QH15

HIỆU LỰC NGÀY 01-01-2026

1. Luật này quy định về dữ liệu cá nhân, bảo vệ dữ liệu cá nhân và quyền, nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.
2. Luật này áp dụng đối với:
   a) Cơ quan, tổ chức, cá nhân Việt Nam;
   b) Cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam;
   c) Cơ quan, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động xử lý dữ liệu cá nhân của công dân Việt Nam và người gốc Việt Nam chưa xác định được quốc tịch đang sinh sống tại Việt Nam đã được cấp giấy chứng nhận căn cước.

Tham khảo toàn văn tại link này

FPT Education

FPT POLYTECHNIC

cdio™

Conceive Design Implement Operate



AN TOÀN THÔNG TIN & ĐẠO ĐỨC SỐ

DEEPFAKE

https://caodang.fpt.edu.vn



DEEPFAKE

90%

Khối lượng nội dung trực tuyến được dự đoán sẽ do AI tạo ra vào năm 2025.

Hiểu Về Khái Niệm

Phương tiện Tổng hợp (Synthetic Media)

Nội dung được tạo ra hoặc chỉnh sửa bằng Trí tuệ Nhân tạo (AI). Thường dùng cho mục đích giải trí, y tế, hoặc giáo dục.

Deepfake

Phương tiện tổng hợp được sử dụng với mục đích độc hại (như lừa đảo, mạo danh, thông thông tin sai lệch). Đây là cuộc khủng hoảng không chỉ về công nghệ, mà còn về đạo đức và xã hội.

Ma Trận Rủi Ro: Tác Động Của Deepfake



Cá Nhân

Tống tiền & Đe dọa.

Trộm cắp danh tính & Lừa đảo tài chính.

Bắt nạt trên không gian mạng.



Tổ Chức

Thao túng giá cổ phiếu.

Lừa đảo doanh nghiệp.

Làm giả bằng chứng pháp lý & Tổn hại thương hiệu.



Xã Hội

Thao túng bầu cử & Dân chủ.

Làm suy yếu truyền thông.

Xói mòn niềm tin vào thông tin đại chúng.

Bức Tranh Ứng Phó Toàn Cầu: 3 Tuyến Phòng Thủ

Tuyến 1: Chính sách & Quyền lợi	Khung pháp lý, bảo vệ bản quyền và người tiêu dùng.	Tổ chức: WIPO, Consumers International.
Tuyến 2: Công nghệ Nhận diện	Công cụ kỹ thuật để phát hiện nội dung thao túng.	Tổ chức: Fraunhofer HHI, DeepMedia, CAICT, China Mobile.
Tuyến 3: Nguồn gốc & Tiêu chuẩn	Dấu chuẩn xác thực và truy xuất nguồn gốc nội dung từ lúc tạo ra.	Tổ chức: C2PA (Adobe/Microsoft), SenseTime, ITU, IETF SCITT, JPEG.

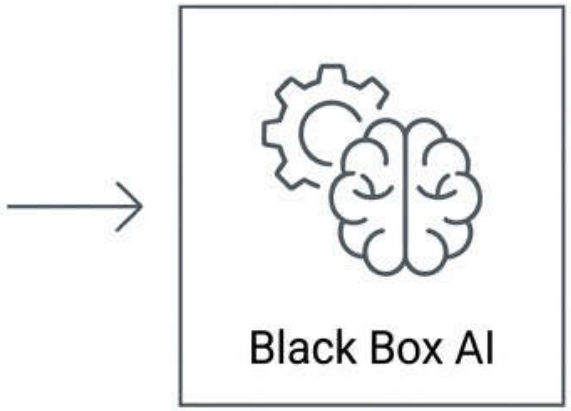
Tuyến 1 | WIPO: Bài Toán Bản Quyền Của AI

Đầu Vào (Inputs)

- Dữ liệu huấn luyện (Training Data).

Vấn đề: Sử dụng nội dung có bản quyền mà không xin phép.

Giải pháp: Các ngoại lệ khai thác dữ liệu & Cơ chế từ chối (Opt-out) cho tác giả.



Đầu Ra (Outputs)

- Sản phẩm AI tạo ra (AI-Generated Content).

Vấn đề: Tác phẩm do AI tạo ra hoàn toàn không được bảo hộ bản quyền.

Đánh giá: Vi phạm hay không phụ thuộc vào "độ tương đồng" với tác phẩm gốc (đánh giá theo từng trường hợp).

