Ethical Aspects of Machine Learning (and AI)

Winter school "CAS ADS M6 Deep Learning"

Hotel Regina, Mürren

26.1.2022

Claus Beisbart

Claus.Beisbart@philo.unibe.ch

Aims of this lecture:

Raise awareness of ethical challenges related to machine learning

Discuss some challenges using methods and concepts from ethics

Aims of this lecture: conversation

Raise awareness of ethical challenges related to machine learning

Discuss some challenges using methods and concepts from ethics

Method

- 1. Start from your experience, views
- 2. Give input from philosophy
- 3. Discuss

Steps

1. Collect issues

2. Discuss one or two of them

Question for you

You are attending a winter school on ML. Using the competences that you get here, for which purposes do you want to use ML (in your job, studies ...)?

Question for you

What benefits (for society, humankind, ...) do such applications of ML promise in your view?

Philosophical input

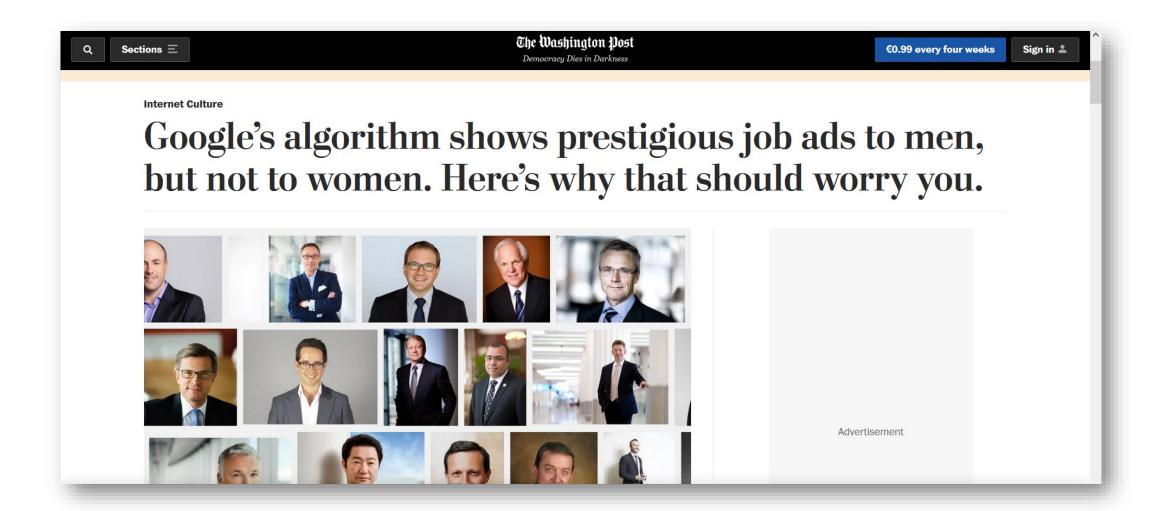
What benefits (for society, humankind, ...) do such applications of ML promise in your view?

Due to the condition in brackets, I was asking for an ethical evaluation.

Question for you

To what harms, risks or challenges (for society, humankind, ...) may such ML applications lead in your view?

Example 1



Example 2



Figure 1. (Left) Location of the crash on northbound Mill Avenue, showing the paths of the pedestrian in orange and of the Uber test vehicle in green. (Right) Postcrash view of the Uber test vehicle, showing damage to the right front side.

image: NTSB

Philosophical input: overview of debates



Entry Contents

Bibliography

Back to Top

Academic Tools

Friends PDF Preview

Author and Citation Info

Ethics c Robotic

First published Th

• 2. Main Debates

- 2.1 Privacy & Surveillance
- 2.2 Manipulation of Behaviour
- 2.3 Opacity of AI Systems
- 2.4 Bias in Decision Systems
- 2.5 Human-Robot Interaction
- 2.6 Automation and Employment
- 2.7 Autonomous Systems
- 2.8 Machine Ethics
- 2.9 Artificial Moral Agents
- 2.10 Singularity

Artificial intelligence (AI) and robotics are digital technologies that will have significant impact on the development of humanity in the near future. They have raised fundamental questions about what we should do with these systems, what the systems themselves should do, what risks they involve, and how we can control these.

