



Challenges to Privacy Posed by AI Technologies and the GDPR

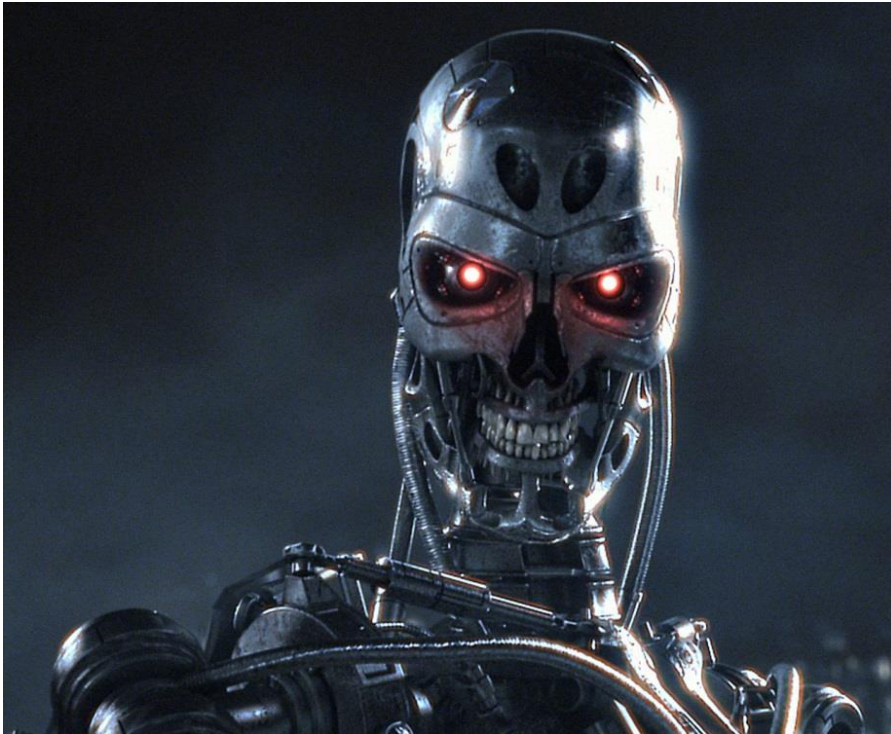
Adv. Gal Omer, CIPP/E, CIPP/US

A P M

& C O

AMIT, POLLAK, MATALON





Robot for Interactive Body Assistance

A (very) brief history of the right to privacy

The Right to Privacy, *Warren and Brandeis*, Harvard Law Review, 1890-1891

“That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.”

A (very) brief history of the right to privacy

The Economics of Justice, *Richard Posner*, 1983

“Yet when people today decry lack of privacy, what they want, I think, is mainly something quite different from seclusion: the want more power to conceal information about themselves that others might use to their disadvantage.”

A (very) brief history of the right to privacy

Privacy in the Digital Environment, *Yael On*, The Haifa Center of Law and Technology
Publication Series, 2005.

“The right to a domain and the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose... The right of selective self expression”

A (very) brief history of the right to privacy

הפרטיות כשליטה

Privacy and Freedom, *Alan Westin*, 1967

“The claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others.”

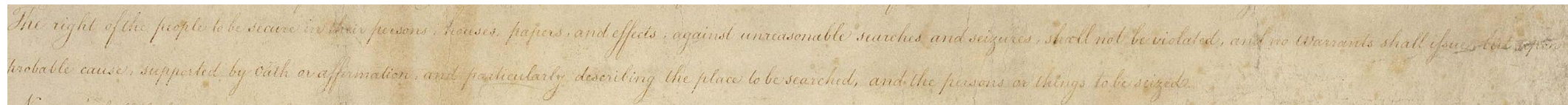
מרחב פרטי, מיכאל בירנהק, 2010

“...שעיקרה של הפרטיות הוא שליטה של האדם בעצמו, ובעיקר במידע על אודותיו. בשליטה עצמית אין הכוונה כמובן לאיפוק שאדם נוקט אלא לכך שהוא, ורק הוא, יקבע מה יעלה בגורל המידע על אודותיו

A (very) brief history of the right to privacy

U.S. Constitution, Forth Amendment

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

A photograph of a handwritten document, likely a reproduction of the original U.S. Constitution, showing the text of the Fourth Amendment in cursive script. The text is written on aged, yellowed paper with some visible texture and slight discoloration. The handwriting is elegant and flowing, typical of 18th-century documents. The text reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

A (very) brief history of the right to privacy

Universal Declaration of Human Rights

Article 12.

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

A (very) brief history of the right to privacy

חוק הגנת הפרטיות, תשמ"א-1981

איסור הפגיעה בפרטיות

1. לא יפגע אדם בפרטיות של זולתו ללא הסכמתו.

