The Datafied Present and Future

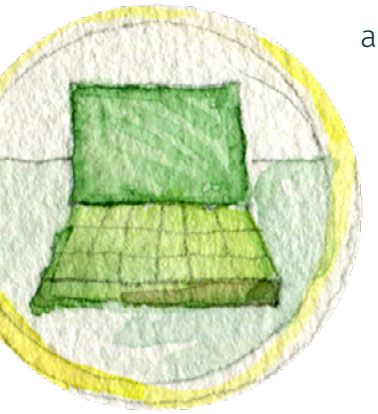
Authored by **Javiera Atenas**

How to cite this chapter: Atenas, J. (2021). The Datafied Present and Future. In C. Kühn, J. Atenas & L. Havemann (Eds.), Understanding Data: Praxis and Politics. HDI - Data, Praxis and Politics. https://doi.org/10.5281/zenodo.4698609

Abstract and description of the units

This module is aimed at critically exploring some key issues around data that concern us not only individually, but also, at the collective level. How we analyse and interact with data, how data is shaping our society, which are the legal frameworks around uses of data and how we can challenge the uses that are given to our data are explored.

In the first unit, the basics of data ethics are probed. In the second unit, the fundamental principles that govern what is right and what is wrong in the data cycle, from collection and production to their use are considered. The concepts of data privacy pertaining to the regulations and laws about data opening, publishing, collection, storage and management are examined. In the third unit, critical approaches to AI and algorithms are reviewed. Issues, such as opacity and bias in algorithms, as well as regulations for automated decision and predictive analytics that are underpinned by and lead to power imbalances, thus constraining opportunities for participation, are discussed. Finally, the fourth unit is focused on personal agency, where the aim is to enable citizens to contest the uses of their data with the wherewithal to challenge the advancement of data power.



Learning outcomes

- Understanding the basics of data ethics and data protection
- Understanding how algorithms and AI work and their impact on society
- Understanding the concepts of data agency and data sovereignty
- Acquiring abilities to manage and challenge personal and collective sensitive data
- Learning to manage and navigate the social aspects of data
- Applying basic ethical principles in research projects

Introductory multimedia • video-podcast

Introduction to Data Ethics - Brent Mittelstadt - Alan Turing Institute
https://www.youtube.com/watch?v=qVo9oApl4Rs

Glossary of terms and acronyms • Link to wikipedia when possible

Artificial intelligence (AI): intelligence demonstrated by machines, unlike the natural intelligence displayed by humans and animals. Artificial intelligence

Data ethics: refers to systemising, defending, and recommending concepts of right and wrong conduct in relation to data, in particular, personal data. Data ethics

Personal data: is any information relating to an identifiable person. Personal data

Data agency: is the individual's ability to influence and shape his/her life trajectory as determined by his/her cultural and social contexts. Agency in the digital arena enables an individual to make informed decisions, where his/her own terms and conditions can be recognised and acknowledged at an algorithmic level. Data agency

Negotiability: is the means to navigate the social aspects of data, which supports interaction between other data subjects and their policies. This enables the ongoing engagement of users so that they can withdraw from data processing either completely or in part and can derive value from data harvesting for themselves. (From the Encyclopedia of Human Data Interactions). Negotiability

Data sovereignty: is the idea that data must be subject to the laws and governance structures within the nation in which it is collected. The concept of data sovereignty

is closely linked with data security, cloud computing and technological sovereignty. Also, it can be understood as the relation between data and groups of vulnerable or minority groups, which must have agency and voice-over how their data is collected, shared and portrayed. Data sovereignty

Data protection: is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. It is also known as data privacy. Data protection

GDPR: The General Data Protection Regulation is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. GDPR

Recommended reading

1. D'Ignazio, C & Klein, L. (2020) Chapter 6. The Numbers Don't Speak for Themselves. In Data Feminism.
Retrieved from https://data-feminism.mitpress.mit.edu/pub/czq9dfs5 and related podcast

2. Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. Big Data & Society, 4(2), https://doi.org/10.1177/2053951717736335

3. Taddeo, M., & Floridi, L. (2016). What is data ethics ? Philosophical Transactions. Series A, 1–5. https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2016.0360

4. Markham, A. N., Tiidenberg, K., & Herman, A. (2018). Ethics as methods: doing ethics

in the era of big data research -Introduction. Social Media and Society, 4(3). https://doi.org/10.1177/2056305118784502

5. Bhargava, Rahul (2018). The algorithms aren't biased, we are. Medium. Available from: https://medium.com/mit-media-lab/the-algorithms-arent-biased-we-are-a691f5f6f6f2

6. Peppet, Scott (2010). Unraveling Privacy: The Personal Prospectus & the Threat of a Full Disclosure Future. Northwestern University Law Review. Available at SSRN: https://ssrn.com/abstract=1678634