Tuyến 1 | Quyền Người Tiêu Dùng & Đạo Luật AI

Đảo Ngược Gánh Nặng Chứng Minh

(Consumers International) Người tiêu dùng không có công cụ chuyên sâu. Trách nhiệm chứng minh và gắn nhãn nội dung giả mạo phải thuộc về nền tảng công nghệ và người tạo ra chúng.



Minh Bạch Bắt Buộc

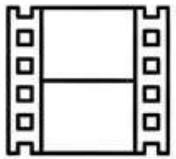
(Dựa trên Đạo luật AI của EU) Nội dung do AI tạo ra phải được dán nhãn rõ ràng để tránh hiểu lầm. Các ứng dụng Deepfake rủi ro cao (thao túng chính trị, giám sát) bị kiểm soát nghiêm ngặt hoặc cấm hoàn toàn.

Tuyến 2 | Fraunhofer HHI: Máy Móc Nhìn Thấy Gì?



Không gian (Spatial - CNN)

Nhận diện hình ảnh tĩnh. Tìm kiếm các lỗi hòa trộn, mờ viền, hoặc phản chiếu ánh sáng sai lệch trong mắt.



Thời gian (Temporal - R-CNN)

Nhận diện video. Phân tích sự thiếu nhất quán trong chuyển động qua nhiều khung hình (ví dụ: tần suất chớp mắt bất thường).

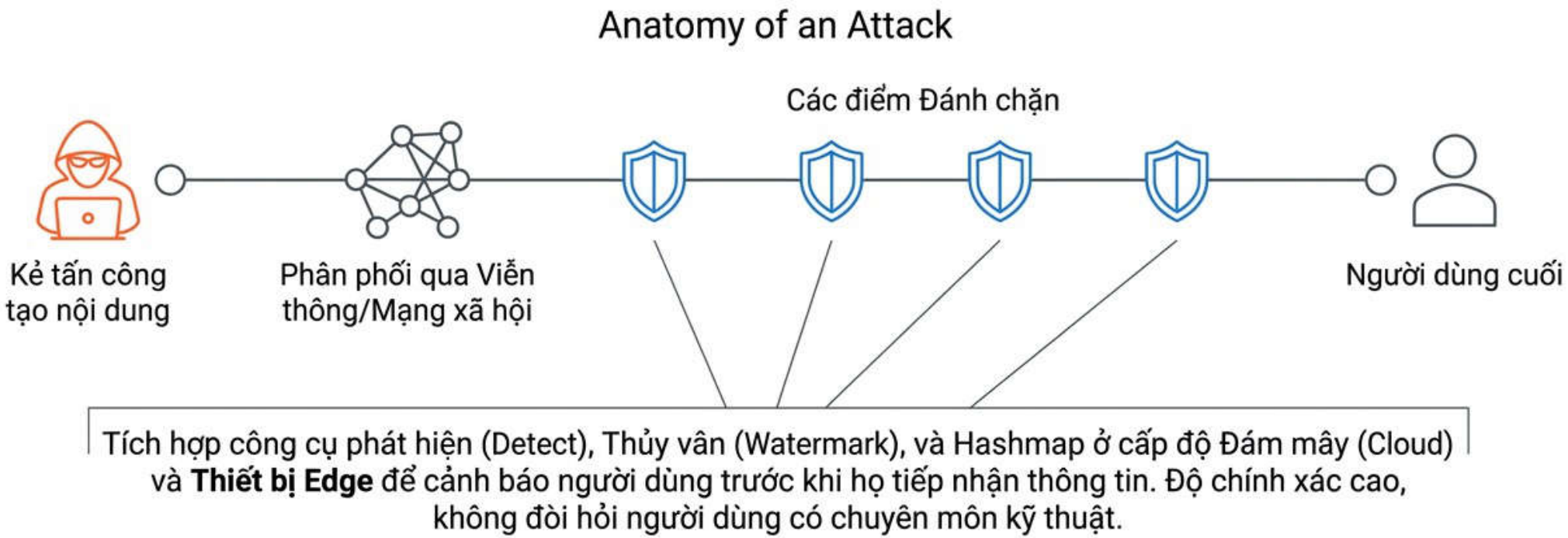


Dấu Hiệu Sinh Học (PPG)

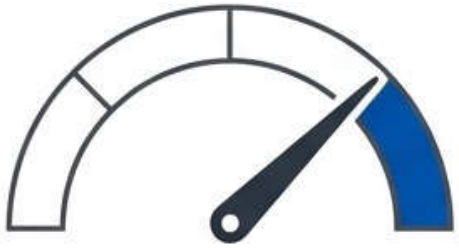
Deepfake hiện tại rất khó sao chép tín hiệu sinh học. Thuật toán phân tích sự thay đổi màu da vi mô (vi tuần hoàn máu) theo nhịp tim để phân biệt người thật và khuôn mặt do AI tổng hợp.