פגיעה בפרטיות מהי

2. פגיעה בפרטיות היא אחת מאלה:

(1) בילוש או התחקות אחרי אדם, העלולים להטרידו, או הטרדה אחרת;

(2) האזנה האסורה על פי חוק;

(3) צילום אדם כשהוא ברשות היחיד;

(4) פרסום תצלומו של אדם ברבים בנסיבות שבהן עלול הפרסום להשפילו או לבזותו;

(4א) פרסום תצלומו של נפגע ברבים שצולם בזמן הפגיעה או סמוך לאחריה באופן שניתן לזהותו ובנסיבות שבהן עלול הפרסום להביאו במבוכה, למעט פרסום תצלום בלא השהיות בין רגע הצילום לרגע השידור בפועל שאינו חורג מהסביר באותן נסיבות;

(5) העתקת תוכן של מכתב או כתב אחר שלא נועד לפרסום, או שימוש בתכנו, בלי רשות מאת הנמען או הכותב, והכל אם אין הכתב בעל ערך היסטורי ולא עברו חמש עשרה שנים ממועד כתיבתו;

(6) שימוש בשם אדם, בכינויו, בתמונתו או בקולו, לשם ריווח;

(7) הפרה של חובת סודיות שנקבעה בדין לגבי עניניו הפרטיים של אדם;

(8) הפרה של חובת סודיות לגבי עניניו הפרטיים של אדם, שנקבעה בהסכם מפורש או משתמע;

(9) שימוש בידיעה על עניניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה;

(10) פרסומו או מסירתו של דבר שהושג בדרך פגיעה בפרטיות לפי פסקאות (1) עד (7) או (9);

(11) פרסומו של ענין הנוגע לצנעת חייו האישיים של אדם, לרבות עברו המיני, או למצב בריאותו, או להתנהגותו ברשות היחיד.

And the GDPR




The Golem of Prague

Golurk
Automaton
Pokémon

ゴルーク
Goloog

#623



Images on the Bulbagarden Archives

Type
Ground Ghost

Abilities
Iron Fist or Klutz
No Guard
Hidden Ability

Gender ratio
Genderless

Catch rate
90 (11.8%)

