Ethical Issues and Concerns in Digital Innovation

ISM-E2002

Kari Koskinen

Hadi Ghanbari

Department of Information and Service Management

Aalto University
School of Business

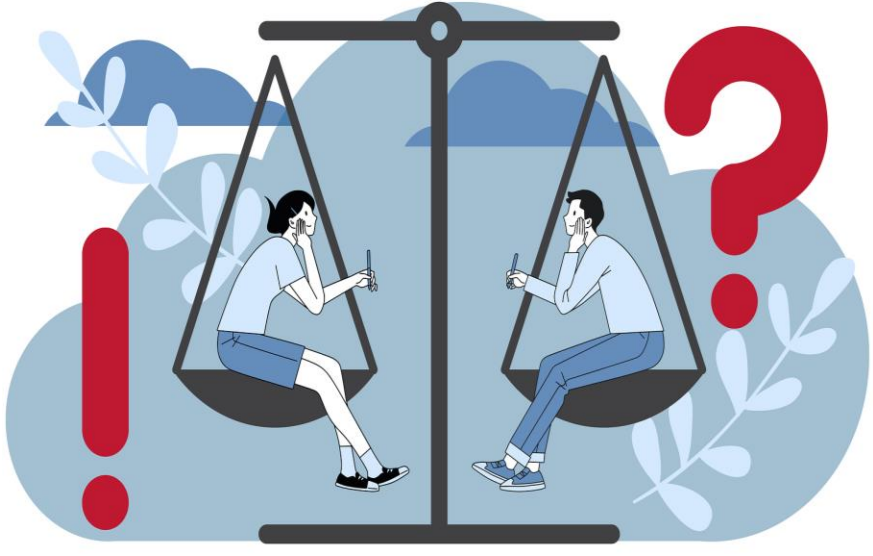

Image by Rosy from Pixabay

Session 2 - Ethics and regulations, policies and laws

Today’s session

- **Ethics and regulations, policies and laws**
  - Regulation and ethics
  - Cyberlaw
  - GDPR & GDPR exercise
  - DSA
  - Other EU Acts

Ethics, morality and law

- Ethics aims to answer questions such as “What should I do?” through a process of reflection of different values, principles, and purpose rather than plainly following habits, social conventions, or self-interest
- Morality can be seen as a coherent, consistent account that has been refined through history and can be applied to different situations. Moral system lays out the norms according to which one should go about their daily lives and are occasionally accepted as is without questioning their basis.
- Law tries to create basic, enforceable standards of behaviour necessary in order for, e.g., a community to succeed and social institutions to keep functioning. Law is narrower in focus than ethics or morality. Law can be silent on some ethical issues, go against or not far enough on ethics.
- What is the relationship between ethics and law? How to assess whether a law is moral or ethical?

Laws, principles, policies, standards

- *"Trustworthy AI has three components, which should be met throughout the system's entire life cycle:*
  - *(1) it should be lawful, complying with all applicable laws and regulations*
  - *(2) it should be ethical, ensuring adherence to ethical principles and values*
  - *(3) it should be robust, both from a technical and social perspective since, even with good intentions, AI systems can cause unintentional harm."*

  (ETHICS GUIDELINES FOR TRUSTWORTHY AI: High-Level Expert Group on Artificial Intelligence set up by the European Commission)
- Regulation and laws tend to require compliance, whereas ethical principles, codes of conduct may not
- Ethical principles may impact legislation but may also go beyond legal norms
  - Ethical principles by companies as a way to avoid regulation?
- Policies guide actions towards those actions that armost likely to achieve desired outcome
  - Not necessarily codified into laws
- Standards as models, examples, or points of reference established by authority, custom, or general consent

Regulation and digital innovation

- Impact to innovation
  - Hindrance by making it more difficult to pursue certain innovations
    - Meeting regulatory requirements
    - More bureaucracy
  - Provide structure, clarity and order
    - Standardization
    - Increased development and other costs due to *lack* of regulation
  - Create business opportunities?
    - E.g. consultants but also technical fixes etc.
- Legislation often has difficulties in keeping up with the latest technological developments
  - Legislation usually a slow process
    - Clashing viewpoints & interests, mapping implications, lobbying

EU pitches cyber law to fix patchy Internet of Things

Products carrying the CE marking would have to meet a minimum level of cybersecurity checks.

https://www.politico.eu/article/new-cyber-act-to-raise-safety-standards-across-the-bloc/

