Table of contents

Outline 5

Avant-propos 9

Foreword 13

PART 1
GOVERNANCE AND REGULATION

CHAPITRE 1. – Le fonctionnement du marché intérieur de l'Union européenne devrait-il être repensé pour intégrer les impacts environnementaux des technologies numériques ? 19
Camille BOURGUIGNON

Introduction 19

I. – L'absence d'intégration des enjeux environnementaux dans le principe de libre circulation des services de la société de l'information 26

II. – Les conséquences de l'absence d'intégration des enjeux environnementaux dans le principe de libre circulation des services de la société de l'information 33

III. – L'intégration souhaitable des enjeux environnementaux dans le principe de libre circulation des services de la société de l'information 38

Conclusion 42

CHAPTER 2. – How Blockchain Could Impact the Relationship Between Public Authorities and SMEs 43
Ludovic DESCHAMPS
Matthieu HARDY

Introduction 43

I. – The revolutionary potential of blockchain 44

II. – The specific needs of SMEs 46

III. – European initiatives to support the development of blockchain 47

IV. – Opportunities to Support Belgian and European SMEs Through DLTs 49

A. Regulated profession, freedom of movement and mutual recognition 49

1. Regulated profession: what, why, how? 49

2. DLTs to enforce the regulation of professions? 51

3. Implication on the relations between authorities and SMEs 52

4. Freedom of movement and mutual recognition 53

B. Public procurement and access to SMEs 55

1. Principles 55

2. Modalities and structuring in the context of public procurement 56

3. The procedures related to public procurement 57

4. Central purchasing body 57

5. Mandatory grounds for exclusion 58

Conclusion 58

CHAPITRE 3. – *Pornhub* selon une perspective cyberféministe : Vers une responsabilité coopérative et une gouvernance multiniveau 61

Évelyne Jean-Bouchard
Sandrine Prom Tep
Maya Cachecho

Introduction 61

I. – *Pornhub* et la gouvernance des plateformes 62

II. – Le consentement et le droit à l'oubli numérique 66

III. – Le cyberféminisme 68

IV. – Les responsabilités partagées 71

A. Les plateformes 71

B. Les utilisateurs 72

V. – L'État 74

Conclusion 76

PART 2
Enforcement and Compliance

CHAPTER 1. – The directive on whistleblowers to the test of the digital society: Between hope and desillusion 79
Dimitrios Kafteranis & Amélie Lachapelle

Introduction 79

I. – Why do we need to take seriously persons who blow the whistle in the digital technology area? 81
A. The need to ensure security of networks and information systems 81
B. The need to have watchdogs in the digital environment to ensure the respect for human rights 83

II. – Is the "technological risk" totally covered by the scope of the Directive? 84
A. Reporting channels in the privacy, data protection and cybersecurity area 85
B. The whistleblower, a vital link in the risk management policies 87
C. The Union acts mentioned in the Annex of the DWB 89

III. – Are all the potential whistleblowers in digital technology matters covered by the Directive? 90
A. The work-related context 91
B. The motivation of the reporting person 93
C. The granting of a bounty 94

Conclusion 95

CHAPTER 2. – The Role of User-Generated Evidence in Criminal Investigations Versus the Removal of Terrorist Content Online: Towards a More Balanced Approach 97
Eline Labey
Juncal Montero Regules

Introduction 97

I. – User-Generated Evidence and the Role of SMPs 98

II. – Case Study: YouTube and The Syrian Armed Conflict 101

III. – EU'S Strategy to Counter the Spread of Terrorist Content Online 103
A. EU Initiatives and Soft Law Instruments 103
1. EU Internet Forum 103
2. EU Internet Referral Unit ("EU IRU") 104
3. EU Crisis Protocol 105
4. EU Security Union Strategy 105
5. New Counter-Terrorism Agenda 106
B. Terrorist Content Online Regulation 107
1. Geographical, personal, and material scope 107
2. Obligations for HSPs 108
3. Competent authority of the EU Member State 110
4. Penalties 110
5. Use of automated means 110
6. Towards more removal of terrorist content online? 111
Conclusion and Recommendations 112

CHAPTER 3. – Mandatory Information under GDPR: A Conceptual Model for Automated Privacy Policy Analysis 115
Sébastien Meeùs

Introduction 115

I. – Purposes 116

II. – Overview of the key elements of privacy policies 118
A. A construction resulting from practice 118
B. The legal obligations, principles, and rights that shape privacy policies 118
C. The function(s) of privacy policies 119

III. – The compliance of privacy policies 120
A. The tasks of compliance checking 120
1. Document to Regulation 120
2. Document to Document 120
B. Current and prospective assessment methods 121