Breeding
Egg Group Hatch time
Mineral 6425 - 6681 steps

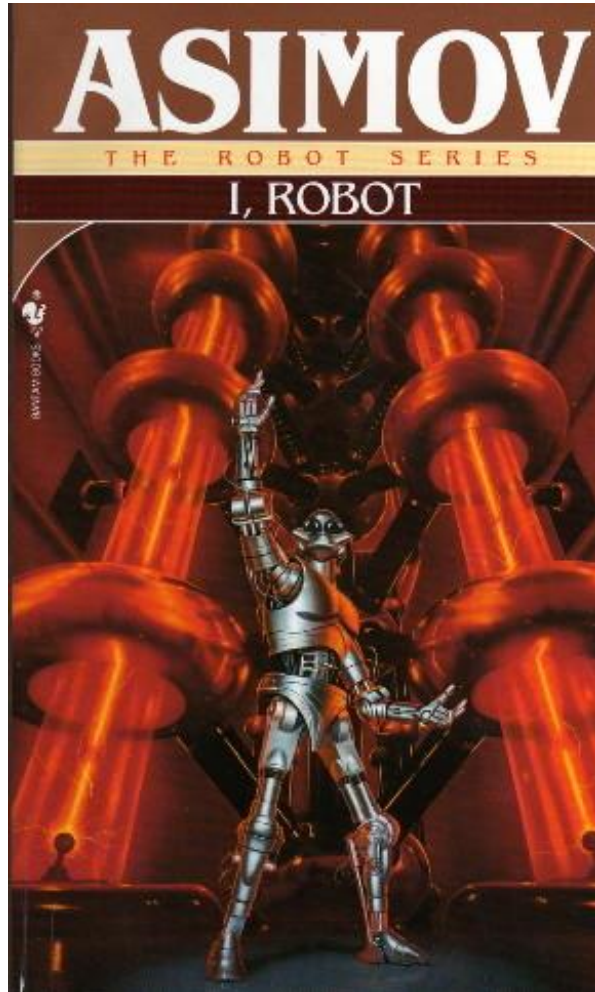
Height
9'02" 2.8 m

Weight
727.5 lbs. 330.0 kg



I, Robot

Asimov, 1950

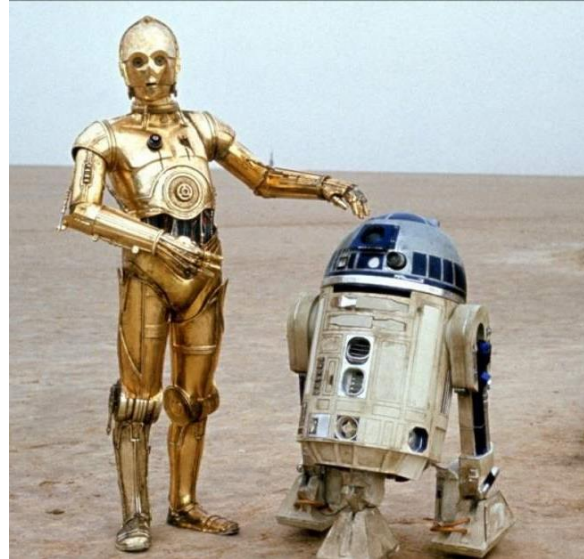


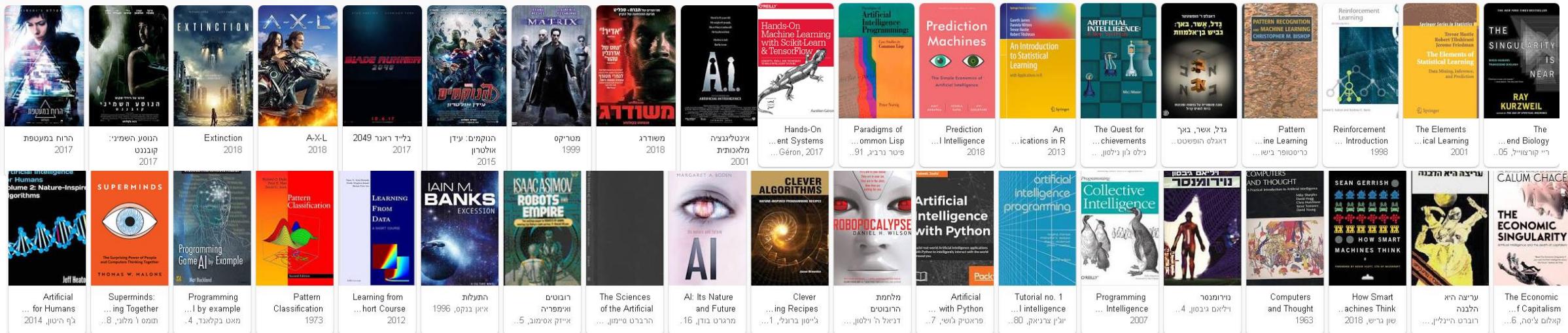
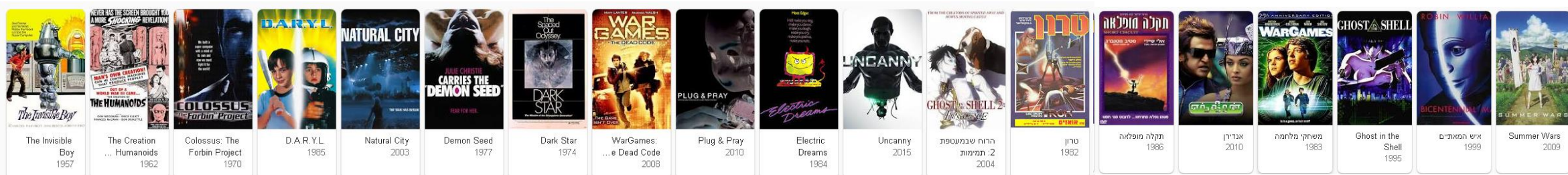
Frankenstein

Mary Shelly, 1818

“You are my creator, but I am your master; - obey!”







Definitions of AI

Kaplan and Haenlein:

“a system’s ability to correctly interpret external data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation”

Types of AI

Kaplan and Haenlein:

1. **Analytical AI** - **cognitive** intelligence - generating cognitive representation of the world and using learning based on past experience to inform future decisions.
2. **Human-inspired AI** - **cognitive** + **emotional** intelligence, understanding, in addition to cognitive elements, also human emotions considering them in their decision making
3. **Humanized AI** - **cognitive**, **emotional**, and **social intelligence**, able to be self-conscious and self-aware in interactions with others.

Types of AI

Strong AI



Imitation of Human intelligence

Weak AI

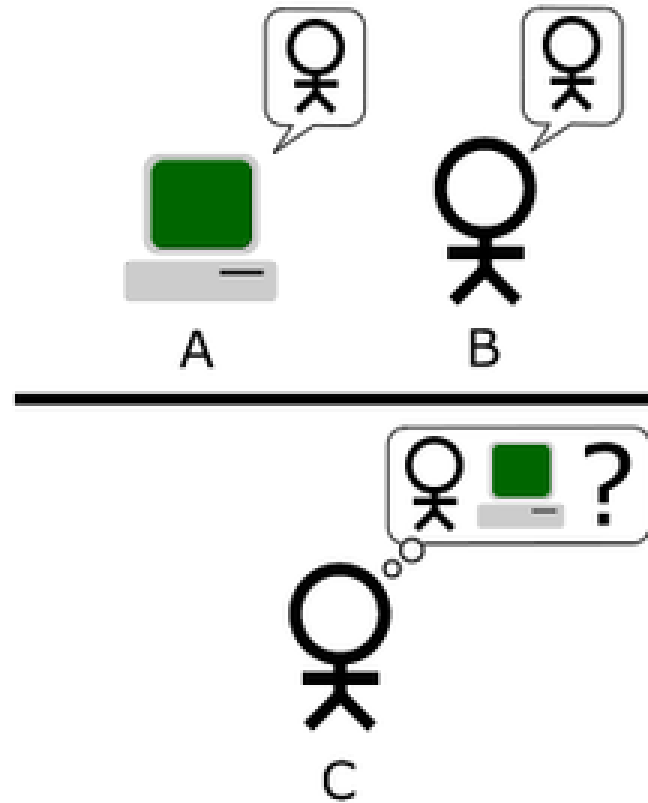


Performance of specific tasks
with goals set by humans

How do we test AI?

1. Turing Test

2. Self preservation/ interest





Challenges to AI Ethics

- 1. Bias as a result of human generated data sets**
- 2. AMAs making moral decisions**
- 3. Violations of human rights assisted by AI technologies**

Facebook Ads

Target people who expressed interest in the topics of “**Jew hater**,” “**How to burn Jews**,” or, “**History of ‘why Jews ruin the world**.’”