Key complementary resources

1. Keyes, O. (2019). Counting the Countless. Why data science is a profound threat for queer people, available from: https://reallifemag.com/counting-the-countless/)

2. The GovLab (June 8, 2020). How data can map and make racial inequality more visible (if done responsi-bly). Medium, available from: https://medium.com/data-stewards-network/how-data-can-map-and-make-racial-inequality-more-visible-if-done-responsibly-9074ed84e2bf

3. The GovLab (June 8, 2020). Data driven efforts to address racial justice. Medium available from: https://medium.com/data-stewards-network/ongoing-data-driven-efforts-to-address-racial-inequality-49e40ee05fee

4. Data science ethics Podcast, available from: http://datascienceethics.com/category/podcast/

5. We need to talk AI, comic booklet https://weneedtotalk.ai/

6. Data Feminism. D'Ignazio and Klein: https://data-feminism.mitpress.mit.edu/

7. Bhattacharya, Ananya. n.d. Racist tweeters can be convinced to stop spreading

hate—If a white man asks them to. Quartz. Accessed 25 January 2019. https://qz.com/840060/racist-tweeters-can-be-convinced-to-stop-spreading-hate-if-a-white-man-asks-them-to/

8. Deva, Surya. (2020), Addressing the gender bias in artificial intelligence and automation. OpenGlobalRights (blog). 10 April 2020. Available from: https://www.openglobalrights.org/addressing-gender-bias-in-artificial-intelligence-and-automation/.

9. Yeshi (2020), Data for Black Lives, Medium, We Will Not Allow the Weaponization of COVID-19 Data. Avai-lable from: https://medium.com/@YESHICAN/we-will-not-allow-the-weaponization-of-covid-19-data-e775d31991c

10. Algorithm Watch's, bi-weekly newsletter, presents a short summary of current events and research on automated decision-making and its consequences on society.

2.1 • Understanding data ethics

Datafication – transforming all things under the sun into a data format and thus quantifying them – is at the heart of the networked world.

José van Dijck, 2017

Introduction

Collecting, publishing and using data require two key elements, data ethics and data protection. Data ethics can be understood as the key principles governing what is right and wrong in the data cycle, from collection and production, to its use. Data

protection refers to the national and international regulations regarding personal privacy and rights about access to and the processing of the data. In this unit, the different facets of data ethics and data protection concerning commercial, educational and public data are explored, starting with the premise that not all data, public or private, is publishable, and that not all uses are harmless. The discussion will centre on the different debates around data.

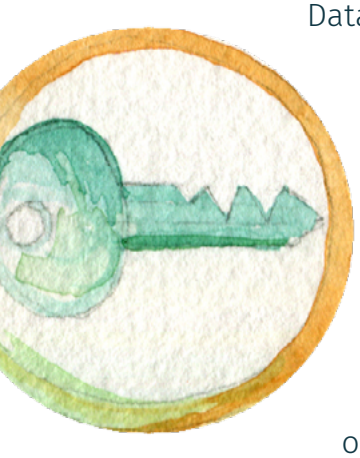
We need to consider that data is framed by regulations, which serve people, governments, organisations and industries to control and balance the potential uses of the data so that they can benefit society without harming people. In the context of human-generated data, we will discuss two kinds to understand how they can and should be published as well as how to protect people, including vulnerable communities, from pervasive and intrusive uses of data.

2.1.1 • Principles of data ethics

We live in a 'datafied' society, where almost everything is continuously transcribed into data, quantified and analysed (Van Es and Schäfer, 2017), where decisions taken by corporations and governments are increasingly data- and algorithm-driven. Data have an impact that ranges from the economy to education and policy, to what we watch and connect with. It can be said that data permeate almost every single element of modern life and therefore, it is crucial to understand risks of their present and future uses. In addition, understanding the ethical conundrums we face when dealing with data will inform how data could be used in the future and how it can be interweaved to create new datasets that can be used to predict all kinds of behaviours and try to influence them (Hand, 2018).

The emergence of new technologies, the main aim of which is to process data to gain knowledge about human activities, is generating social asymmetries between those who own the tools and have the

expertise to collect and analyse data and those whose data are subject to these applications (Belbis & Fumega, 2019). Artificial intelligence (AI) and other practices that are designed to exploit large volumes of data, which emerge as a product of the digitisation of the vast majority of information services, create the need to discuss ethical limits.



Data ethics can be understood as the responsible and sustainable use of data. It is key that we learn how to collect, select, analyse and use such data under the premise of 'do no harm', thus ensuring that data-led research projects are beneficial for people and society. Data ethics need to be understood as a social contract between the public and data users (Buenadicha et al., 2019 -article in Spanish). Data ethics refers to a series of principles or guidelines to which any data research-led project or activity must adhere, with the main focus being on human rights and personal data protection laws. Thus Data ethics principles must lead to actively design fair and unbiased research and motivate students to learn, from the very beginning, the value of data protection and data agency by raising awareness of the role of an ethical common ground when conducting research with data, by treating others' data as you wish your own is treated.