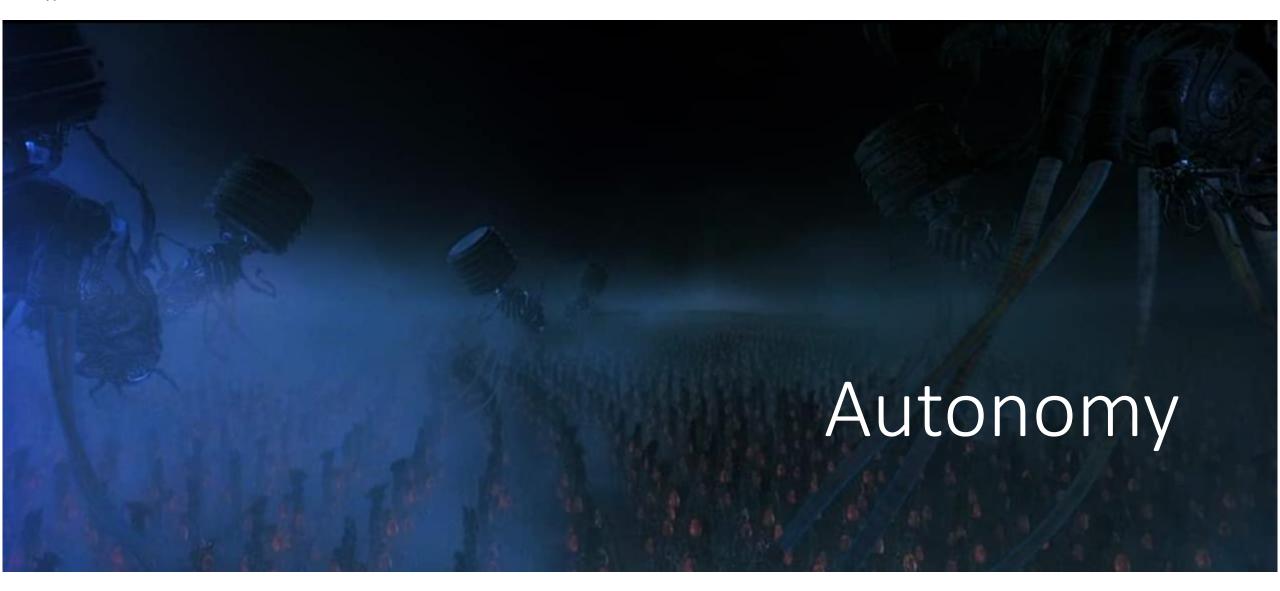
Müller, V. C., <u>Ethics of Artificial</u>
<u>Intelligence and Robotics</u>, *The Stanford Encyclopedia of Philosophy* (Summer 2021 Edition), Edward N. Zalta (ed.).

Getting started



Logo: Wachowski Brothers

"The Matrix"



Wachowski Brothers 14

2010

«Eine einzige Simulation genügte, um in die Schicksale von Millionen von Menschen einzugreifen und Europa lahmzulegen.

Plötzlich werden alle zu Zuschauern: die Fluggäste, die Piloten, die Airlines, der Wetterdienst, die Behörden. Die "human response", die menschliche Antwort auf die Maschine, ist nicht mehr möglich, weil auch in den menschlichen Entscheidungsgruppen ein Programm von Befehlen, Verördnungen und Routinen abläuft.»

Frank Schirrmacher



Does Al pose a threat to human autonomy?

Philosophical input: concept

Gr. autos: self **autonomy**Self determination Heteronomy

Being determined by others

Gr. nomos: law

Philosophical input: Immanuel Kant



(1724 - 1804)

"Autonomie des Willens ist die Beschaffenheit des Willens, dadurch derselbe ihm selbst (unabhängig von aller Beschaffenheit der Gegenstände des Wollens) ein Gesetz ist."

Grundlegung zur Metaphysik der Sitten, Akademie-Ausgabe IV, 440

Philosophical input: Kant's ethics of autonomy



(1724 - 1804)

"Autonomie ist also der Grund der Würde der menschlichen und jeder vernünftigen Natur."



