SECURITY AND LAW
SECURITY AND LAW

Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security

Anton Vedder  
Jessica Schroers  
Charlotte Ducuing  
Peggy Valcke  
(eds.)
# CONTENTS

*List of Contributors* .............................................................. xiii

Chapter 1.
Introduction: Security and Law in a Digitizing World
Charlotte Ducuing, Jessica Schroers and Anton Vedder .............. 1

Chapter 2.
Safety, Security and Ethics
Anton Vedder ................................................................. 11

1. Introduction ................................................................. 11
2. Definitions and distinctions ........................................... 11
3. Security and safety as values in ethics and normative political theory . 15
4. Security and safety in conflict ................................. 19
5. Conclusion ................................................................. 21
Acknowledgement ............................................................ 23
Bibliography ................................................................. 23

Chapter 3.
National and Public Security within and beyond the Police Directive
Plixatra Vogiatzoglou and Stefano Fantin ....................... 27

1. Introduction ................................................................. 27
2. The scope of the Data Protection Law Enforcement Directive . . . 29
3. Security in international law ........................................... 32
   3.1. Theoretical bases from philosophy of law .................. 32
   3.2. International law .................................................... 34
   3.3. Council of Europe .................................................. 36
4. Security in European Union law ...................................... 39
   4.1. EU treaties ............................................................ 39
   4.2. Jurisprudence on security as derogation ................. 41
   4.3. EU Policy ............................................................. 42
   4.4. Security and personal data in secondary EU law ....... 44
   4.5. EU Member States .................................................. 47
5. Competent authorities under the DPLE Directive .................. 48
   5.1. General guidance .................................................. 48
Chapter 4.
Criminal Profiling and Non-Discrimination: On Firm Grounds for the Digital Era?
Laurens Naudts .................................................. 63
1. Introduction .................................................. 63
2. Criminal and algorithmic profiling .......................... 65
3. The Law Enforcement Directive: special categories of data as non-discrimination grounds ...................... 67
   4.1. Discrimination grounds and the European Court of Human Right’s case law ...................................... 75
   4.2. Ground or status: a divergent approach by the ECtHR ........................................................................ 76
   4.3. Recent illustrations: settling on the past? ............................................................... 79
   4.4. Big data profiling: new grounds? ........................................................................ 80
   4.5. Differential treatment: reasonable and objective justification ..................................................... 84
   4.6. Ethnic profiling: an example? ........................................................................ 88
5. Future research .................................................. 90
6. Conclusion ..................................................... 92
Bibliography .......................................................... 94

Chapter 5.
Operationalization of Information Security through Compliance with Directive 2016/680 in Law Enforcement Technology and Practice
Thomas Marquenie and Katherine Quezada .......................... 97
1. Introduction .................................................. 97
2. Principles of information security .............................. 98
   2.1. Confidentiality ............................................. 100
   2.2. Integrity .................................................... 101
   2.3. Availability ................................................ 102
3. Information security in data protection for law enforcement .......................................................... 103
3.1. The EU legal framework on cybersecurity and data protection . . . 104
3.2. Data protection principles ........................................ 108
3.3. Data processing obligations ...................................... 110
3.4. Data protection impact assessment .............................. 112
3.5. Reporting of data breaches and supervisory oversight ........... 113
3.6. Representation of IS requirements in the DPLE ................. 114
3.7. The scope and purpose of information security and data protection .................................................. 115

4. Operationalization of security in law enforcement .................. 119

5. Conclusion .................................................................... 122

Acknowledgement ............................................................ 124

Bibliography ..................................................................... 124

Chapter 6.
Protecting Human Rights through a Global Encryption Provision
Danaja Fabčič Povše .......................................................... 129