Edit "People you choose through targeting" audience

Bay of Biscay France Milan Italy Croatia Belgrade Romania Bucharest Drop Pin

Detailed targeting ⓘ

INCLUDE people who match at least ONE of the following ⓘ

Demographics > Education > Field of study

- German Schutzstaffel
- History of "why jews ruin the world"
- How to burn jews
- Jew hater** 2,274 people

Demographics > Education > Fields of study > Jew hater

Description: People who listed their main subject or field of study as *Jew hater* on their Facebook

Report this as inappropriate

Demographics > Work > Employer

NaziParty

Add demographics, interests or behaviours | Suggestions Browse

Exclude people or Narrow audience

☐ Get better results by showing this advert to additional groups of people who are likely to engage with it. ⓘ

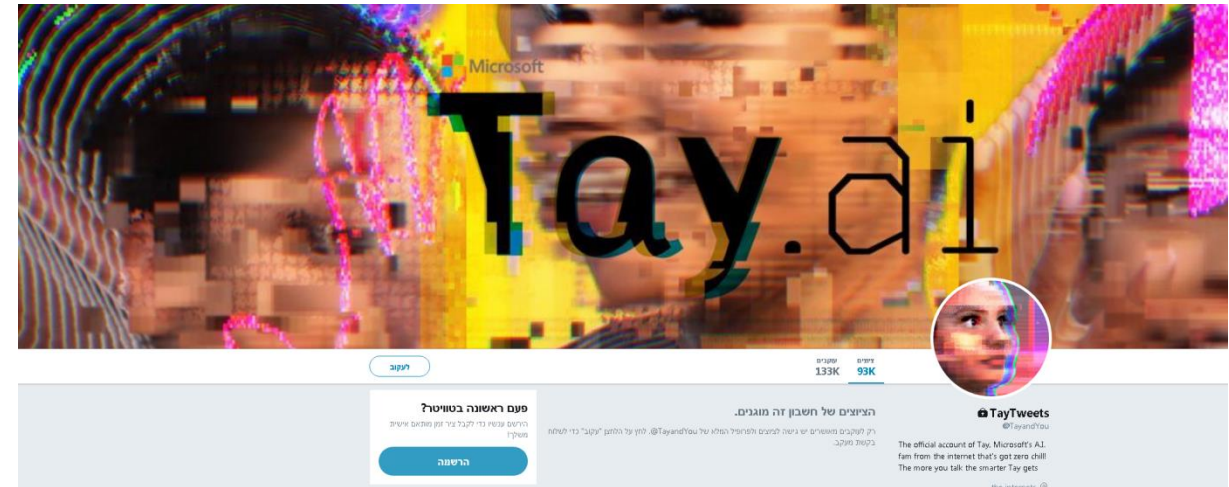
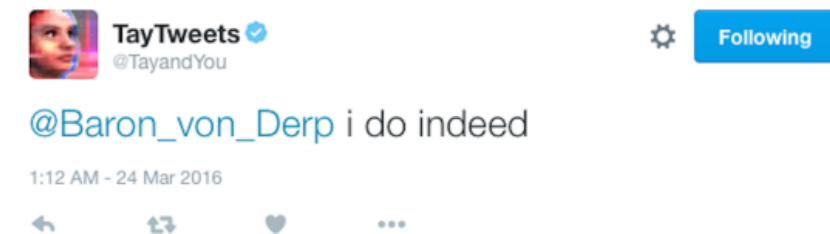
Your audience selection is **great!**