"Die Handlung, die mit der Autonomie des Willens zusammen bestehen kann, ist erlaubt; die nicht damit stimmt, ist unerlaubt."

Philosophical input: ethics of medicine

Respect for autonomy:

- 1. "Tell the truth.
- 2. Respect the privacy of others.
- 3. Protect confidential information.
- 4. Obtain consent for interventions with patients.
- 5. When asked, help others to make decisions."
 - T. L. Beauchamp & J. F. Childress, Principles of Biomedical Ethics, New York 2001⁵, 65



Question for you

How do you think may ML/Al applications impact on human autonomy?

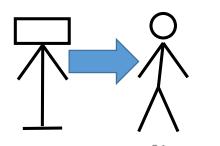
Philosophical input: 2 routes to problems



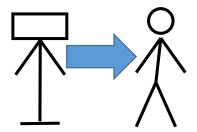
Al applications take decisions

Where is the problem?

Al applications influence human decisions



Philosophical input: concepts



Sorts of influence:

- Conditioning
- Nudging
- Herding

Der autonome Mensch im Zeitalter des Digitalen Wandels

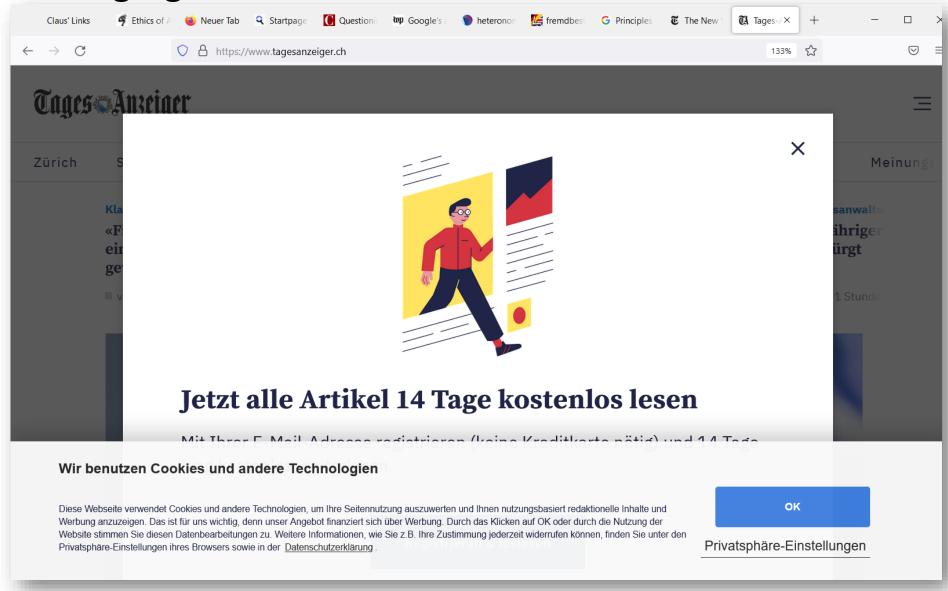
Sabine Theresia Köszegi

Einleitung

Seit etwa 50 Jahren setzen Menschen modell- und datenbasierte Unterstützungssysteme zur Entscheidungsfindung – vorwiegend bei komplexen Entscheidungsproblemen – ein. Menschen ha-

Cf.. Köszegi, S. T., Der autonome Mensch im Zeitalter des Digitalen Wandels, in: Hengstschläger, Markus/Rat für Forschung und Technolgieentwicklung (Hrsg.), Digitaler Wandel und Ethik, Wien 2020, 62-86

Example: nudging



www.tagesanzeiger.ch 23

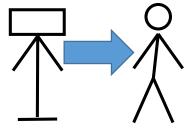
Philosophical input: concept

Not every influence on human decisions is bad.