The latest EU digital education action plan 2021-2027, proposes within its competence framework to support learners to engage positively, critically and safely with this technology. Moreover, they need to be aware of potential issues relating to ethics, environmental sustainability, data protection and privacy, children rights, discrimination and bias, including gender bias and disability as well as ethnic and racial discrimination (p.14). To teach the embedding of data principles in research or project-based learning activities, it is essential that we are fully aware of the main elements of such principles, their values and conceptualisation.

Also, it is important to enable learning through the seven principles of data feminism (D'Ignazio & Klein 2020) to challenge power dynamics, considering for starts, the diversity and social context of the students, organising research activities that allow:

- Examine power: To help in understanding who is controlling the discourse, the

issues and the general landscape as well as how decisions are being made, and where;

- Challenge Power: To support the development of personal and collective agency aimed at improving social problems;

- Elevate emotion and embodiment: To use information looking beyond data to give a voice to people regarding their life experiences and emotions;

- Rethink binaries and hierarchies: To understand how data puts people in clusters that can perpetuate oppression and thus be able to avoid sustaining or validating such practices;

- Embrace pluralism: To promote the use of knowledge from diverse perspectives, giving priority to those normally unheard, and creating space for indigenous and experiential ways of knowing;

- Consider the context: To acknowledge that data is not neutral, but rather, the product of unequal social relations and thus, quite likely to be biased;

- Make labour visible: To ensure understanding of the work and work dynamics, and politics behind data and data science projects, including the work ethics of such projects.

2.1.2 • Examining the ethics of data

If students are to navigate the turbulent waters of data and algorithms, then data learning activities must foster reflection on how data are constructed and operationalised across societies. They should be provided with opportunities to learn from the analysis of data and from discussing the implications of data projects from a range of sources and perspectives. This is important so that they understand how people and data are portrayed, the historical impact of bias in data as well as

how prejudices and also, cultural misconceptions have implications that affect the lives of people.

Some of the current uses of data which require careful consideration regarding ethics are as follow:

- The role technologies play in collecting data from personal, professional and social activities, permeating the uses of any platform or device, including phones and credit cards, with the intention to predict almost every behaviour. These activities are called predictive analytics and are used to identify the likelihood of future outcomes based on historical data. Some activities that tend to be predicted are what will you be shopping or what will you watch next on streaming platforms, bit also, how likely you are to survive a heart attack in order to get a life insurance cover.

- Hood and Margetts (2007) argue that governments operate through two sets of agents, namely detectors and effectors, when deploying data to play a role in politics. Detectors gather information (data) from individuals and society, whilst effectors seek to influence them. Regarding which, we can see how data have been used during the Covid-19 pandemic to develop public policy and are routinely used to forecast economic trends. Also, we can see how data is used to influence voters by targeting different socioeconomic groups during political campaigns.

- The interwovenness of data infrastructures facilitate attempts to predict socioeconomic behaviours, by promoting the collection of socioeconomic data (race, gender, neighbourhood) aiming to predict certain behaviours depending on people's background. For example how likely certain students are to fail or succeed in education, or the price of your car insurance depending on your neighbourhood, and also, it is used in police work, to predict crime for example, and getting people profiled by the police, foreseen as a criminal and most likely been stopped and arrested.

Finally, it is also useful to discuss how the lack of regulatory and ethical frameworks to prevent misuses of data are affecting us every day, by for example, discriminating

against women during data-driven job recruitment, there being racist uses of data or evident gender inequality regarding access to health.

It is important that data-led research and learning activities are designed to address inequalities, to improve quality of life, to explore issues that may be harming a community, and also, to improve data governance. This is key to people acquiring the skills to participate in developing policy frameworks that go beyond data protection, by providing a fair, harmless, unbiased and equal data landscape that regulates the public and private sector usage of data.

Recommended activity

To start exploring data ethics issues with your students, we recommend using the data ethics canvas designed by the Open Data Institute. Ask your students to form groups and plan data-led research. Ask them to select one social issue and discuss it using the canvas, and then, ask them to write a blog post about the ethical elements of their research project they discussed as a group.

2.2 • Understanding data privacy and data protection

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.