ChatGPT broke the EU plan to regulate AI

Europe's original plan to bring AI under control is no match for the technology's new, shiny chatbot application.

https://www.politico.eu/article/eu-plan-regulate-chatgpt-openai-artificial-intelligence-act/

Cyberlaw

- Law bearing on the world of computer networks, especially the Internet, and deals with matters such as the right of privacy, freedom of speech, regulation of electronic commerce, applicability of copyright laws, different cyber crimes
- Not a separate area of law but spread across many legal areas, e.g., intellectual property, privacy, data protection and others
  - Applicability of old/existing legal norms to cyberspace and digital realm not always clear
- Globally interconnected systems and global flows of data via internet
    - Geographical, jurisdictional boundaries not always clear
      - The location of the user, server, the entity offering a service may all play a role in deciding the jurisdiction to be deployed
    - Regulation on a national, regional and international level

Cyberspace governance models

CYBER GOVERNANCE	CHARACTERISTICS	ORGANIZATION/FRAMEWORKS
Distributive	Self-regulating: code, architecture and markets, decentralized	Open-source communities/WIPO/Linux/software code, social norms
Globalism/ transnationalism	Treaties, norms, cooperative problem-solving arrangements, multi-stakeholderism, soft power, networks, interlocking governance systems, multilateralism, bilateralism	ICANN, Internet Society (ISOC), World Wide Web Consortium (W3C), NATO Cyber Centre of Excellence, Cybercrime Conventions, United Nations Charter, OSCE, Council of Europe, The Organization for Economic Cooperation and Development (OECD), WTO, INTERPOL
Regionalism	Geographic contiguity, democratic, co-regulation, shared values and cultures, interaction, common political institutions, military interaction, norms pertaining to conflict resolution	Regional agreements such as: The Shanghai Cooperation Agreement, The Arab Convention on Combating IT Offenses, The African Union Convention on Cyber Security, The Organization of American States Inter-American Cybersecurity Strategy, The Agreement on Cooperation Among the States Members of the Commonwealth of Independent States, and the European Council Convention on Cybercrime
Nationalism	Geographically bounded, single government, state-centric laws, and frameworks, state control, top-down decision making, historic cultural and linguistic cohesiveness	National and international cyber security strategies, privacy policies, laws and regulations, cybercrime law enforcement, standards (NIST) (ISO) frameworks, information sharing

(Greiman 2022)

General Data Protection Regulation (GDPR)

GDPR

- European Union's General Data Protection Regulation
  - 99 articles, 173 Recitals
  - Entered into force in 2016, compliance by May 25, 2018
  - Drafted by EU but has implications to any organization that targets people in the EU, collects or processes data about them – including third parties to data, i.e. service providers to companies
  - Focus particularly on personal data - any information relating to an individual that can be identified from the data
- Failure to adhere to the law may result in fines of considerable value
  - Max at €20 million or 4% of global revenue, whichever is higher, while individuals (data subjects) have the right to seek compensation for damages
  - Implications to risk management (risk as likelihood of an event and its impact)

Key terms

- Personal data: Personal data is any information that relates to an individual who can be directly or indirectly identified. Pseudonymous data can also fall under the definition if it's relatively easy to ID someone from it
- Data processing: Any action performed on data, whether automated or manual. This includes collecting, recording, organizing, structuring, storing, using, and erasing data
- Data subject: The person whose data is processed
- Data controller: The entity/person that decides why and how personal data will be processed
- Data processor: A third party that processes personal data on behalf of a data controller

GDPR – Fair Information Practices

- Lawfulness, fairness and transparency - Processing must be lawful, fair, and transparent to the data subject
- Purpose limitation - Data processed for the legitimate purposes specified explicitly to the data subject when it was collected
- Data minimization – Collect and process only as much data as absolutely necessary for the purposes specified
- Accuracy - Personal data to be kept accurate and up to date
- Storage limitation - Personally identifying data can only be stored for as long as necessary for the specified purpose
- Integrity and confidentiality - Processing to ensure security, integrity, and confidentiality
- Accountability - The data controller (Data Protection Officer) is responsible to demonstrate GDPR compliance with these principles