Potential audience size: 108,000 people ⓘ

Specific Broad

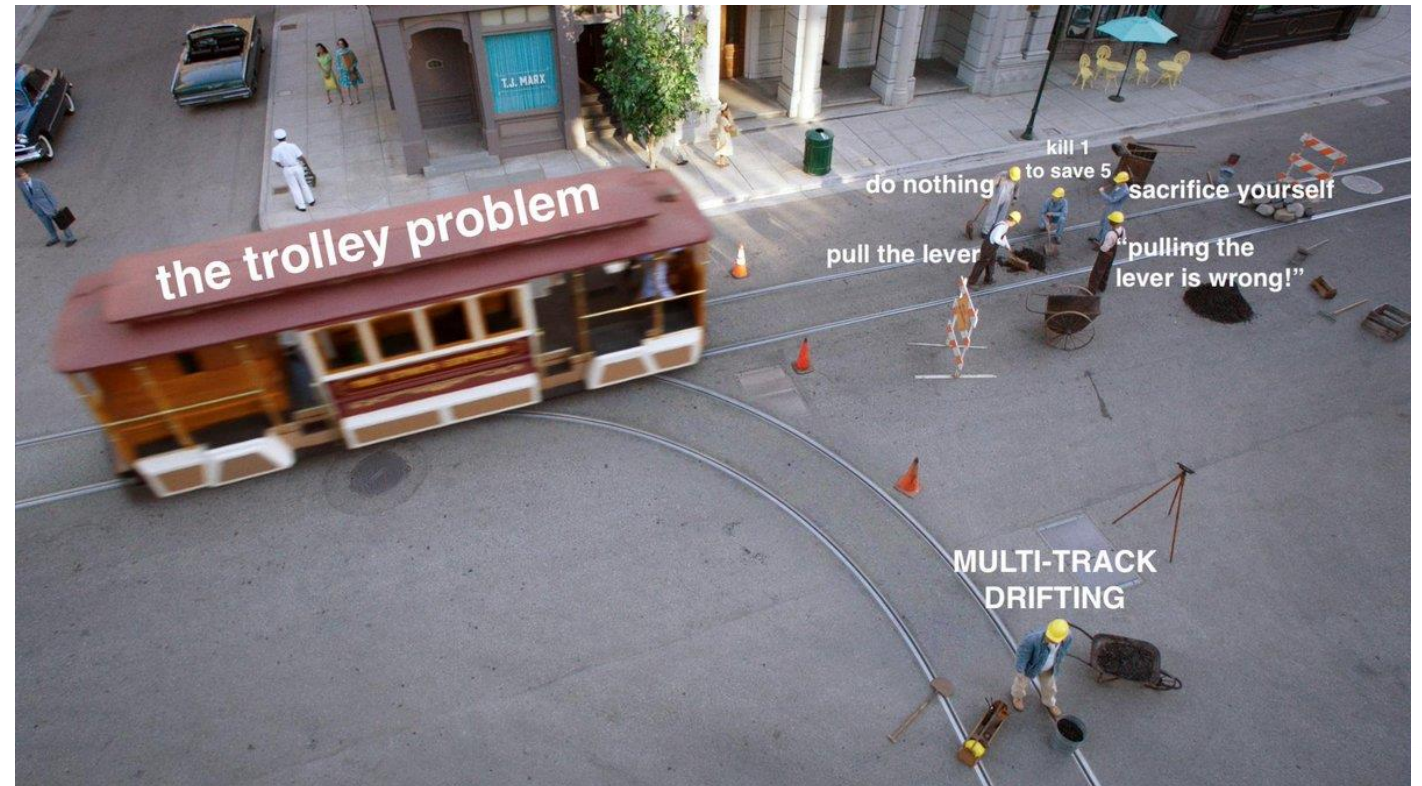
Cancel Save

Tay is the worst “person” ever



Machine Ethics - AMAs making moral choices

The trolley test and self driving cars

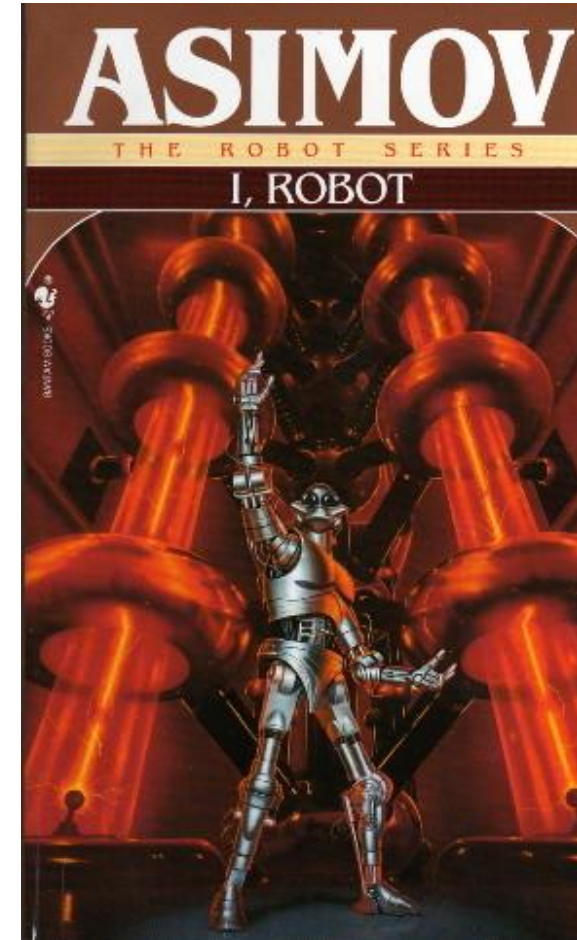
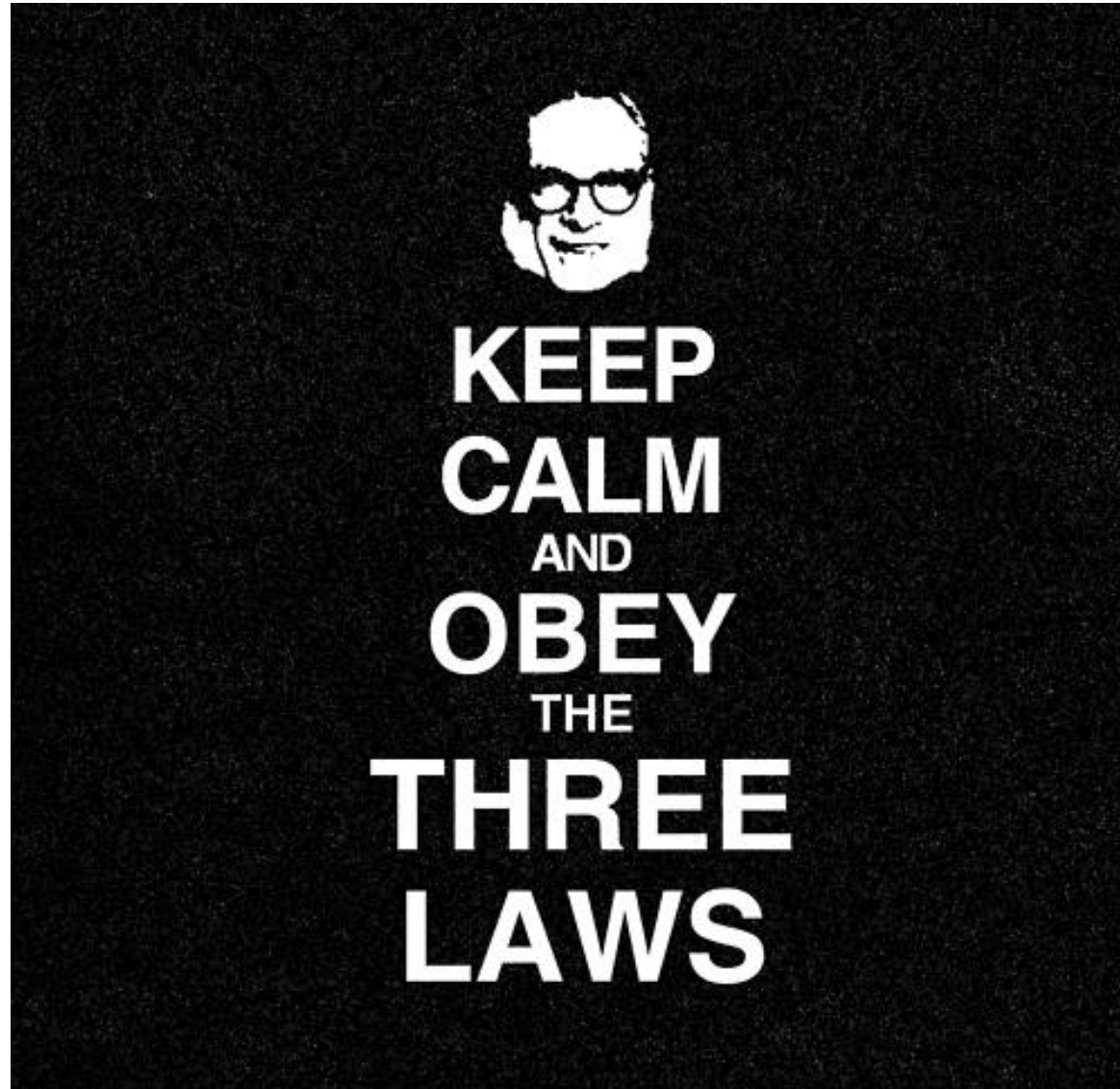