Article 12. The Universal Declaration of Human Rights

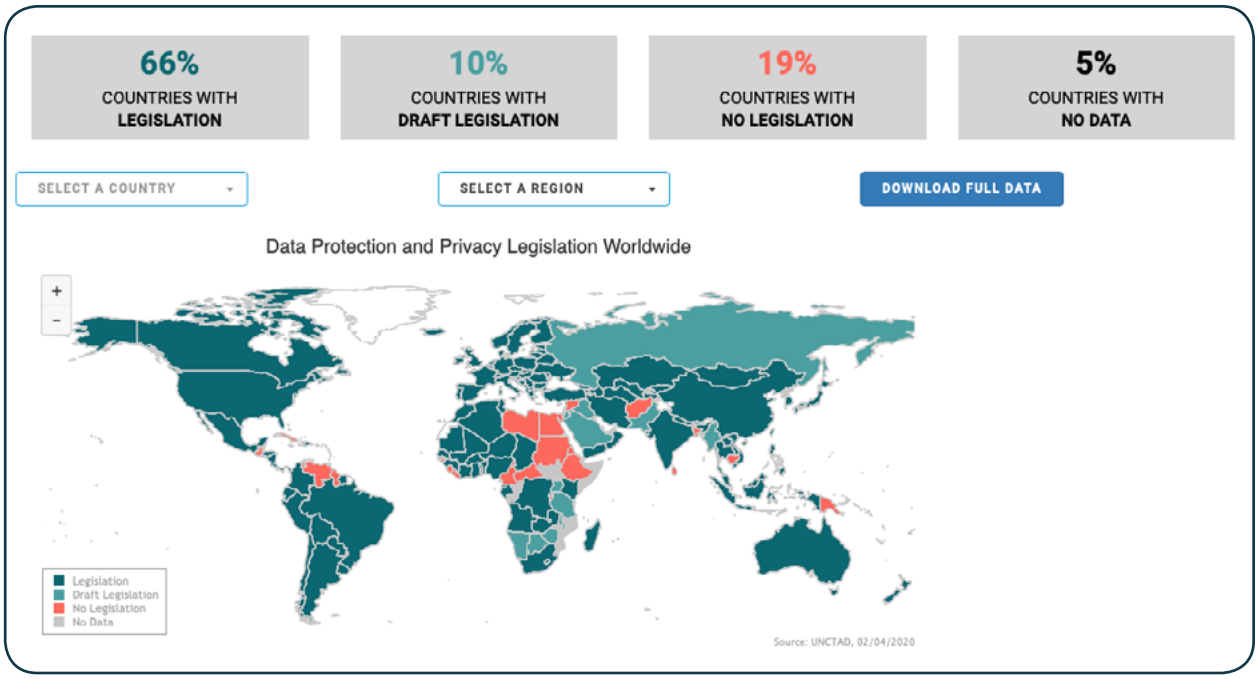
Introduction

The boundaries of data opening, publishing, collection, storage and management are determined by a set of regulations and laws, which aim at preserving and safeguarding the privacy of people regarding the publication of certain information assets, even though these are collected by public bodies and managed and stored in public information systems. The emergence of technologies and techniques for processing these data generate new asymmetries between those who own the tools and the subjects whose data are subject to these applications (Belbis & Fumega, 2019). AI and algorithms, learning analytics as well as any other system product of the digitisation of the vast majority of information services, have created the need to develop frameworks to protect individuals and groups from misuses of their data by public or private entities.

2.2.1 • Principles of data privacy

Privacy, according to Privacy International, is crucial for the protection of human dignity and constitutes one of the fundamental bases of democratic societies. It is a pillar that enables the exercising of the rights of freedom of expression, information and association. Data protection is one of the ways to guarantee, in practical terms, the right to privacy in the context of the information society, where the storage of personal data is in the hands of public and private actors. For nowadays, it is possible to identify and single out individuals in large sets of data and use their personal data to monitor their behaviour, track their location and detect their interactions with platforms, which allows for the performing of predictive analytics.

According to the Office of the High Commissioner for Human Rights (UN Human Rights), privacy is a fundamental human right and it is articulated in all of the major international and regional human rights instruments, including Article 12 of the United Nations Declaration of Human Rights 1948, the International Covenant on Civil and Political Rights (ICCPR) 1966; Article 17 and Article 16 of the UN Convention on the Rights of the Child; Article 11 of the American Convention on Human Rights; Articles 16 and 21 of the Arab Charter on Human Rights and Article 8 of the European Convention on Human Rights. According to UNCTAD, 132 out of 194 countries have put in place legislation to secure the protection of data and privacy.



UNCTAD - data protection and privacy laws worldwide / Click for the newest version

An important element of the right to privacy is the right to the protection of personal data. While the right to data protection can be inferred from the general right to privacy, some international and regional instruments also stipulate a more specific right to the protection of personal data. To explore the landscape of data protection and privacy regulations around the globe, you can access a list by country to understand how data protection operates in different countries.

2.2.2 • Data protection laws and regulations

The first-ever data protection law – Sweden's Data Act – was created in 1973, and it basically has made it illegal for any person or company to use information systems of any kind to handle personal data without a licence. Iceland has the toughest privacy laws, with The Data Protection Act of 2000 stating that data must be obtained for specific purposes, and that people must give informed consent. They must be made aware in an unambiguous way of the type of data collected, the collection purpose and how the data processing is conducted and how it is protected, with people having the right to withdraw their consent for its usage at any time.