https://gdpr.eu/

GDPR – Legal basis to process data

- Data subject has given a specific, unambiguous consent to process the data – yet there are limitations on the extent consent can be given
- Processing is necessary to execute or enter into a contract to which the data subject is a party – e.g. asking address to deliver an order
- Required to comply with a legal obligation – e.g. obligation of an employer to report the salary information of its employees to the tax authorities
- To protect the vital interests of a data subject or another natural person
- Processing is necessary to perform a task in the public interest or to carry out some official function – e.g. processing of personal data for scientific or historical research
- Legitimate interest to process someone's personal data (*"necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data"*) - e.g. relevant relationship between the data subject and controller (direct marketing for customers can be legitimate interest)

https://gdpr.eu/

GDPR – Rights of the data subject

- The right to be informed (of the collection and processing of their personal data)
- The right of access (confirmation from the controller on whether the controller is processing personal data that concerns them)
- The right to rectification (of inaccurate personal data concerning them and to have incomplete personal data completed)
- The right to erasure (data concerning him or her without undue delay, right to be forgotten)
- The right to restrict processing (of personal data concerning the data subject)
- The right to data portability (receive personal data in the right format and transmit it)
- The right to object (in certain situations, object to the processing of personal data)
- Rights in relation to automated decision making and profiling (right to demand human involvement in decisions that concern the data subject)

https://gdpr.eu/

GDPR and its ethical foundations

- What kinds of values GDPR upholds? Does it oppose some other values?
  - Value as a consideration of something being important or beneficial, to have a high opinion of
- Is GDPR more 'compatible' with deontology or with consequentialism?
- If you were a strong advocate of the stockholder theory, how might you react to GDPR? What about stakeholder theory?
- What does the GDPR (if anything) tell us about the morals/ethical foundations of the EU?

GDPR exercise

Case description – part 1

You are a researcher who has noticed that not only doctors but also any layman person can hear changes in the voices of Parkinson's patients. You embark upon on a research project, in which you collect voices from volunteers of Parkinson's patients at different stages of the disease to see whether a pattern can be found. The objective is to build an algorithm that would detect early signs of Parkinson's disease. To create the algorithm, you collect voice samples, age of the participants, the date of their diagnosis, and whether they speak any dialect. The participants are all volunteers who have signed a consent form to participate in this study. This form indicates, among others, the type of data collected, the purpose of collection and processing of the data, and the participants' rights as data subjects (such as how to withdraw their consent or ask for the deletion of their data).

- Which of that data would be personal data (Art. 4(1) GDPR)? What about sensitive data (Art. 9(1) GDPR)?
- What types of data processing operations are likely to occur in the project (ART. 4(2) GDPR)?
- What is the legal basis for processing the data (Art. 9.2 (a) GDPR)?
- What does it mean to pseudonymise data and how is that different from anonymisation (Recital 26 + Art. 4(5) GDPR)? Why might you have to do that (Art. 25 GDPR and Art. 89 (1) GDPR)?

Case description – part 2

You manage to develop the algorithm, and an insurance company approaches you regarding a follow-up project. The insurance company would like to develop an app based on the algorithm to profile its clients. It sees a benefit in finding out whether its clients show signs of Parkinson's disease. The company wants to involve its clients (volunteers) to test the app. Once the app is tested, it plans to deploy it.

- Can the algorithm be considered as personal data? Might some other data that is seen personal be transferred to the insurance company in the process? (Art. 4 (1) GDPR)
- If some personal data is transferred, what would be the legal ground for that? What about the legal basis for collecting data from the clients? (Art. 5.1(b) GDPR; Art. 6 GDPR)
- What kinds of procedures or technical solutions would the insurance company need to consider in developing its app (Art. 25 GDPR)?
- Considering the use case of the app, what might the GDPR's article on automatic decision making (Art. 22 GDPR) entail for the insurance company?

Digital Services Act (DSA)

Digital services and DSA

- Digital services contain a broad category of online services
  - Simple websites, internet infrastructure services (e.g. cloud and hosting services), online platforms and very large online platforms (reaching more than 10% of 450 million consumers in Europe)
- DSA primarily concerns online intermediaries and platforms such as online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms.
- Seeks to regulate for instance:
  - Trade and exchange of illegal goods, services and content online
  - Misuse of online services by manipulative algorithmic systems to amplify the spread of disinformation, and for other harmful purposes

https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

Key objectives of DSA

- For citizens: better protection of fundamental rights, transparency of advertisement, more control and choice, stronger protection of children online, less exposure to illegal content
- For providers of digital services: legal certainty, harmonisation of rules across member states, easier to start-up and scale-up in Europe
- For businesses using digital services: access to EU-wide markets through platforms, level-playing field against providers of illegal content
- For societies: greater democratic control and oversight over systemic platforms, mitigation of systemic risks such as manipulation or disinformation

