

# ÍNDICE

## INTRODUCTION

### CHAPTER I

#### **AN INTRODUCTION TO ALGORITHMIC DECISION-MAKING**

##### **1. Big data**

- 1.1. The three Vs in big data*
- 1.2. The need to process (raw) big data*
- 1.3. The fourth V: value*

##### **2. Data processing tools and technologies**

- 2.1. Machine learning and data mining*
- 2.2. Supervised and unsupervised learning*
- 2.3. Algorithms and models*

##### **3. The application of automated systems**

- 3.1. The use of algorithms by the private sector*
  - 3.1.1. Scoring individuals
    - 3.1.1.1. The banking sector and the expansion of credit scores
    - 3.1.1.2. Healthcare
    - 3.1.1.3. Human resources
  - 3.1.2. Consumer profiling and advertising
- 3.2. The use of algorithms by the public sector*
  - 3.2.1. The use of algorithms in public service management and provision
    - 3.2.1.1. The use of algorithms in public aid and welfare programmes
    - 3.2.1.2. Automation of public services, aid and welfare programmes and the perpetuation of inequality
  - 3.2.2. The use of algorithms in public administration's regulatory and coercive activity: law enforcement
    - 3.2.2.1. Police departments and the criminal justice system
    - 3.2.2.2. Other algorithmic applications in the exercise of administrative regulatory and coercive powers

##### **4. Types of algorithmic decision-making**

- 4.1. Automatic and autonomous systems*
- 4.2. Automated and semi-automated systems*
- 4.3. Profiling and automated decision-making: descriptive, predictive, classification and recommendation purposes*

### CHAPTER II

#### **RISKS AND HARMS GENERATED BY THE USE OF AUTOMATED SYSTEMS**

##### **1. Problems and risks for the protection of the rights of individuals subjected to automated decision-making**

- 1.1. *Biases and errors*
  - 1.1.1. Biased humans and accurate machines
  - 1.1.2. Measuring baseball vs. measuring humans
  - 1.1.3. Human bias and machine error
  - 1.1.4. The technological heuristic
- 1.2. *Algorithmic discrimination*
- 1.3. *Risks to dignity: individuality, autonomy and privacy*
- 1.4. *Transparency, due process and traceability*
  - 1.4.1. Transparency
  - 1.4.2. Justification and understandability
  - 1.4.3. Participation and due process
  - 1.4.4. Traceability
- 2. The legitimacy and legality of public automated decision-making**
  - 2.1. *Transparency and justification of public decisions*
    - 2.1.1. The private exercise of inherently public tasks
- 3. Market failures and intervention in the private sector**
  - 3.1.1. The precautionary principle
  - 3.1.2. Market failures and other problems generated by the data services sector
    - 3.1.2.1. Negative externalities
    - 3.1.2.2. Monopolistic behaviour
    - 3.1.2.3. Asymmetric information, imperfect rationality and transaction costs

## CHAPTER III

### **THE INFORMATIONAL PRIVACY FRAMEWORK. GENERAL ASPECTS**

- 1. The informational privacy framework as a solution for the harms caused by algorithms**
  - 1.1. *The right to data protection as an anti-classification instrument*
  - 1.2. *The fundamental right to data protection*
- 2. EU and US privacy traditions**
- 3. The scope of application of informational privacy regulations**
  - 3.1. *Anonymisation*
  - 3.2. *Pseudonymisation*
  - 3.3. *Scope of application of the EU's data protection framework*
- 4. Privacy principles**
  - 4.1. *Data processing principles: lawfulness, fairness, transparency, integrity and confidentiality*
  - 4.2. *Data collection principle: purpose limitation*
  - 4.3. *Data and storage requirements: data minimisation, accuracy and storage limitation*

## CHAPTER IV

### PROHIBITIONS TO ACCESS AND PROCESS INFORMATION

#### 1. The US approach to protection through data collection and processing prohibitions

- 1.1. *The Health Insurance Portability and Accountability Act*
- 1.2. *The Americans with Disabilities Act*
- 1.3. *The Genetic Information Nondiscrimination Act*
- 1.4. *The Family Educational Rights and Privacy Act (FERPA)*
- 1.5. *The Fair Credit Reporting Act (FCRA) and Equal Credit Opportunity Act (ECOA)*