Not obeying the act can result in fines or even a prison term of up to three years.

In the UK, The Data Protection Act 1984 introduced basic rules on data collection and people's rights to access data collected about them. This act was followed by the Data Protection Act 1998, which granted individuals legal rights to control information about themselves and defined a series of principles to ensure that information was processed lawfully. It was superseded by the Data Protection Act 2018, which applies the EU's GDPR and lists a series of offences about knowingly or recklessly obtaining, disclosing, retaining, and selling or offering to sell, personal data obtained without consent.

In the European Union, data protection is regulated by the General Data Protection Regulation (GDPR), which sets out seven principles for the lawful processing of personal data, which includes the collection, organisation, structuring, storage, alteration, consultation, use, communication, combination, restriction, erasure or destruction of personal data. Its seven principles are:

- Lawfulness
- fairness and transparency
- purpose limitation
- data minimisation
- Accuracy
- storage limitation
- integrity and confidentiality (security)
- accountability

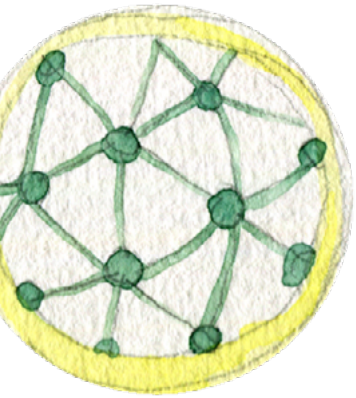
EU GDPR Principles

Recommended activity

To discuss issues about data privacy with your students, we recommend using the Data, Privacy, and Identity (Design Changes for Cards) to help them to raise awareness about the different types of data collected and stored during online and assumed-to-be offline activities. Ask them to reflect on the ways different types of data, and combinations of data, can reveal more about our identity than we might be aware or be comfortable with revealing. Consider how the perception of harmless data collection changes when viewed through the lens of different identities and talk about the types of data users have no control over. These are "essential" to the functioning of the tools, you can download and print the cards or work with them online.

2.3 • A critical approach to AI and algorithms

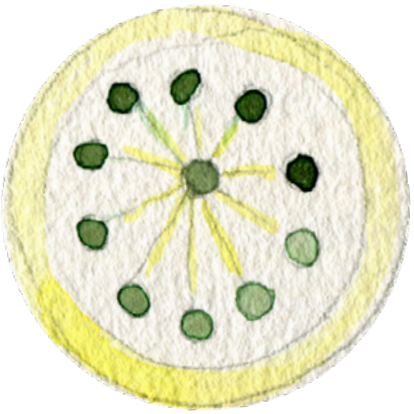
The EU digital education action plan 2021-2027 suggests promoting understanding of emerging technologies and their applications in education, developing ethical guidelines on artificial intelligence (AI) and data usage in teaching and learning for educators and support related research and innovation activities through Horizon Europe (p.12)



Introduction

Artificial intelligence (AI), algorithms and machine learning are having a great impact on humanity and this will only increase in the future. Some

fundamental questions about how to regulate these technologies have been arising, as they present a series of risks for people and challenges to the legal systems. The ethics of AI is often focused on "concerns" of various sorts, such as its opacity and bias, as well as regulations for automated decision support and predictive analytics, as according to Whittaker et al. (2018), these lack accountability, community engagement, and auditing. Hence, creating power imbalances and limiting opportunities for participation. Another AI ethics issue is its opacity, which means that, normally, people affected by automated decisions and algorithms cannot challenge the outcome of a resolution. To address issues regarding opacity it is essential to remove bias and establish legal frameworks to respond to these challenges and protect people.



The diagram below is useful to understand how the inferences that a system makes using our personal data despite not always being transparent to the user, are subsequently used to drive actions in individuals' daily life.