Tuyến 2 | DeepMedia: Đánh Chặn Đa Phương Thức

Nền tảng DeepID. Phân tích đồng thời nhiều loại dữ liệu (Hình ảnh, Video, Âm thanh) thay vì chỉ một.

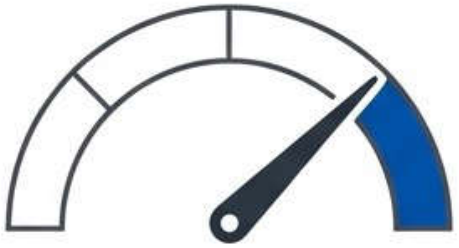


Tuyến 2 | CAICT & China Mobile: Tiêu Chuẩn Hóa Đánh Giá



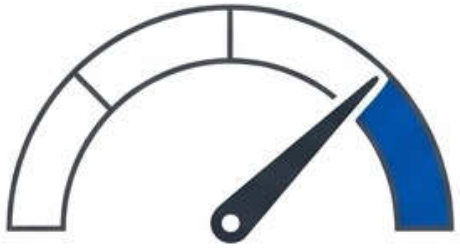
ACC (Độ chính xác)

Tỷ lệ thuật toán đoán đúng (Thật hay Giả).



AUC (Hiệu suất phân loại)

Khả năng phân tách rõ ràng giữa nội dung thật và giả ở nhiều ngưỡng khác nhau.



AP (Độ chính xác trung bình)

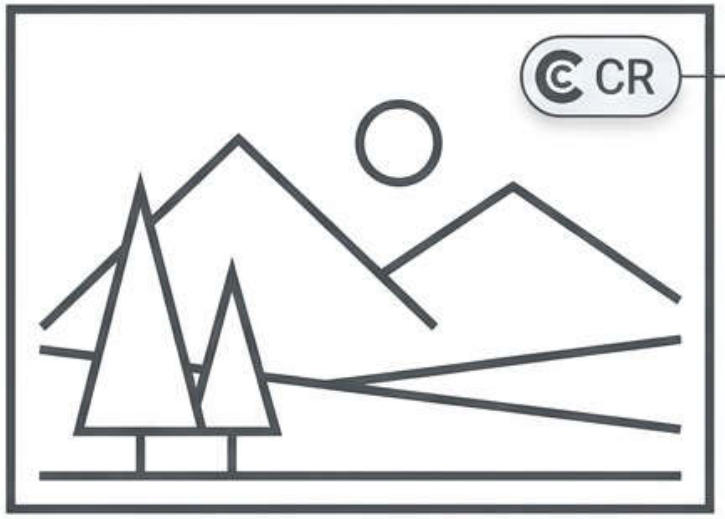
Khả năng phát hiện nhiều loại/phong cách giả mạo khác nhau.

Thử Thách Khái Quát Hóa (Generalization)



Thuật toán thường 'bó tay' trước các công cụ AI mới (như Sora). Cần cải thiện khả năng thích ứng của mô hình để phát hiện các kiểu giả mạo chưa từng có trong dữ liệu huấn luyện.

Tuyến 3 | C2PA: "Nhãn Thành Phần" Cho Kỹ Thuật Số



Content Credentials (C2PA)

- Do Adobe, Microsoft và các đối tác phát triển. Là một siêu dữ liệu (metadata) chống giả mạo được đính kèm vào tệp.
- Chức năng: Trả lời câu hỏi: Ai tạo ra? Tạo bằng công cụ gì (AI hay máy ảnh thật)? Đã qua chỉnh sửa ở đâu?
- Tạo thành một "chuỗi lịch sử" (provenance graph) minh bạch từ lúc sinh ra đến lúc phân phối.

