AI + BD & EU citizens/consumers

Hans Micklitz, Przemyslaw Palka
European University Institute

Giovanni Sartor
European University Institute, Cirsfid-University of Bologna
The great convergence

- The Internet provides AI with data
- AI enables the Internet to exploit the data
Data-hungry AI meets data-abundant Internet

- Pervasive data collection
- Learning from big data
- Ubiquitous algorithmic intelligence
The AI & BD: the promise

- overcome the information overload
- world-wide generation and distribution of knowledge and solutions
- economic efficiency, wealth creation
- cost-effective, individualised private and public services
- environmental-friendly management of utilities, traffic, logistics
- support for transparency, overcome bias and discrimination
- etc.
The AI & BD: The catch

- Data collection/analysis/surveillance
- We cannot get out of the infrastructure
- We cannot effectively resist/contest influence and manipulation
Ethics and law violations by AI + BD

By 2018, 50% of violations of business ethics will be performed by algorithms

Gartner 2016
What answers?

• Competition
  • To limit market power. Will it work? Are there natural monopolies (network effect)?

• Regulation
  • To direct the use of AI+BD by private and public organisations
    • https://artsy.eui.eu/

• Empowerment
  • To make the power of AI+BD available to citizen and civil society
    • https://claudette.eui.eu/
A value-based approach to regulating AI

A disrupting flow of innovations, generates multiple and diverse legal/social issues

How to proceed:

• Start from first principles
• Promote valuable socio-technical practices through tailored regulations and technologies
• Adapt existing legal frameworks, multi-layered regulation

Individual and social values

Social practices and technologies to protect/enhance values

Regulatory solutions to induce/enforce practices, make technologies available
The legal-ethical framework: rights and social values

• Human/fundamental rights:
  • privacy, data protection, dignity, autonomy, freedom of expression, non-discrimination, equality, participation

• Social/economic goals:
  • welfare, competition, efficiency, science, art and culture, cooperation, civic dialogue, democracy
The legal framework: Multiple sectorial legal regimes and principles

• Data protection law
  • Principles: lawfulness, fairness and transparency; purpose limitation; data minimisation, accuracy; integrity and confidentiality; accountability; legitimate interest, data subject rights, etc.

• Consumer protection law
  • Principles: Protection of the weaker party, Regulated autonomy, Non-discrimination, etc.

• Competition law
  • Principles: fair competition, consumer welfare, etc.
Synergy and tensions: EDPS Opinion On Package “A new deal for consumers”

• **Consumer** and **data protection law** share common goals of **redressing imbalances of informational and market power**

• Together with **competition law**, data protection and consumer protection need to work to ensure that people are **treated fairly**.

An issue: **are personal data a tradable property?**

• Can a consumer pay with his or her data? What about revocable consent under GDPR? What about privacy as a fundamental right?
What interests/rights are at stake

• Privacy-data protection
  • to lawful and proportionate processing of personal data, to control processing

• Fair algorithmic treatment
  • not to be subject to unfair differentiated treatment

• Algorithmic transparency
  • to know why a certain algorithmic response or decision has been given

• Interest in fair algorithmic interaction
  • not to be misled or manipulated

• Interest in fair algorithmic (cognitive) competition
  • Interest in accessing data sources and algorithms that are available to big players
Focus on risks for consumers

- Unfair algorithmic decisions
- Unfair, excessive data processing/profiling
- Limitations on consumers’ autonomy
- Discriminatory/unfair/ aggressive/exploitative advertising
- Filter bubbles/echo chambers
- Information asymmetry; arbitrary power
- Exploitation of vulnerabilities
- Opacity, inability to contest
- Risk of erroneous diagnoses, suggestions
Issue: Price discrimination

- AI enables sellers to figure out the highest price a client can pay
- Should there be price discrimination in consumer retail markets? For what good/service, on what grounds? 
  - cost structures, risks 
  - spending capacity, needs, interests, vulnerabilities 
- What legal response: 
  - Consumer protection law: is it unfair/discriminatory? 
  - GDPR: is it an automated decision, is there a legitimate interest? A free consent?  
  - Competition law: does this affect competition?
Issue: Discrimination in algorithmic offers