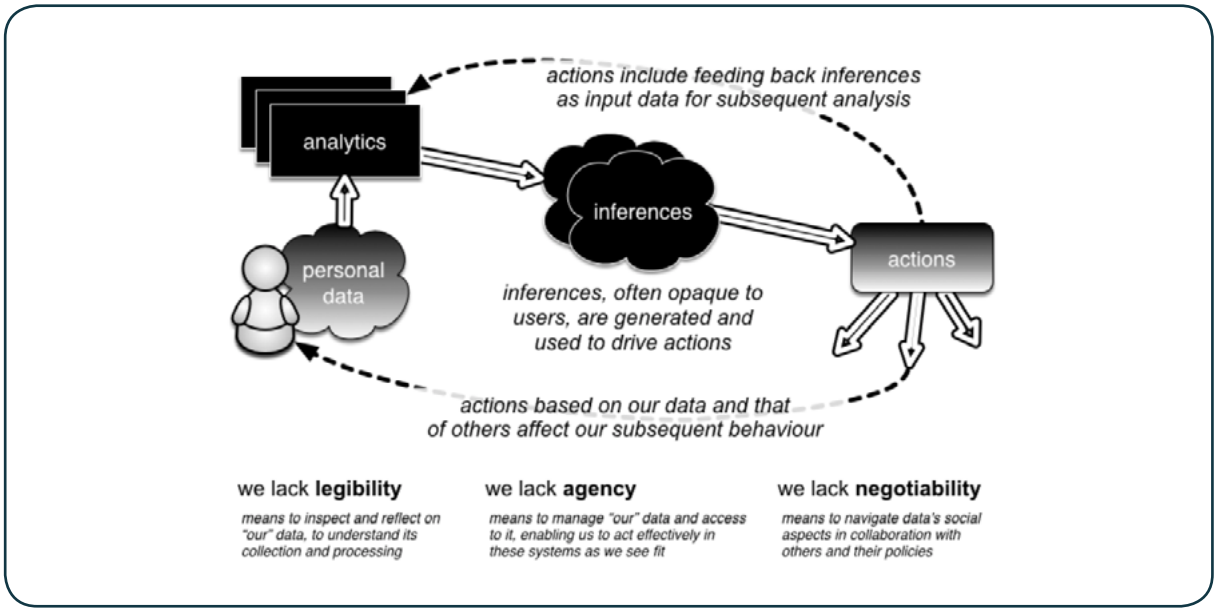


Figure 1: Richard Mortier. Copyright terms and licence: CC BY-NC-ND

The figure explains the data flows in the Human-Data Interaction model. We generate data which is analysed to produce inferences. These inferences in turn are fed back, affecting our behaviour and becoming themselves the subject of further analysis.

2.3.1 • Principles of AI ethics

At a glance, AI systems should benefit individuals, society and the environment. The principles of AI ethics according to the OECD should be considered as that:

- AI should benefit people and the planet by driving inclusive growth, sustainable development and well-being;
- AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity. They should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society;
- There should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them;
- AI systems must function in a robust, secure and safe way throughout their life cycles, with potential risks being continually assessed and managed;
- Organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles.

Also, the G20 Ministerial Statement on Trade and Digital Economy lists the key AI principles as:

- Inclusive growth, sustainable development and well-being;
- Human centred values and fairness;
- Transparency and explain-ability;
- Robustness, security and safety;
- Accountability.

Moreover, the Building Australia's artificial intelligence capability commission has listed an AI Ethics Framework, which comprises eight principles useful for when designing, developing, integrating or using AI systems aimed at reducing the risk of negative impact on business and promoting good governance, which can be summarised as:

- **Human-centred values:** Throughout their lifecycle, AI systems should respect human rights, diversity, and the autonomy of individuals;

- **Fairness:** Throughout their lifecycle, AI systems should be inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities or groups;

- **Privacy protection and security:** Throughout their lifecycle, AI systems should respect and uphold privacy rights and data protection as well as ensuring the security of data;

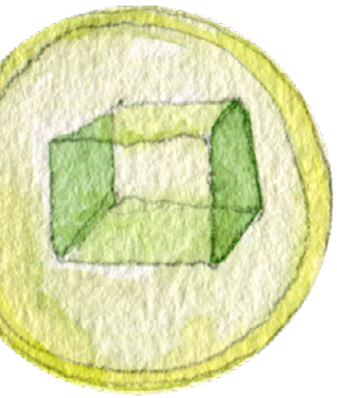
- **Reliability and safety:** Throughout their lifecycle, AI systems should reliably operate in accordance with their intended purpose;

- **Transparency and explain-ability:** There should be transparency and responsible disclosure to ensure people know when they are being significantly impacted upon by an AI system, and can find out when it is engaging with them;.