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

New obligations	Intermediary services *(cumulative obligations)*	Hosting services *(cumulative obligations)*	Online platforms *(cumulative obligations)*	Very large online platforms *(cumulative obligations)*
Transparency reporting	•	•	•	•
Requirements on terms of service due account of fundamental rights	•	•	•	•
Cooperation with national authorities following orders	•	•	•	•
Points of contact and, where necessary, legal representative	•	•	•	•
Notice and action and obligation to provide information to users		•	•	•
Reporting criminal offences		•	•	•
Complaint and redress mechanism and out of court dispute settlement			•	•
Trusted flaggers			•	•
Measures against abusive notices and counter-notices			•	•
Special obligations for marketplaces, e.g. vetting credentials of third party suppliers ('KYBC'), compliance by design, random checks			•	•
Bans on targeted adverts to children and those based on special characteristics of users			•	•
Transparency of recommender systems			•	•
User-facing transparency of online advertising			•	•
Risk management obligations and crisis response				•
External & independent auditing, internal compliance function and public accountability				•
User choice not to have recommendations based on profiling				•
Data sharing with authorities and researchers				•
Codes of conduct				•
Crisis response cooperation				•

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

Other DSA obligations

- Easier reporting of illegal content
- Greater transparency in content moderation and more options to appeal
- More knowledge and choice over what we see, more control on personalisation options
- Ban of targeted advertisement to minors
- Platforms used by children to protect the privacy and security of their users as well as their mental and physical well-being, provide reporting and support tools
- Integrity of elections, mitigate risks related to disinformation
- Access for researchers to key data
- Increase traceability of business users of online marketplaces

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

Reactions to DSA

- Civil Society organisations such as Electronic Frontier Foundation have called for stronger privacy protections, Human Rights Watch has welcomed the transparency and user remedies but called for an end to abusive surveillance and profiling
- Tech companies have repeatedly criticised the heavy burden of the rules and the alleged lack of clarity of the Digital Services Act
- A bipartisan group of US senators have called the DSA and DMA discriminatory, claiming that the legislation would "[focus on] regulations on a handful of American companies while failing to regulate similar companies based in Europe, China, Russia and elsewhere."
- Nevertheless, the DSA's later stage inter-institutional negotiations, or Trilogues, have been criticized as lacking transparency and equitable participation.
- Swedish MEP Jessica Stegrud argued that the DSA's focus on preventing the spread of disinformation and "harmful content" would undermine freedom of speech

https://en.wikipedia.org/wiki/Digital_Services_Act

DSA and its ethical foundations

- Does DSA uphold and oppose similar values than GDPR? Do they share a similar moral system?
- What could be the reasons of EU adopting a particular moral system?
- What kinds of implications might DSA and GDPR have to the moral 'foundations' of the EU?

Other EU regulation of the digital sphere

Digital Markets Act (DMA)

- Aims for a fairer, more contestable digital economy
- The DMA includes rules that govern gatekeeper online platforms
    - 22 major services with a systemic role in the market as mediators between businesses and consumers
- The gatekeepers, i.e., large platforms, control important ecosystems and can exercise power as private rule-makers
- These rules can result in unfair conditions for businesses using these platforms, leading to less choice for consumers
    - Need for regulation to ensure higher degree of competition
- Objective to regulate the behaviour of the big tech firms within the European Single Market and beyond

EU AI Act (ongoing)

- AI systems used in the EU need to be safe, transparent, traceable, non-discriminatory and environmentally friendly.
- Obligations for providers and users depending on the level of risk from the AI
  - Unacceptable risk – threat to people and hence banned (e.g. social scoring)
  - High risk – negatively affect safety or fundamental rights, separate categories for products falling under EU's product safety regulation and AI systems in 8 specific areas (e.g. law enforcement, education). High-risk AI systems to be assessed before entering and while in the market, requirements on technical robustness, data training and governance, transparency, human oversight, and cybersecurity
  - Generative AI – transparency requirements, e.g., disclosure if content created by AI, prevention from generating illegal content, publish summaries of copyrighted data used for training
  - Limited risk – minimal transparency requirements that allow users to make informed decisions

https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Questions and comments?