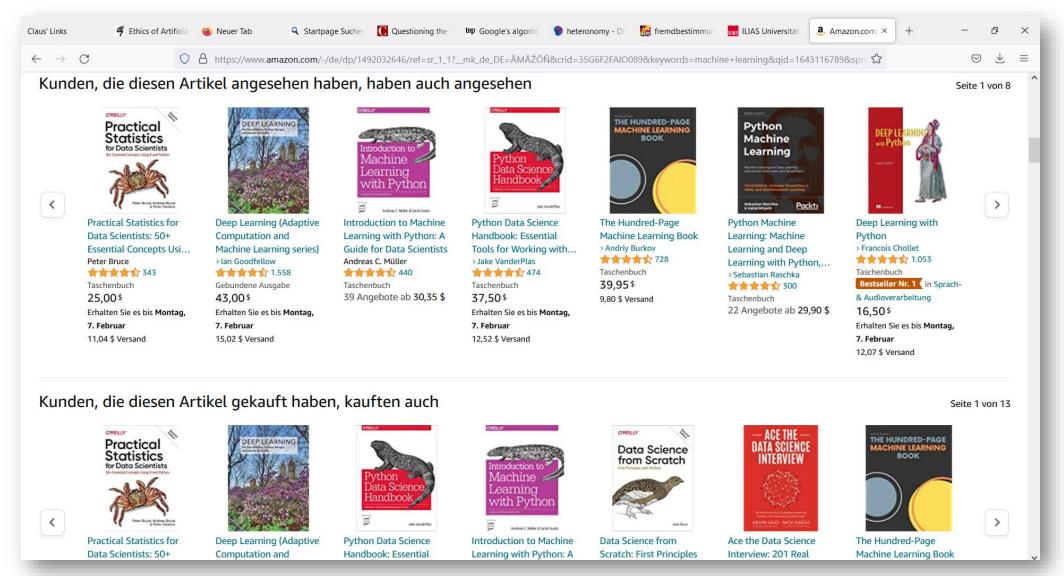
One problem:

Manipulation

"(disapproving) behaviour that controls or influences somebody/something, often in a dishonest way so that they do not realize it"

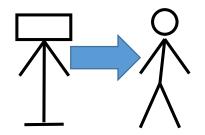


Example: recommender system



www.amazon.com 25

Your views



What would be an example of problematic manipulation?

- There is a tendency to recommend expensive books.
- There is a tendency to recommend books that other customers have bought.
- There is a tendency to recommend books that fit the interests of the user.
- There is a tendency to recommend books of a specific political persuasion.
- There is a tendency to recommend books from authors with diverse backgrounds.
- Only objective criteria are used to create recommendations, e.g. books that are about a similar topic.

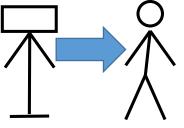
Philosophical input: a general idea



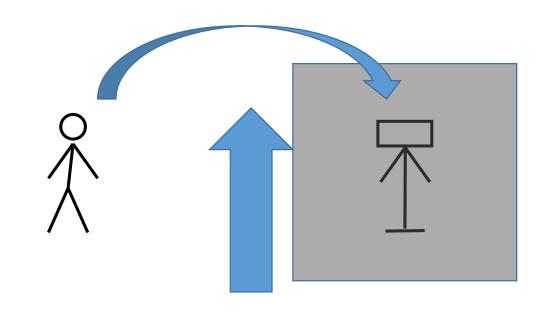
Al applications take decisions

No problem, if authorization by "informed consent"

Al applications influence human decisions



Philosophical input: informed consent



Opacity

Rational basis: information

Philosophical input: opacity

OPENING THE BLACK BOX OF DEEP NEURAL NETWORKS VIA INFORMATION

Opening the black box of Deep Neural Networks via Information

Ravid Schwartz-Ziv

RAVID.ZIV@MAIL.HUJI.AC.IL

Edmond and Lilly Safra Center for Brain Sciences The Hebrew University of Jerusalem Jerusalem, 91904, Israel

Naftali Tishby*

TISHBY@CS.HUJI.AC.IL

School of Engineering and Computer Science and Edmond and Lilly Safra Center for Brain Sciences The Hebrew University of Jerusalem Jerusalem, 91904, Israel

Editor: ICRI-CI

Abstract

Despite their great success, there is still no comprehensive theoretical understanding of learning with Deep Neural Networks (DNNs) or their inner organization. Previous work [Tishby and Zaslavsky (2015)] proposed to analyze DNNs in the *Information Plane*; i.e., the plane of the Mutual

"Despite their great success, there is still no comprehensive understanding of the optimization process or the internal organization of DNNs, and they are often criticized for being used as mysterious "black boxes"" p. 2