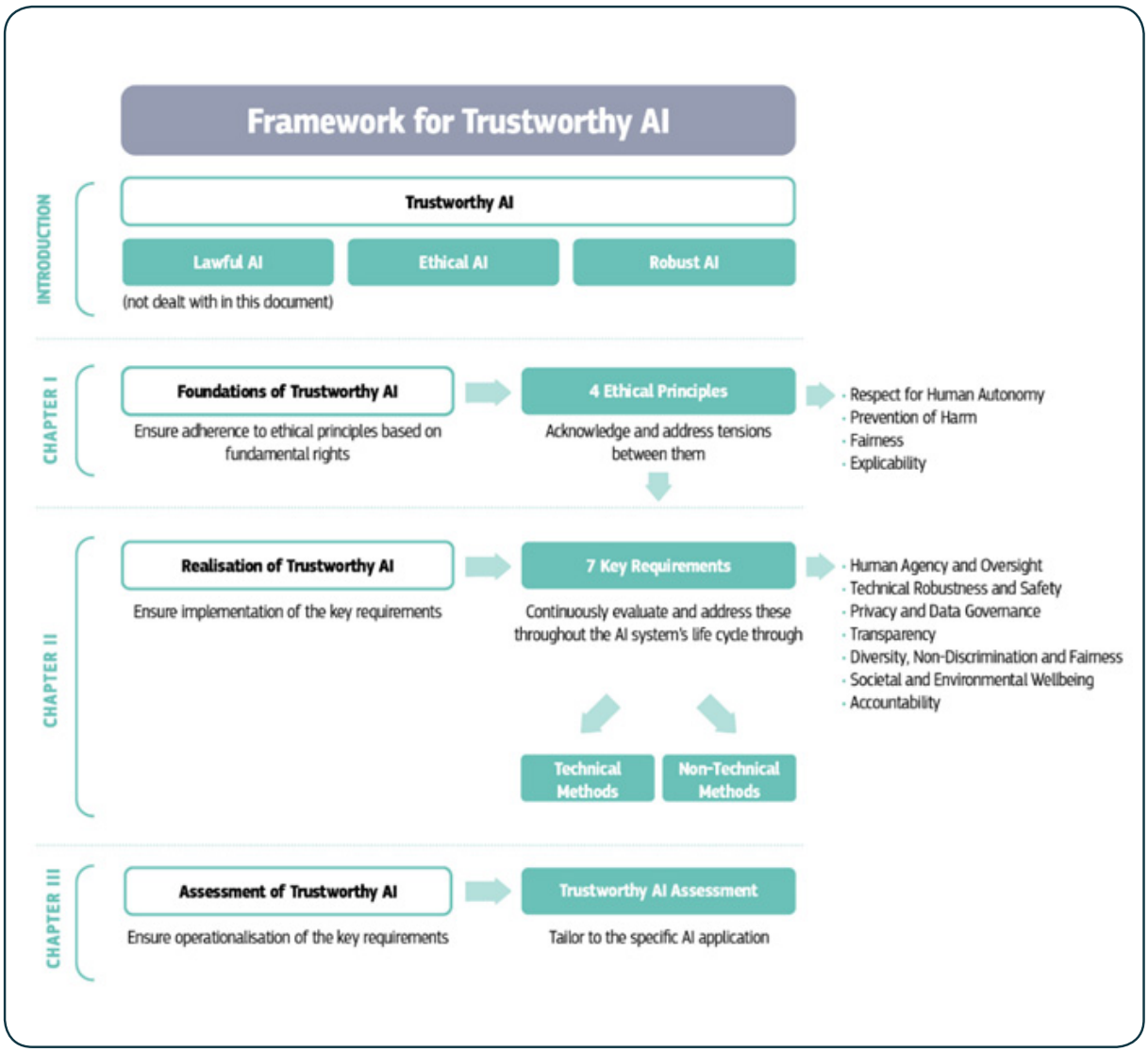
- **Contestability:** When an AI system significantly impacts on a person, community, group or environment, there should be a timely process to allow people to challenge its use or output;

- **Accountability:** Those responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes and human oversight of AI systems should be enabled.

Furthermore the European Alliance of the European Council has developed a series of Ethics Guidelines for Trustworthy AI, which sets up an EU legal framework for AI, stating in its point (22) that AI systems do not operate in a lawless world. A



number of legally binding rules at European, national and international levels already apply or are relevant to the development, deployment and use of AI systems today. We highlight point (26) holding that Ethical AI - Achieving Trustworthy AI requires not only compliance with the law, which is but one of its three components, and point (27) Robust AI, which states that even if an ethical purpose is ensured, individuals and society must also be confident that AI systems will not cause any unintentional harm. Such systems should perform in a safe, secure and reliable manner, with safeguards put in place to prevent any adverse impact. A proposed framework for trustworthy AI proposed by European AI alliance, is presented below.



Framework for trustworthy AI (European AI Alliance)

The Guidelines as a framework for Trustworthy AI promote that AI system objectives should be clearly identified and justified. AI systems that help address areas of global concern, like the United Nations Sustainable Development Goals, should be encouraged. Ideally, AI systems should be used for the benefit of all human beings, including future generations as well as respecting human rights, diversity, and the autonomy of individuals. They should be inclusive and accessible, not discriminating against individuals, communities or groups.

It is key to look at the landscape of ethics of AI, as for example EU Parliament presents a series of issues and initiatives, to raise awareness and prevent AI affecting the democratic process, or the use of deception, unfair manipulation, or unjustified surveillance. Thus, it is key to consider AI's implications in politics, to develop strong regulations towards respecting and upholding privacy rights and data protection, ensuring proper data governance and transparency providing information to help understanding key factors used in algorithmic decision making.