IV. – Shaping the "Mandatory Information" 121
A. Information to be provided in accordance with Articles 13 and 14 121
1. Information that must always be mentioned in the document 122
2. Optional information 122
3. Challenges 123

B. Children and consent 124
1. Age of consent 125
2. Evidence of consent 125
3. Challenges 126
C. Security measures 126

V. – Building and testing the conceptual model 127
A. Conceptual model 127
1. Research basis 129
2. Metadata relationships 129
B. Human-annotated privacy policies 131
C. Early results 132

Conclusion and future work 132

CHAPTER 4. – Personal data class actions three years after the application of the GDPR 135
Grégory Renier

Introduction 135

I. – Representation & Collective Redress in the GDPR 138

II. – The solution established in Belgian and French law 139
A. Action for Collective Redress in Belgium 139
1. The scope of application of the action for collective redress 140
2. Presentation of the procedure 142
B. The solution enshrined in French law: Group Action in France 143
1. Representation in matters of personal data 143
2. Presentation of the procedure 144

III. – Areas of application and role of supervisory authorities through the illustration of recent decisions 146
A. Specific data protection provisions 146
1. The GDPR and the Privacy Directive 2002/58/EC 146
2. Other specific provisions: the example of consumer credit 147
3. Codes of conduct? 147
B. General or cross-cutting data protection provisions 148
1. Unfair commercial practices 148
2. Unfair terms 150
3. Anti-competitive practices 151

IV. – The adoption of Directive (EU) 2020/1828 on representative actions: what to expect? 153

Conclusion 155

CHAPITRE 5. – ARRCIS : Évaluation et renforcement de la conformité réglementaire d'un système d'information 159

Antoine Sacré
Jean-Noël Colin
Benoît Hosselet

Introduction 159

I. – Une solution : faciliter l'évaluation de la conformité des systèmes 161

II. – Travaux connexes 162

III. – Modélisation des normes 164

A. Normes prises en compte 164

B. Caractéristiques de la modélisation 164

C. Extractions des informations 165

D. Modélisation des informations 166

IV. – Méthode d'évaluation de la conformité des systèmes d'information 168

A. Sélection des exigences pertinentes 169

Questionnaire 169

B. Processus d'évaluation de la conformité 171

V. – Application à un cas et discussion 172

Conclusion 174

Bibliographie 175

CHAPTER 6. – Freedom versus Security: Methods of Controlling Information Access by Intelligence and Law Enforcement Agencies 177

Pál Vadász
Zsolt Ződi
Csaba Csáki

Introduction: who guards the guards? 177

I. – Emergence of disruptive technologies 179

II. – Potential irregularities in the practices of LEA and IC organizations 180

III. – Arguments in favor of relaxing legal constraints 180
IV. – Tools and methods to ensure oversight 182
V. – Procedural tools and methods to ensure oversight 182
VI. – Technical tools and methods to ensure oversight 184
VII. – The legal framework to ensure oversight 185
Conclusion 188
References 189

PART 3
DATA

CHAPTER 1. – High-altitude surveillance and data protection: Space, the final frontier of privacy? 195
Anne-Valentine RENSONNET
Alexandre CASSART

Introduction 195

I. – Delimitation Between Airspace and Outer Space 197
A. Air Law 198
B. Outer Space Law 198
The Resolution on the Principles of Remote Sensing and its weaknesses 201

II. – The Processing of Data in Outer Space and Privacy 203
A. Is the GDPR Applicable in Outer Space? 204
1. Establishment Criterion 204
2. Targeting Criterion 204
3. Extension by Virtue of Public International Law 205
B. Material Scope 206
1. Personal data – Possible identification 206
2. Exclusions 206

Conclusion 207

CHAPTER 2. – The end of third-party cookies: nothing but smoke and mirrors if the RTB winner takes it all? 209
Fanny COTON
Victoria RUELLE

Introduction 209

I. – Cookies and Their Heirs 210

A. Legislative Frame 210
1. E-Privacy Directive and GDPR 210
2. Future E-Privacy Regulation 211
3. Legislative Gaps: The Cookie Wall and the Pay Wall 214
B. Third-Party Cookies: Raw Material for RTB 217
C. Federated Learning of Cohorts (“FLoC”): The Google Alternative 219
D. First-Party Cookies: A Better Alternative? 222
E. Competition Issues 223

II. – Real Time Bidding: A GDPR-Compliant Mechanism? 224
A. Consent 226
1. Informed Consent and Transparency 228
2. Explicit Consent 229
3. Proof of consent 230
B. Qualification of Actors 231
C. Data Minimization 231
D. Security 231