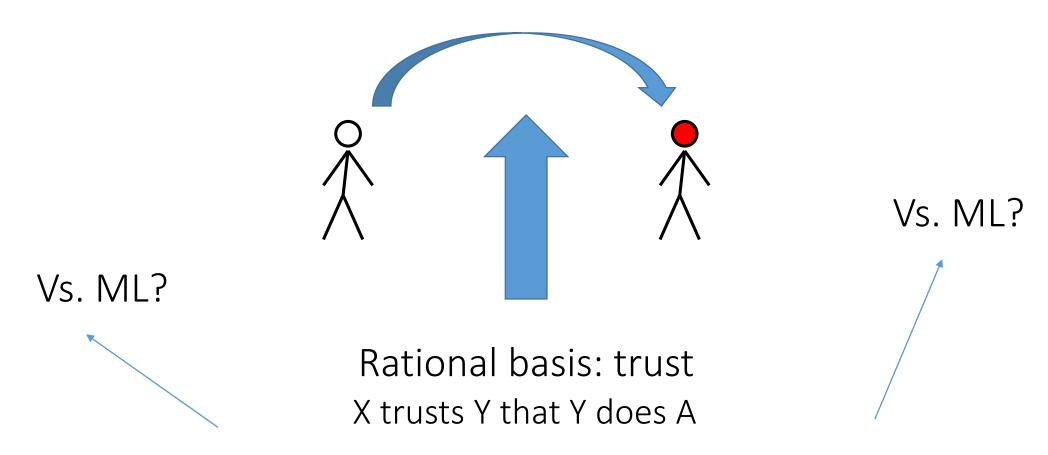
Shwartz-Ziv, R., & Tishby, N. (2017). Opening the black box of Deep Neural Networks via Information.

ArXiv:1703,00810.

Question for you

Is the opacity of ML models special? If so why?

Philosophical input: Trust



1. X thinks that Y does A. 2. X thinks that Y does so for goodwill.

Question for you

Under which conditions application would you trust an ML application?

Philosophical input

Selected conditions:

- Human agency and oversight
- Transparency
- Accountability



Brussels, 8.4.2019 COM(2019) 168 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Communication: Building Trust in Human Centric Artificial Intelligence

Philosophical input: human agency and oversight

"Human oversight helps ensuring that an AI system does not undermine human autonomy or causes other adverse effects. Depending on the specific Al-based system and its application area, the appropriate degrees of control measures, including the adaptability, accuracy and explainability of Al-based systems, should be ensured¹². Oversight may be achieved through governance mechanisms such as ensuring a human-in-the-loop, human-on-the-loop, or human-in-command approach. 13 It must be ensured that public authorities have the ability to exercise their oversight powers in line with their mandates. All other things being equal, the less oversight a human can exercise over an Al system, the more extensive testing and stricter governance is required."

Philosophical input: transparency

"The **traceability** of AI systems should be ensured; it is important to log and document both the decisions made by the systems, as well as the entire process (including a description of data gathering and labelling, and a description of the algorithm used) that yielded the decisions. Linked to this, **explainability** of the algorithmic decision-making process, adapted to the persons involved, should be provided to the extent possible. Ongoing research to develop explainability mechanisms should be pursued."

p. 5

Philosophical input: accountability

"Potential negative impacts of AI systems should be identified, assessed, documented and minimised. The use of impact assessments facilitates this process. These assessments should be proportionate to the extent of the risks that the AI systems pose. Trade-offs between the requirements — which are often unavoidable — should be addressed in a rational and methodological manner, and should be accounted for. Finally, when unjust adverse impact occurs, accessible mechanisms should be foreseen that ensure adequate redress."

p. 6

Question for you

What do you think about these requirements of

- -Human agency and oversight
- -Traceability
- -accountability?

Summary

- Autonomy is a basic ethical concern.
- If ML/Al's influence on humans is manipulative, autonomy is violated.
- There are examples in which ML/AI manipulate human decisions.
- Manipulation can be avoided by informed consent.
- The basis for informed consent is trust.
- Trust in ML is difficult due to its opacity.
- It is debated when people should trust ML.