#### 2. Privacy as anti-discrimination through general prohibitions in the GDPR

- 2.1. *Processing special categories of personal data*
  - 2.1.1. Scope of the prohibition
    - 2.1.1.1. Personal scope of application: search engine operators
    - 2.1.1.2. Material scope of application: the proxy problem
    - 2.1.1.3. Solutions for the discrimination by proxy problem
  - 2.1.2. Processing of personal data relating to criminal convictions and offences
- 2.2. *The right (or general prohibition) not to be subject to decisions based solely on automated processing, including profiling*
  - 2.2.1. The right not to be subject to a decision based solely on automated processing, including profiling
  - 2.2.2. Exceptions to the right (prohibition) recognised in article 22 and safeguards
  - 2.2.3. Special protections for decisions based solely on the automated processing of special categories of personal data
  - 2.2.4. Issues raised with regard to the scope of article 22.1
    - 2.2.4.1. Decisions based solely on automated processing
    - 2.2.4.2. Legal or significantly similar effects
  - 2.2.5. Analysis of the exceptions to the right not to be subject to a decision based solely on automated processing, including profiling
    - 2.2.5.1. Necessary for entering into, or performance of, a contract
    - 2.2.5.2. Authorised by EU or member state law
    - 2.2.5.3. The data subject's explicit consent
    - 2.2.5.4. Additional elements that must concur for applying the exceptions to the processing of special categories of personal data

#### 3. Prohibitions in the Directive for personal data protection in law enforcement and the criminal justice system

- 3.1. *Harmonisation and scope of application*
- 3.2. *Processing special categories of personal data within the scope of Directive 2016/680*
- 3.3. *The prohibition of decisions based solely on automated processing, including profiling*

#### **4. Shortcomings in the prohibitions contained in the eu personal data protection framework**

##### CHAPTER V

#### **TECHNOLOGICAL DUE PROCESS RIGHTS**

##### **1. The informational self-determination approach**

##### **2. Transparency: The rights to information, access and explanation**

###### *2.1. Information, access and explanation rights in the GDPR*

###### 2.1.1. The right to be informed

###### 2.1.1.1. The intended purposes of the processing

###### 2.1.1.2. Meaningful information about the logic involved, significance and envisaged consequences

###### 2.1.2. The right to access

###### 2.1.3. The right to explanation

###### 2.1.3.1. Internal limits to the right to explanation

###### 2.1.3.2. External limits to the right to explanation

###### i) The conflict with trade secrets and intellectual property

###### ii) State secrets and public interests

###### 2.1.3.3. How the right to explanation can be made effective

###### *2.2. Information, access and explanation rights in Directive 2016/680 for data protection in law enforcement: the conflict with state and public security*

###### *2.3. Information, access and explanation rights in US regulatory instruments*

###### 2.3.1. The Fair Credit Reporting Act (FCRA)

###### 2.3.2. The California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

###### *2.4. A few final remarks with regard to the transparency principle and the rights that derive from it*

##### **3. The right to be heard and contest decisions: the right to an effective remedy**

###### *3.1. The right to be heard and contest decisions in the GDPR*

###### 3.1.1. Data subjects' due process rights in art. 22

###### 3.1.1.1. The right to obtain human intervention

###### 3.1.1.2. The right to express his or her point of view

###### 3.1.1.3. The right to challenge the decision

###### 3.1.2. Individual rights to be heard and challenge decisions recognised outside of article 22 of the GDPR

###### 3.1.2.1. The rights to data portability, rectification, erasure and restriction of processing

###### 3.1.2.2. The right to object

###### 3.1.2.3. The rights to lodge complaints before supervisory authorities and to judicial remedies

###### *3.2. The rights to be heard and challenge decisions in Directive 680/2016*

###### *3.3. Rights to be heard and challenge decisions in US regulatory instruments*

- 3.3.1. The Fair Credit Reporting Act
- 3.3.2. The California Consumer Privacy Act and California Privacy Rights Act
- 4. The need to complement technological due process rights with a system for algorithmic oversight and control**

## CHAPTER VI

### **REGULATORY MECHANISMS FOR SYSTEM TRANSPARENCY AND ACCOUNTABILITY THROUGH DATA PROTECTION**

#### **1. Regulatory frameworks**

- 1.1. Self-regulation*
- 1.2. Co-regulation (or regulated self-regulation)*
- 1.3. Regulation (state intervention)*