III. – Perspective 232

CHAPITRE 3. – Le consommateur de données 235
Malo Depincé

I. – Le consommateur qui transfère 240
A. Les dispositions spécifiques du règlement général sur la protection des données personnelles 240
B. Les dispositions générales du Code de la consommation 243

II. – Le consommateur qui reçoit 246
A. Le service reçu et sa conformité 247
B. Le droit au retour des données : la portabilité 248

CHAPTER 4. – Privacy concerns related to the digital tax administration 2.0 253
Sylvie De Raedt

Introduction and limitation of the scope of this contribution 253

I. – The extent of the legal protection in the post GDPR era – research question and methodology 255

II. – The intentions of the legislator in repealing the existing model 257

III. – The scope of the protocol duty 260
A. The risk of exchanging personal data that is not strictly necessary for the legitimate purpose of the public authority 260
B. The risk of incompatible reuse 263
C. The risk of non-transparent exchange of information 265
IV. – Are we going backwards? 267

CHAPTER 5. – All's FAIR in Europe? 269
Freya De Schamphelaere

Introduction 269
I. – From Public Sector Information to Open Data 272
A. Public Sector Information directives 272
B. Open Data movement 274
C. Open Science movement 274
D. Open Data Directive 275
II. – Definition of research data 276
A. Characteristics of the definition 276
1. Digital form 276
2. Other than scientific articles 276
3. Evidence or commonly accepted 277
4. Also including meta data 277
B. Research data as collected by the SODHA – repository 277
III. – Principles governing the availability of research data (Art. 10, § 1 Open Data Directive) 278
A. Principles 279
1. Principle of 'open by default' 279
2. FAIR – principles 279
3. 'As open as possible, as closed as necessary' 280
B. Access to research data through the SODHA repository 281
1. Open access vs restricted access 281
2. Access to sensitive research data 282
IV. – Re-use of research data (Art. 10, § 2 Open Data Directive) 284
A. Re-use of research data 284
1. Re-usable research data is publicly funded 284
2. Re-usable research data has already been made available 285
3. Beware of other interests 285

B. Re-use through the SODHA repository 286
1. General information 286
2. Three re-use regimes 286

V. – All's FAIR in Europe? 287
A. Availability of research data 287
B. Re-use of research data 288
C. All's fair in Europe? 288

CHAPITRE 6. – Big Data dans l'IA et principe de minimisation : Défis et risques 289
Sophie Everarts de Velp

CHAPITRE 7. – Données à caractère personnel et sécurité des systèmes d'information : quand faut-il siffler la fin de la récréation ? 299
Jean-François Henrotte
Fanny Coton

Introduction 299

I. – Violations dont le signalement est protégé 302
A. Dispositions dont la violation est concernée 302
B. Notion de « violation » 303
C. Cas de « violations » envisageables 304
1. Violations de sécurité impliquant une obligation de notification du responsable 304
2. Niveaux de sécurité inadéquats 307
3. Faits sanctionnés pénalement 308
4. Non-respect des recommandations et lignes directrices 309

II. – Cheminement de l'alerte 310
A. L'obligation de désigner un DPD 310
B. Le DPD échelon du système d'alerte 311
C. Signalement à l'autorité compétente 312
D. Signalement au grand public 314
1. En tant qu'ultime échelon du système d'alerte 314
2. Directement 315

III. – Le DPD, lanceur d'alerte ? 315
A. Cadre 316
B. Mission particulière du DPD 317

C. Obstacle ? 318
D. Application du système d'alerte mis en place au DPD 319

Conclusion 319

CHAPTER 8. – Automated Decision-Making Under Amsterdam's District Court Judgements: 321
Guillermo Lazcoz

Introduction: Algorithmic regulation in the legal discussion 321

I. – Uber transparency request case – UTR – 323

II. – Ola transparency request case – OTR – 325

III. – Uber deactivation case – UD – 327

IV. – Algorithmic regulation and the GDPR in the Amsterdam District Court's judgements 328

V. – Limitations to the right of access 330

VI. – Art. 22(1): General prohibition or a right to object on request? 331

VII. – The production of legal or significant effects 332

VIII. – Human intervention in 22(1) decisions 333

IX. – Is there a right to an explanation for decisions based solely on automated processing? 334

Conclusions and future work 335

Acknowledgements 336

References 336

CHAPTER 9. – Big Boss is Watching You: Is Technology a Good or a Bad Thing for Human Employees? 339
Nicolas Roland

I. – Setting the scene 339

II. – What is the current and prospective legal framework? 342
A. Privacy is a cornerstone 342
1. Privacy is a fundamental human right 342
2. The regulation is multifold 343
3. What do the judges look for? 343
4. So, what to keep in mind? 345