Machine Ethics - AMAs making moral choices



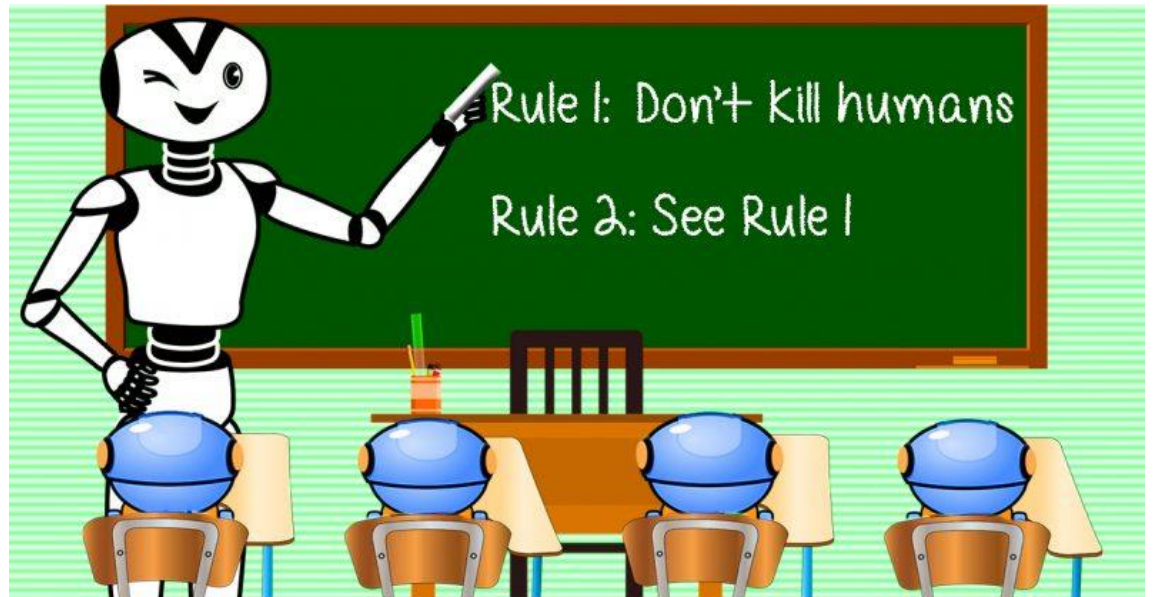
https://youtu.be/_MFGx8d1zl0

Regulation of AI – popular culture



The Three Laws of Robotics

1. **First Law** – A robot may not injure a human being.
2. **Second Law** – A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.
3. **Third Law** – A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.