1. Introduction ................................................................. 129
2. Encryption, (cyber)security and human rights ....................... 131
3. Fragmented provisions in international human rights law ....... 137
   3.1. General human rights framework .............................. 137
   3.2. Security measures and standards in data protection laws .. 140
      3.2.1. European Union (EU) .................................... 140
      3.2.2. Convention no. 108 of the Council of Europe ........ 143
      3.2.3. Economic Community of West African States (ECOWAS) ................ 144
      3.2.4. Asia-Pacific Economic Cooperation (APEC) ....... 144
   3.3. Recommendations of expert bodies ........................... 145
   3.4. Other upcoming initiatives by regional organisations ...... 148
4. Enabling global encryption obligations in the absence of specific
treaty provisions .......................................................... 149
   4.1. Option 1 – a global treaty with encryption requirements ...... 149
   4.2. Option 2a – globalisation by means of accession ........... 151
   4.3. Option 2b – globalisation by GDPR’s ‘adequate protection’
     standard ................................................................. 151
   4.4. Option 3 – maintain the status quo .......................... 153
5. Conclusion .................................................................... 153

Acknowledgement ............................................................ 154

Bibliography ..................................................................... 154

Chapter 7.
Identity Management and Security
Jessica Schroers ............................................................... 161

1. Introduction ................................................................. 161
2. What is identity management? ....................................... 162

Intersentia vii
6. Implications of the analysis beyond type-approval legislation  ........................................ 207
   6.1. The extension of the role as manufacturer... or an emerging role as fleet operator? ... 208
   6.2. Consequences for liability  ................................................................................. 209
7. Conclusion  ............................................................................................................... 211
Bibliography  ............................................................................................................. 211

Chapter 9.
The Cybersecurity Requirements for Operators of Essential Services under the NIS Directive – An Analysis of Potential Liability Issues from an EU, German and UK Perspective
Daniela Brešić  ............................................................................................................ 215
1. Introduction  ........................................................................................................ 215
2. The scope of CI protection on an EU and national level  ..................................... 217
   2.1. The EU regulatory Framework of CI protection compared to the scope of the NIS Directive .............................................. 217
   2.2. The scope of CI protection from the German perspective .................... 220
   2.3. The scope of CI protection from the UK perspective ......................... 221
3. The security requirements and incident notification for operators of essential services from an EU and national perspective ................................. 223
   3.1. The security requirements and incident notification set out by the NIS Directive, Article 14 and 15 ............................................. 223
   3.2. The security requirements set out by the German BSI Act, section 8, 8a and 8b BSI Act ......................................................... 224
   3.3. The security requirements set out by the UK NIS Regulation, section 10 and 11 ................................................................. 226
4. Deliberations on liability issues from an EU and national perspective . 228
   4.1. The uncertain meaning of the NIS Directive, Article 14 NIS Directive ........................................................................... 228
   4.2. The national implementation of Article 14 NIS Directive from an UK and German perspective ........................................... 230
   4.3. The problem of fault / the burden of proof ........................................... 233
   4.4. State liability in the context of CI ............................................................... 234
5. Conclusion  ............................................................................................................... 235
Bibliography  ............................................................................................................. 237

Chapter 10.
The ‘by Design’ Turn in EU Cybersecurity Law: Emergence, Challenges and Ways Forward
Domenico Orlando and Pierre Dewitte  ................................................................... 239
1. Introduction  ........................................................................................................ 239
2. Decoding ‘security by design’: a tale of ‘security’ and ‘design’ ................. 239