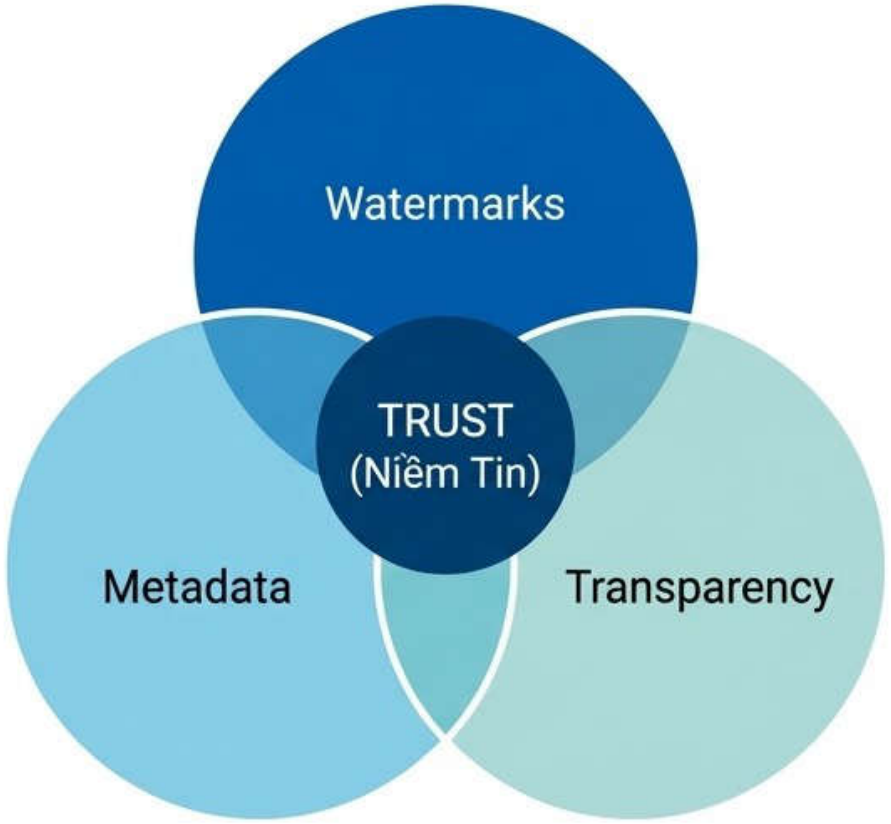
Khung So Sánh: 3 Công Cụ Xác Thực Cốt Lõi

	Thủy Vân Số (Watermarking)	Siêu Dữ Liệu (Secure Metadata)	Dấu Vân Tay (Fingerprinting)
Cách Hoạt Động	Nhúng thông tin ẩn trực trực tiếp vào điểm ảnh/âm thanh.	Gắn nhãn lịch sử (manifest) đi kèm tệp tin.	Tạo mã băm (Hash) độc nhất lưu trên cơ sở dữ liệu.
Đặc Điểm Cốt Lõi	Chống lại việc cắt ghép ảnh, thêm nhiễu âm thanh.	Có thể bị xóa khi chụp màn hình (screenshot), cần chữ ký mã hóa.	Không can thiệp vào file gốc, miễn nhiễm với việc 'xóa dữ liệu'.

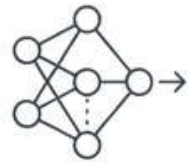
🔒 Không công cụ nào là hoàn hảo tuyệt đối. Một hệ thống an toàn cần kết hợp cả ba.

Tuyến 3 | Tiêu Chuẩn Toàn Cầu & Vòng Tròn Niềm Tin

The Trust Triad



SenseTime & Thủy Vân AI



Sử dụng mạng nề sâu (deep neural networks) để tạo thủy vân vô hình, chịu được các phép biến đổi ảnh phức tạp.