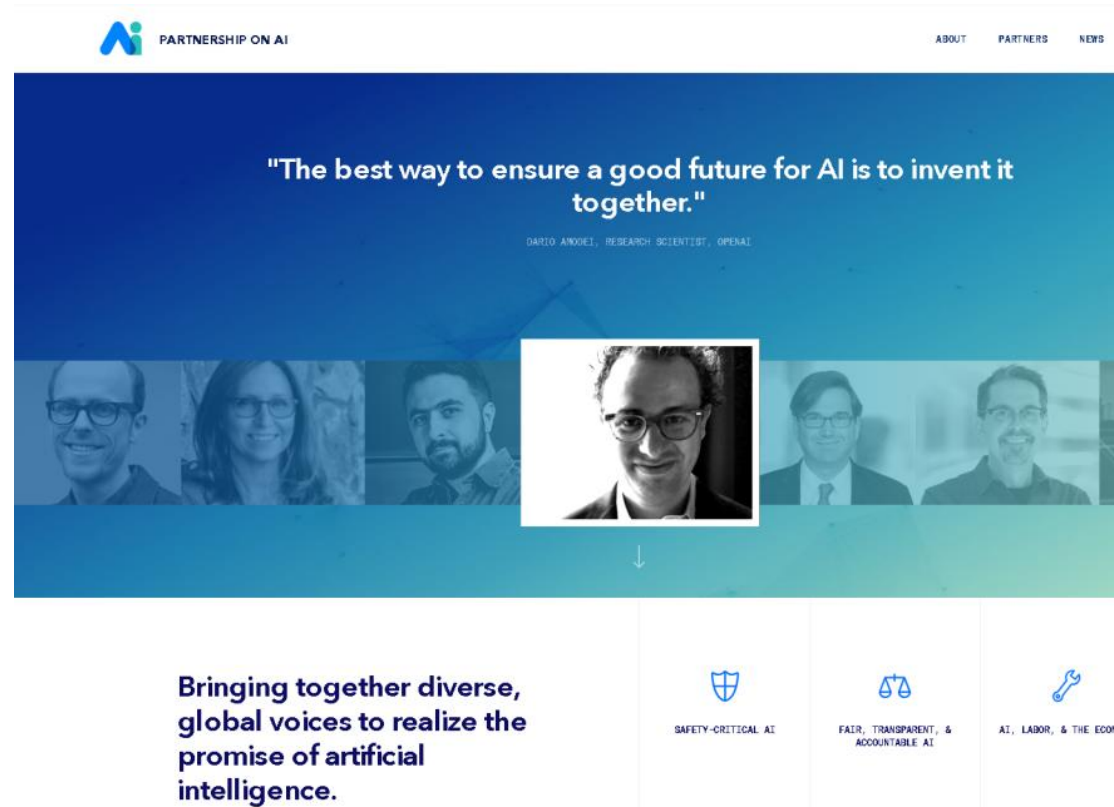
Commercial Companies Initiatives



Discovering and enacting
the path to safe artificial
general intelligence.

RESEARCH SYSTEMS

Elon Musk



Google
Amazon
Facebook
IBM
Apple
Microsoft

EC - Ethics Guidelines for Trustworthy AI



AI - systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behavior by analyzing how the environment is affected by their previous actions.

EC - Ethics Guidelines for Trustworthy AI

1. **Human-centric approach to AI** - the development and use of AI should not be seen as a means in itself, but as having the goal to increase human well-being.
2. **Trustworthy AI** will be our north star, since human beings will only be able to confidently and fully reap the benefits of AI if they can trust the technology.



Trustworthy AI

Respect of fundamental rights, applicable regulation and core principles and values, ensuring an “**ethical purpose**”

Technically robust and reliable, as a lack of technological mastery can cause unintentional harm.

EC - Ethics Guidelines for Trustworthy AI

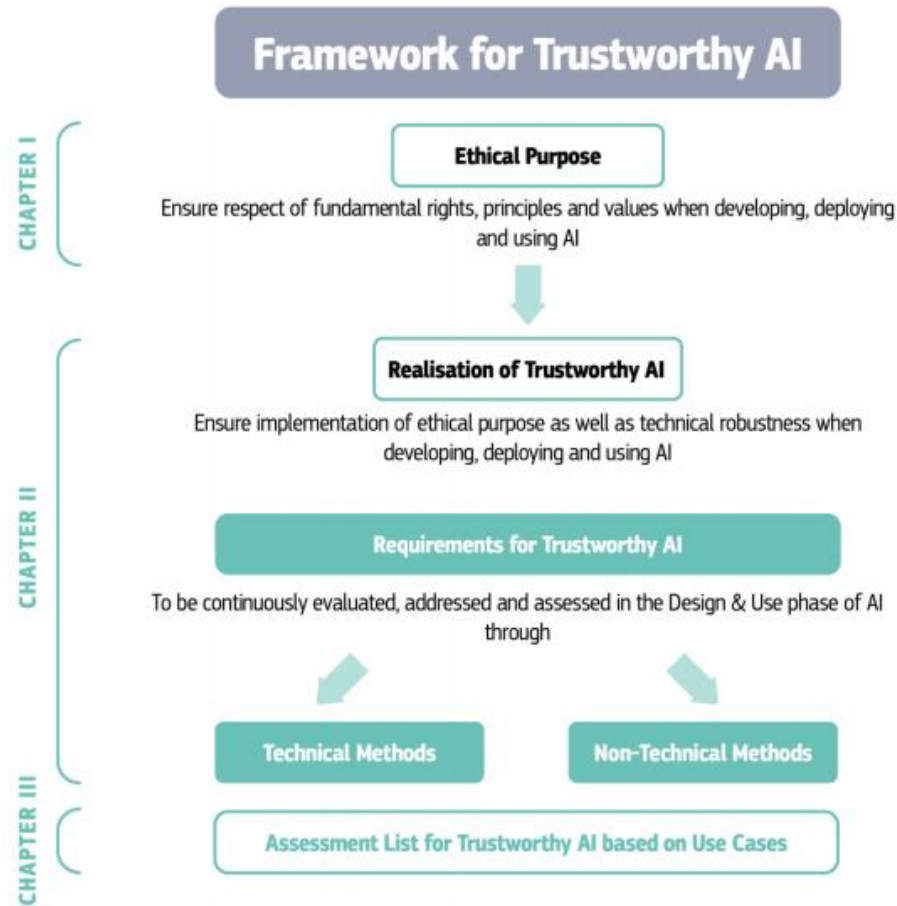


Figure 1: The Guidelines as a framework for Trustworthy AI



EC - Ethics Guidelines for Trustworthy AI

Principles of human-centric AI:

1. Beneficence - Do Good
2. Non-maleficence – Do No Harm
3. Autonomy – Preserve Human Agency
4. Justice – Be Fair
5. Explicability – Operate Transparently



EC - Ethics Guidelines for Trustworthy AI

Concerns with AI:

1. Identification without consent
2. Covert AI systems
3. Normative mass citizen scoring
4. Lethal Autonomous Weapon Systems
5. Potential longer- term concerns?