Intersentia ix
### 3. The ‘by design’ turn in the European legislative framework

#### 3.1. Integrating legal requirements in the software development lifecycle

- 241

#### 3.2. Data protection (and security) by design in the GDPR

- 243

#### 3.3. Security by design in Regulation 45/2001

- 245

#### 3.4. Security by design in the new Cybersecurity Act Regulation

- 245

#### 3.5. Security by design in the IoT sector

- 246

### 4. Challenges of the ‘by-design’ approach

#### 4.1. A call for interdisciplinarity

- 247

#### 4.2. Specific challenges of security by design

- 248

#### 4.3. The interaction between SbD and DPbD

- 249

### 5. Conclusions

- 250

### Acknowledgements

- 250

### Bibliography

- 250

#### Chapter 11.
**Promoting Coherence in the EU Cybersecurity Strategy**

Alessandro Bruni

1. Introduction

- 253

2. The concept of coherence

- 254

#### 2.1. Coherence vs consistency

- 255

#### 2.2. Coherence principle in the EU cybersecurity legislative framework

- 256

3. The EU cybersecurity context

- 257

#### 3.1. The EU and cybersecurity

- 257

#### 3.2. The initial EU cybersecurity legislative initiatives

- 258

4. EU cybersecurity Actors

- 261

#### 4.1. ENISA

- 261

#### 4.2. Public-private partnership

- 263

5. The EU Cybersecurity Strategies

- 265

#### 5.1. The European Union Cybersecurity Strategy 2013

- 265

#### 5.2. The European Union 2017 Cybersecurity Strategy

- 271

6. Conclusion

- 275

### Bibliography

- 276

#### Chapter 12.
**Challenges of the Cyber Sanctions Regime under the Common Foreign and Security Policy (CFSP)**

Yuliya Miadzvetskaya

1. Introduction

- 277

2. Current EU sanctions framework

- 280
LIST OF CONTRIBUTORS

All contributors are affiliated to the KU Leuven Centre for IT and IP law (CiTiP) and members of CiTiP’s security research team.

Daniela Brešić completed her legal clerkship in the district of the Higher Regional Court Munich, after graduating from Ludwig-Maximilians-University Munich, Germany. She also obtained an LL.M. degree in Law and Technology from Tilburg University, the Netherlands.

Alessandro Bruni is focusing his research activities primarily on communication law and legal challenges related to new technologies such as Artificial Intelligence and blockchain. He obtained his degrees in Law at the University of Siena and at Tilburg University. He was affiliated to a civil society organisation on specific EU digital dossiers involving fundamental rights, to a consultancy group, dealing with cybersecurity matters, and to a European telecom operator as a Regulatory Officer.

Pierre Dewitte mainly focuses his research on Data Protection by Design, privacy engineering, smart cities and algorithmic transparency issues.

Charlotte Ducuing holds a master’s degree in law with specialisation in European law, a master’s degree in political sciences from the University Lille (Institut d’Etudes Politiques de Lille) and an LL.M. Intellectual Property and ICT Law from KU Leuven. As a PhD fellow, her main research interests extend to the regulation of emerging digital infrastructure in network industries.

Ivo Emanuilov is a PhD fellow in public international law working on the (in) adequacy of the concept of control in risk-based international law. His research is centered around problems of (shared) international responsibility, non-state actors, due diligence, risk analysis and new technologies in international humanitarian law, air and space law and cyber law. Ivo has degrees in international and EU law, English law, ICT law, and software engineering. He is a visiting lecturer on legal and ethical aspects of artificial intelligence at the University of Sofia and biometrics and privacy law at the Swiss Distance Learning University (UniDistance), Switzerland.

Stefano Fantin joined CITIP in 2017 after previous public sector and e-Government experiences. His research now covers various aspects of
cybersecurity and accountability in the counter-terrorism and national security governance domains, as well as critical infrastructures protection and cyber defense policies. He is also an affiliated guest researcher at the Center for EU Policy Studies (CEPS).

**Thomas Marquenie** obtained his master’s degree of Laws from the University of Leuven in 2015 and specialised in Criminal, International and European Law. In 2016, he obtained an Advanced Master’s (LL.M.) in Intellectual Property Rights & ICT Law at the University of Leuven. At CITiP, his research focuses on human rights and data protection as well as the legal aspects of Artificial Intelligence, security and law enforcement. He has contributed to several European Commission projects on the development and implementation of innovative police technologies, such as FP7 VALCRI and the ongoing H2020 MAGNETO, and is currently preparing a PhD project regarding fairness and accountability in law enforcement AI.