B. Is there any "right to disconnect"? 345
C. Does technology conflict with the "well-being at work" legislation? 346
III. – Concluding remarks 347

PART 4
Contract and Liability

CHAPTER 1. – Agile Project Management and Contract Law 351
Alexandre Cruquenaire
I. – Agile (Scrum) in a nutshell 352
II. – Legal questions raised by the use of Agile in IT contracts 353
A. The scope of the advice obligation 353
B. The collaboration obligation 355
C. The acceptance of the provided services 356
D. The scope of the warranty obligation 358
Conclusion 358
CHAPITRE 2. – Quelques réflexions sur la rencontre des véhicules autonomes avec le droit des assurances 359
Thomas Derval
David-Alexandre Sauvage
Introduction 359
I. – L'assurance obligatoire de la responsabilité en matière de véhicules automoteurs 366
A. Présentation de la loi du 21 novembre 1989 366
B. Rencontre entre la loi du 21 novembre 1989 et les véhicules autonomes 373
II. – Le futur de l'assurance (responsabilité civile) face aux véhicules autonomes 378
Conclusion 384

CHAPTER 3. – Intermediary liability and freedom of expression in the algorithmic age: swaying the balance? 387
Valentina GOLUNOVA

I. – Introduction 387

II. – Algorithmic Content Moderation 389

III. – Impact of Algorithmic Content Moderation on the EU "Safe Harbour" Regime 392
A. "Passive" v. "active" providers 392
B. Knowledge test 394
C. Expeditious action 396
D. Prohibition on general monitoring 399

IV. – Impact on the Freedom of Expression 401

V. – Conclusion 402

PART 5
ARTIFICIAL INTELLIGENCE

CHAPITRE 1. – Les armes létales autonomes et le droit international humanitaire : le nécessaire contrôle humain sur l'usage de la force 407
Noémi BONTRIDDER

Introduction 408

I. – C'est au combattant humain qu'incombe l'obligation de respecter les principes de distinction, de proportionnalité et de précaution 415
A. Les machines ne sont pas liées par le droit 415
B. Seul le combattant humain est légalement habilité à participer directement aux hostilités 419
C. Une attaque est lancée dès l'activation d'une arme 421

II. – Le combattant doit évaluer si l'attaque est conforme au principe de distinction 422
A. La détermination des cibles humaines légitimes est complexe 423
B. La détermination du caractère militaire d'un objectif nécessite un jugement 426

C. La sélection et l'engagement d'une cible par une arme autonome sont intrinsèquement imprévisibles 427

III. – Le combattant doit évaluer si l'attaque est conforme au principe de proportionnalité 432

IV. – Le principe de précaution doit être appliqué par les humains qui préparent ou décident l'attaque 435

Conclusion : un prescrit légal, reflet de considérations éthiques 437

CHAPTER 2. – From the Regulation of Artificial Intelligence by Society to the Regulation of Society by Artificial Intelligence: All Along the Watchtower 441
Jerome De Cooman

Introduction 441

I. – Regulation by Design: Two-Dimensional Definition Proposal 444

II. – Regulation of Human Behavior by Design 448
A. Automated Enforcement 450
B. Recommender systems 456

III. – Regulation of Technology by Design: The Case of Privacy 465

IV. – Laws of AI Designers 473

Conclusion 482

CHAPTER 3. – Breaking into the Black Box: How to Build Trust between Machine Learning-based Systems and their Users 485
Benoit Frénay
Bruno Dumas

I. – A Need for Machine Learning-Based Systems that Can Be Trusted 486

II. – Interpretability & Explainability, Interactivity, Constraint Enforcement 487

Conclusion 489

References 489

CHAPTER 4. – AI as a Medical Device: Between the Medical Devices Framework and the General AI Regulation 491
Anastasiya Kiseleva

I. – Introduction 491

II. – How Does the EC Proposal for AI Regulation Deal with Limitations of the Medical Devices Framework in Terms of AI's Transparency and Accountability? 493
A. Limitations in the Regulated Subjects 493
B. Limitations in the Regulatory Scope 495
C. Limitations in Procedures 496
1. Self-learning of AI 496
2. Control over data 498
III. – The Synergy of the Two Frameworks 499
IV. – What Else Is Needed 501
V. – Conclusion 507

CHAPTER 5. – Negotiating the Legal Status of Artificial Intelligence Systems in Future Societies 509
Diana Mădălina Mocanu

CHAPTER 6. – About some international documents relating to the ethics of Artificial Intelligence – Some insights 523
Yves Poullet

Table of contents 541