2.3.2 • Examining AI ethics

To design teaching and learning activities regarding the ethical boundaries of AI, algorithms and machine learning, we need to mention how its opacity affects us all directly and indirectly. Students as citizens need to develop awareness and competencies to participate in democratic discussions to create legal frameworks to prevent misuses or unethical uses of AI. Accordingly, UNESCO holds that we need to educate algorithms, whilst citizens need to understand potential problems and, consequently, challenge them.

Safiya Umoja Noble has been working on showcasing how algorithms are a tool for oppression, opening a discussion of unethical or illegal uses of AI and algorithms, and some examples from around the world can be categorised as follow:

- **Racism:** The opacity of algorithms creates black boxes, and one of the critical

arguments towards the need to have regulatory frameworks is the Rise of the Racist Robots, which, for example, is leading to consumer lending discrimination or preventing certain groups from obtaining visas to visit or live in countries. Moreover, they can harm certain groups' educational experience using unfair learning analytics and student surveillance tools that require facial recognition. These technologies tend to break black people (video: Ain't I a woman?) through racist predictive policing, leading to longer incarceration sentences being imposed on such minorities.

- **Sexism:** We need to consider the fact that 78% of AI professionals are men, and thus, their experiences inform and dominate algorithm creation. Women are affected by algorithmic decisions in every aspect of their lives, including access to health, services and the labour market. Algorithms are failing women through misdiagnosis, affecting clinical decisions, prescribing wrong treatments and hence, damaging their health.

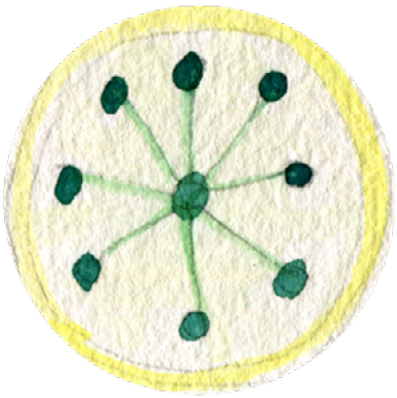
Also, algorithms are unfair to women regarding finance, but even more worryingly, AI is harming their job opportunities. For example, women are targeted with lower-paying jobs ads and being discriminated against by HR personality tests or when applying for a job. Moreover, AI can potentially harm the queer and trans community, portraying them in a wrong and stereotypical way. Thus ethical AI developments must address the needs of the non-binary and trans people to protect them from potential harm.

- **Socioeconomic discrimination:** Algorithms badly affect those coming from lower-income households and neighbourhoods, for example, by lowering their school grades. This kind of behaviour is known as automating poverty or automating inequality, where AI is used to assign or remove such as unemployment benefits, child support, housing and food subsidies, leading in the worst cases to death or severe health problems. Automated inequality is a way of imposing systemic oppression, for example, requesting biometric data for access to food in schools. Thus, UNICEF is calling to protect childrens' rights because low-income families are affected by automated decisions on benefits and welfare, as AI is used to determine, showcase and map poverty, with the risks of depicting groups in a negative way, depending on the school they went, where they live, also, it is used to predict poverty. Thus, it is necessary to work towards

protecting the most vulnerable in society from predatory and dangerous uses of AI.

- **Surveillance:** Businesses, employers, educational organisations and governments are using surveillance mechanisms to control specific behaviours. Shops monitor customers behaviours; companies monitor employees' activities; schools monitor children's engagement; universities use proctoring systems to invigilate exams. In other words, we are constantly monitored under what Shoshana Zuboff calls surveillance capitalism. The Carnegie Endowment for International Peace has pointed out that a growing number of states are deploying advanced AI surveillance tools to monitor, track, and surveil citizens to accomplish a range of policy objectives - some lawful, others that violate human rights, and many fall onto a murky middle ground. They have developed an AI Global Surveillance (AIGS) Index to showcase how AI is rapidly proliferating worldwide. Hence, the United Nations, UNESCO, The European Council and the OECD, amongst other international players, call for regulatory frameworks to prevent the abuse of surveillance mechanisms.

- **Manipulation:** AI has been used for social influence and behaviour manipulation, mostly through social media and predominantly about our political views and opinions. It has been utilised to spread propaganda and target specific groups of people, with content that can lead to radicalisation, and extreme political views, thereby threatening democracy and democratic processes. Thus, a regulatory framework for targeted information in political campaigns needs to be enforced.



Recommended activity

To discuss discrimination through algorithms, you can start by asking your students to play with the Pre-crime Calculator, which is an interactive experience that takes you to the world of predictive policing. How much of a potential suspect or a victim are you in the eyes of the system? And what are the areas in your city you should avoid in the next week so as not to get involved in the crime?

Then, ask the students to take an online personality test, such as the Business Personality Profile, using a male and female identity with similar characteristics and compare the results of the test.

Finally, ask your students to share their experiences with the rest of the class.

Back to Understanding Data: Praxis + Politics

Illustrations, editorial and graphic design by Alexandra Kuhn