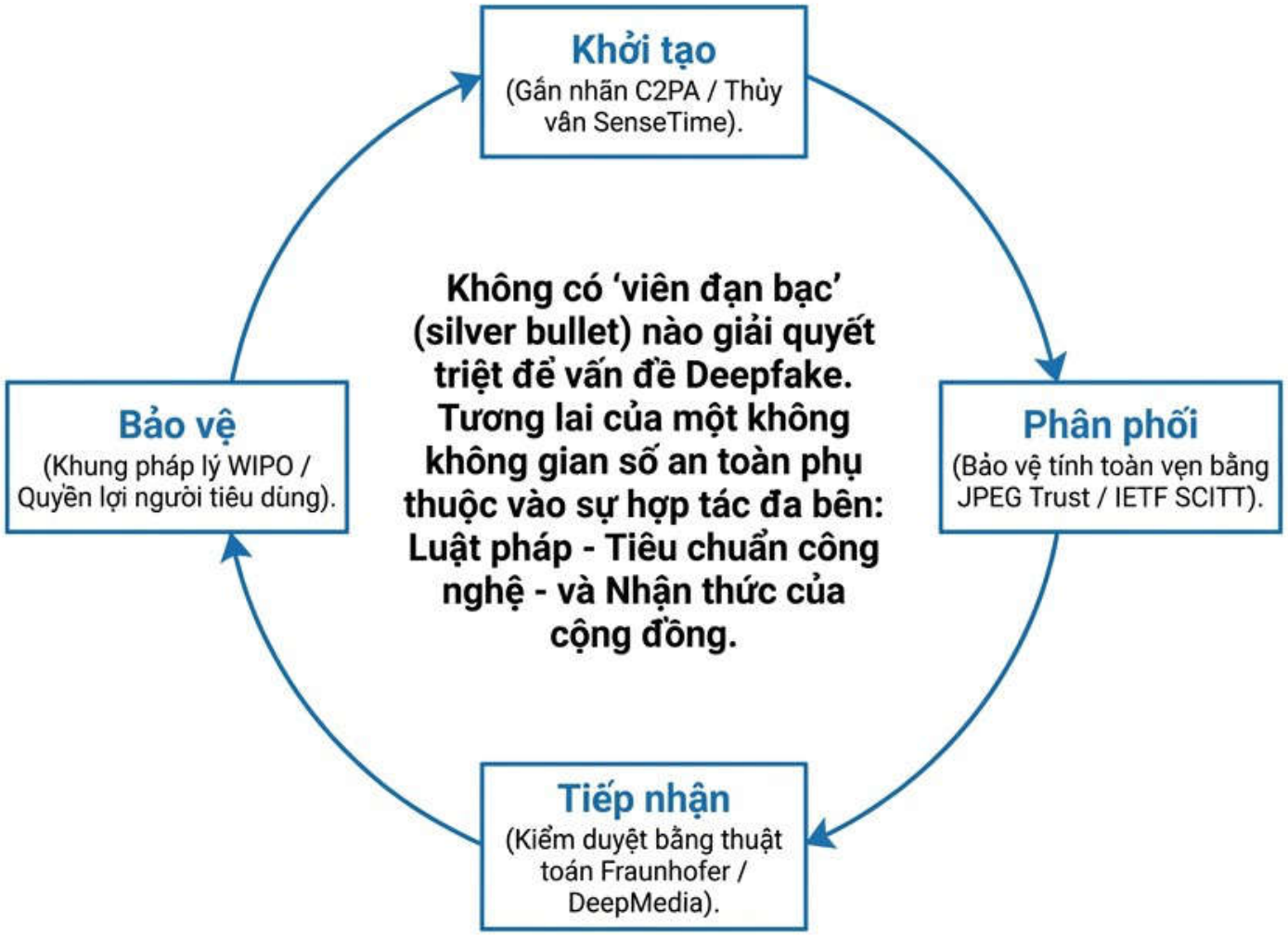
IETF SCITT

Đảm bảo tính minh bạch, lưu trữ lịch sử bằng công nghệ sổ cái phân tán (tránh xé lẻ hoặc lùi ngày dữ liệu).

ITU (X.1280/X.1220) & JPEG Trust

Tiêu chuẩn hóa chữ ký số và xác thực máy chủ để bảo vệ an toàn cho cả thuật toán AI lẫn dữ liệu người dùng.

Tổng Kết: Hệ Sinh Thái Phòng Thủ Đa Bên



Summary

- Giới thiệu các khái niệm cơ bản
  - An toàn thông tin
  - Các tiêu chuẩn về An toàn thông tin (ISO và TCVN)
  - Vấn đề "đạo đức số"
  - Vấn đề "deepfake"
  - Một vài luật ở Việt Nam




FPT Education
FPT POLYTECHNIC
Thank you
TIN HỌC VĂN PHÒNG QUỐC TẾ THEO CHUẨN ICDL
Syllabus 5 - Office 2007
LUẬT KINH TẾ
KỸ THUẬT SOẠN THẢO VÀ TRÌNH BÀY VĂN BẢN