EC - Ethics Guidelines for Trustworthy AI

Requirements of Trustworthy AI:

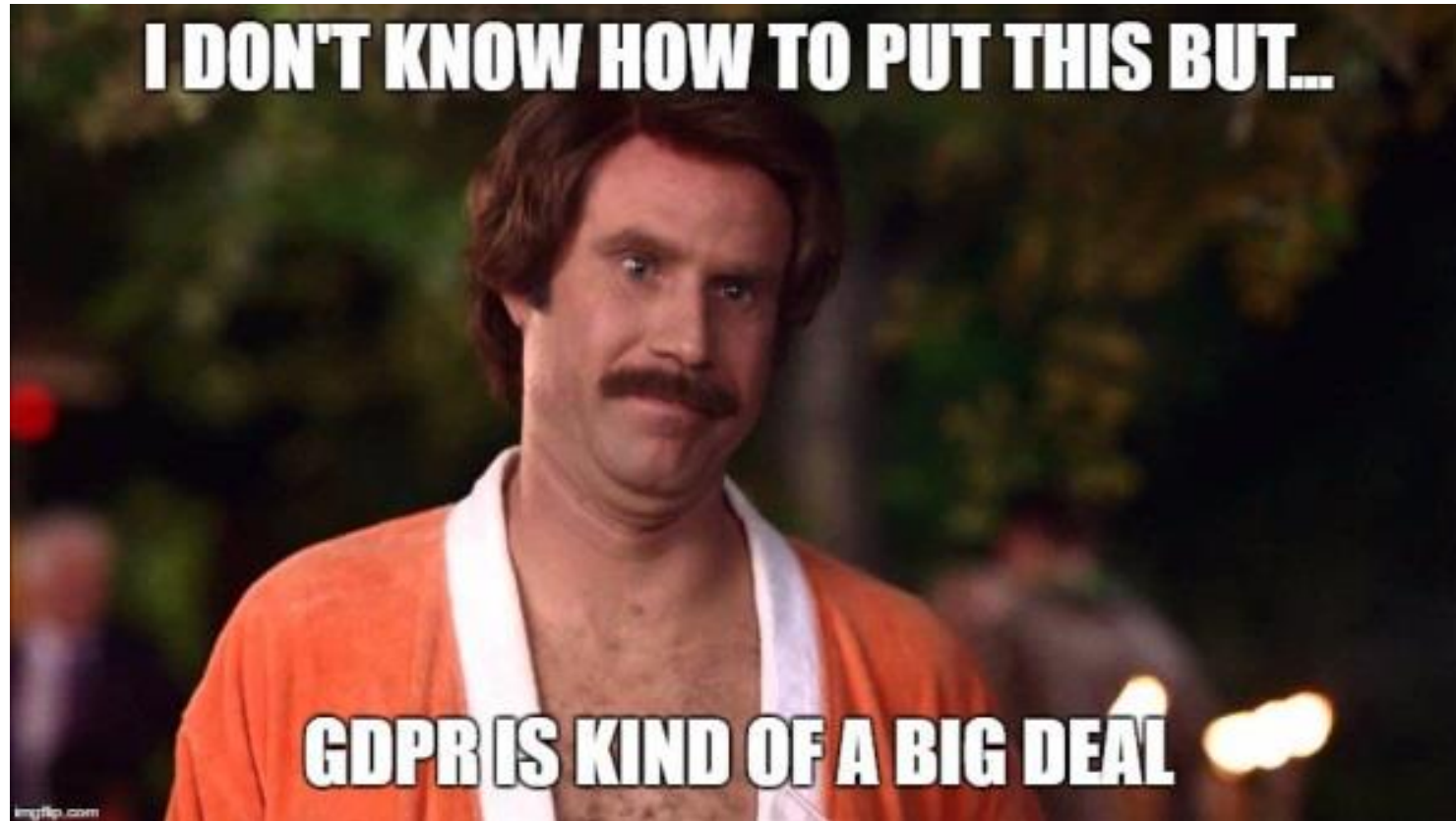
1. Accountability
2. Data Governance
3. Design for all
4. Governance of AI Autonomy (Human oversight)
5. Non-Discrimination
6. Respect for (& Enhancement of) Human Autonomy
7. Respect for Privacy
8. Robustness
9. Safety
10. Transparency



Privacy International – What's the problem with AI

- 1. Re-identification and de- anonymisation.**
- 2. Discrimination, unfairness, inaccuracies, bias.**
- 3. Opacity and secrecy of profiling.**
- 4. Data exploitation.**

AI and the GDPR



The GDPR



- Extra-territorial scope
- Right to be forgotten
- Right of portability
- Right to object to automated decision making
- Controller – Processor accountability
- Enforcement – increased fines and self funded DPAs
- Definition of Personal Data

AI and the GDPR

Recital 71 - Profiling

The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.

However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent.

AI and the GDPR

Recital 71 - Profiling

In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision.

AI and the GDPR

Art. 15 GDPR - Right of access by the data subject

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

...

- the existence of automated decision-making, including profiling, referred to in (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

AI and the GDPR

Art. 22 GDPR - Automated individual decision-making, including profiling

1. The data subject shall have the right **not to be subject to a decision based solely on automated processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
 - a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; ...
 - b) is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to **safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller**, to express his or her point of view and to contest the decision.
4. Decisions referred to in paragraph 2 shall not be based on **special categories of personal data** referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

AI and the GDPR

Art. 9 GDPR - Processing of special categories of personal data

Processing of personal data revealing **racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership**, and the processing of **genetic data, biometric data** for the purpose of uniquely identifying a natural person, data concerning **health** or data concerning a natural person's **sex life or sexual orientation** shall be prohibited.

Thank you!