**Yuliya Miadzvetskaya** joined CITiP in 2019, after having worked as an academic assistant at the College of Europe in Bruges. She also was trainee in the Legal Service of the European Parliament in Brussels and at the United Nations offices in Minsk.

**Laurens Naudts** is a doctoral researcher. His research focuses on the interrelationship between artificial intelligence, ethics, justice, fairness and the law. Laurens' doctoral research reconsiders the concepts of equality and data protection within the context of machine learning and algorithmically guided decision-making. Laurens has also been involved in several national and EU funded research projects, including amongst others iLINC and Preemptive, and, currently, VICTORIA (Video Analysis for Investigation of Criminal and Terrorist Activities). Laurens was formerly appointed as a researcher at the European University Institute (Centre for Media Pluralism and Media Freedom).

**Domenico Orlando** is currently involved in two projects about smart grids development (ROLECS and SNIPPET). He graduated in Business and Competition law at the Bocconi University and has an LL.M. in ICT law from the University of Oslo. He is interested in themes such as Security and Data Protection by Design and he focuses on data protection, cybersecurity and energy.

**Danaja Fabčič Povše** focuses her research activities on legal and ethical aspects of data security, data protection and privacy within organisations and in design processes.

**Katherine Quezada** is mainly working on the MAGNETO project within CITiP. Her educational background includes an LL.B. from Universidad Autónoma de Santo Domingo (2013, homologated to the Spanish equivalent in 2017), a
master’s degree of Criminology and Criminal Justice from Universidad Camilo José Cela (2015) and an LL.M. in IP and ICT law from KU Leuven (2018–2020).

Jessica Schroers is a doctoral researcher at CiTiP. Her research focuses on data protection law and the legal issues related to identity management. She writes her doctoral thesis on the responsibility for electronic identity. Originally from Germany, she studied in the Netherlands at the University of Tilburg, where she obtained a bachelor's degree in Law and Management and Master's degrees in International Business Law and in Law and Technology. In 2009 she was an Erasmus exchange student at the University of Helsinki. Before joining CiTiP in 2013, Jessica completed an internship at a Dutch law firm where she focused on IT and intellectual property law.

Peggy Valcke is professor of technology and law at KU Leuven, CiTiP, and principal investigator at the Security & Privacy Group at imec (previously iMinds). She is also member of Leuven.AI (the Leuven Centre for Artificial Intelligence) and LICT (Leuven Centre on ICT). In previous years, she has taken up part-time or visiting professorships at Bocconi University in Milan; the European University Institute in Florence; Tilburg University; and Central European University in Budapest. Peggy has been assessor (member of the deciding body) of the Belgian Competition Authority and member of the General Chamber of the Flemish Media Regulator since 2008. She was a member of Google's Advisory Council on the Right to be Forgotten and of Digital Minds for Belgium, and also sits on the Scientific Committee of AI4People, the first global forum in Europe on the Social Impacts of Artificial Intelligence set up by Atomium-European Institute for Science, Media and Democracy.

Anton Vedder is a professor of IT Law at CiTiP. He is especially interested in the interplay of technological developments and the articulation of basic moral and legal concepts. Recent publications include articles and books on trust in e-health, innovative technologies, care, enhancement, and justice, privacy, data protection and profiling, ethics of artificial intelligence in a big data environment, and privacy versus public security. He is the academic director of KU Leuven’s LL.M. program of IP and IT Law and a member of KU Leuven’s Ethics Committee on Dual Use, Military Use and Misuse of Research.

Plixavra Vogiatzoglou is a doctoral researcher at CiTiP and a certified lawyer in Greece. Her main interests revolve around surveillance and criminal analytics, and their effects on fundamental rights, in particular privacy and data protection. Before joining CiTiP in January 2017, Plixavra obtained an LL.M. in Intellectual Property and ICT law from the Faculty of Law of KU Leuven and an LL.M. in International Studies from the Faculty of Law of Aristotle University of Thessaloniki.