• What if different people are offered different opportunities
  • Men getting better loans, women better insurance
  • People of certain ethnicity being more often refused opportunities

• What if the AI system has “innocently” learned to apply differential treatment
  • based on previous practice
  • to achieve a business purpose

• What legal response
  • Data protection law: legitimate purpose, sensitive data, consent?
  • Consumer protection law/discrimination law: unacceptable discrimination?
Issue. Targeted advertising/malicious nudging

• AI can deliver each consumer the ads that most trigger purchasing, depending on:
  • how well they match consumer’s needs and interest
  • how well they exploit consumer’s vulnerabilities (e.g., predatory loans to people in difficulties, gambling offers to gambling addicts, drugs to depressed people)

• What legal response?
  • When is it permissible? When a prevailing “legitimate interest”? 
  • When does it “materially distort the economic behaviour of consumers”
Issue: Aggressive personalised advertising

• What if personalized advertising, to maximize clicks and revenues, exploit individual vulnerabilities (economic hardship, propensity to gambling, etc.)
  • This may be non-intentional, as the system may just aim to use any factors correlated to clicks and purchases

• What legal response?
  • Data protection law: Is exploiting vulnerabilities acceptable?
  • Consumer protection law: does it count as “aggressive advertising”
Issue: Discrimination in Ad delivery

• Systems meant to address Ads and offers to those who are most probably interested in them may reproduce biases and discrimination
  • Offers for top jobs to male people
  • Offers for houses to those who match current ethnic ownership

• What legal response?

• Unlawful processing of sensitive data? Is there a discrimination issue?
Issue: “Turn off” personalization?

• Personalised treatment of consumer can provide the with advantages, but also disadvantages

• What legal response?
  • Have consumers a right that they profiled, for what specific purposes?
  • Should consumers be offered the option to trade and purchase anonymously?
  • The GDPR allows consumer to withdraw consent and object to profiling. Is there a right to trade anonymously?
Issue. Rights to information/transparency

• Have (should have) consumers a right to know that they are offered personalised prices? Calculated in what way?

• Have (should have) consumers a right to know to know that their treatment is dependant on the tracking of their behaviour, and on consequent classifications/profiling? With what impacts?

• What legal response
  • Data protection law: information obligations on data controllers
  • Consumer protection law: information obligations on suppliers
  • What about platforms?
Other issues to be addressed

• Right to procedural regularity
• Right to substantive legality
• Right to explanation/justification
• Right to have a human answer
• Right to be protected from abusive manipulation
• Liabilities for mistaken decisions/advice
Powers and Synergies: What answers

How to address imbalances in Knowledge (Data) Technologies (AI) Resources (Market power)
Countervailing power

• An opposing exercise of power is the principal solvent of economic power, the basic defense against its exercise in economic affairs (J.K. Galbraith)

• How to enable civil society to achieve
  • Awareness
  • Accountability
  • Contestation
  • ...
Empowering civil society?

• Remedy the imbalance for AI-powered platforms and suppliers through citizen and consumer-empowering AI
  • Protection against unwanted monitoring
  • Support in detecting unfair/unlawful use of AI
  • Control over fairness of commercial practices

• Some examples:
  • Spam filters
  • Ad-blocking tools
  • Anti-tracking tools
  • Price comparison platforms
  • Detection of, and response to, violations of law and ethics

• Should consumer-empowering initiatives be supported and incentivised?
Detect, and respond to, violations of law and ethics

- AI can contribute to address online violations:
  - Unlawful and unethical behaviour often unnoticed, rarely acted upon.
  - AI for cost-effective prevention/detection/reaction

- The AI-empowerment should be available to those who most need it:
  - Commercial actors, and resourceful individuals already use AI to apply the law
  - This opportunity should be open to citizens and civil society
What about privacy policies and terms of service?

• Most online terms of service and privacy policies contain unlawful/unfair clauses, or miss relevant information:
  • Consumers agree but don’t read
  • NGOs (consumer organisations) lack resources

• AI can contribute:
  • AI support to citizens and civil society to detect and react
  • An example: An automatic detector of unfair clauses in online contracts and privacy policies: https://claudette.eui.eu/
Thanks for your attention

Giovanni Sartor, European University Institute / University of Bologna