#### **2. The GDPR as a system of governance**

#### **3. System transparency and accountability**

#### **4. Regulatory Tools For System Transparency And Accountability**

##### *4.1. Rule-setting mechanisms*

- 4.1.1. Safe harbour and privacy shields
- 4.1.2. Codes of conduct
- 4.1.3. Technical and organisational standards

##### *4.2. Control mechanisms*

- 4.2.1. Certification mechanisms
  - 4.2.1.1. General issues
  - 4.2.1.2. Certification in the GDPR
- 4.2.2. Data protection impact assessments
- 4.2.3. Re-certification, DPIA reviews and audits

##### *4.3. Enforceability mechanisms*

- 4.3.1. Ethics committees and data protection officers
- 4.3.2. The European Data Protection Board and Data Protection Authorities
- 4.3.3. Penalties

## CHAPTER VII

### **THE PRIVACY FRAMEWORK: SHORTCOMINGS AND TENSIONS**

#### **1. General shortcomings of the privacy approach**

- 1.1. The unrealistic expectations of anonymisation*
- 1.2. The limits of personal data protection*
  - 1.2.1. Group profiling
  - 1.2.2. Output data
  - 1.2.3. Failure to focus on varieties of processing

#### **2. The shortcomings of the informational-self determination approach**

- 2.1. The myth of consent and the privacy paradox*
- 2.2. Asymmetric information and burdens*

2.3. *Creating systemic inaccuracies*

2.4. *The difficulty of detecting systemic errors*

### **3. Privacy approaches are not appropriate for the use of algorithms by the public sector**

3.1. *Private sector limits to transparency for algorithms used by public bodies*

3.1.1. Intellectual property and the Spanish “energy social bond”

3.1.2. Administrative courts granting transparency

3.2. *Banning the use of algorithms in the public sector: the Dutch “SyRI” case*

3.3. *The regulatory nature of algorithms employed by public administrations*

3.3.1. Algorithms used by public administrations are legal instruments

3.3.2. Algorithms are regulatory instruments

3.3.2.1. Proposals that reject the regulatory nature of algorithms

3.3.2.2. Administrative court of Lazio-Roma, Judgment No. 3769

3.3.2.3. Solely automated non-binding and semi-automated decision making

3.3.2.4. The importance of recognising the regulatory nature of algorithms

3.3.3. The principle of legality must apply to the public use of algorithms

3.3.4. Frictions between traditional and algorithmic regulation

### **4. The shortcomings of accountability mechanisms**

### **5. The relationship between personal data protection, equality and non-discrimination**

5.1. *The privacy vs. antidiscrimination dilemma*

5.1.1. Less information can lead to wrong inferences

5.1.2. Anti-classification does not prevent indirect algorithmic discrimination

5.1.3. Anti-classification through privacy does not solve group disadvantage and can reinforce it

5.2. *Combining the anti-discrimination and data protection frameworks*

## **CHAPTER VIII**

### **POSSIBILITIES AND PROPOSALS FOR THE REGULATION OF ALGORITHMS**

#### **1. Trade-offs in the regulation of algorithms**

#### **2. The need for more algorithmic transparency**

#### **3. A system of public intervention to control algorithms**

3.1. *Organisational options*

3.1.1. Algorithmic control mainstreaming

3.1.2. Creating a non-independent supervisory task force or body

3.1.3. An independent supervisory agency

3.2. *Risk-based market approval of algorithms*

3.2.1. The three (plus two) tier system

3.2.1.1. Prohibited algorithmic systems

3.2.1.2. High-risk algorithmic systems

- i) Administrative testing, documentation and general explanation requirements
- ii) Justification and explainability requirements
- iii) The proportionality analysis of pre-market authorisations
- iv) Specific requirements for public sector algorithms included in this category

3.2.1.3. Medium-risk algorithmic systems

3.2.1.4. Low-risk algorithmic systems

3.2.1.5. Non-risky algorithmic systems

3.2.2. System enforcement

3.3. *Public procurement as a mechanism to prevent the risks of the public and private use of algorithms*

3.4. *Establishing a “best available techniques” regime*

3.5. *Using algorithms to detect discrimination*

3.6. *Empowering individuals through understandable information: choice architectures*

3.7. *Increased communication between disciplines and establishing general principles upon which to construct automated systems*

CONCLUSIONS

BIBLIOGRAPHY