

Table of contents

Outline	5
----------------	---

Introduction	9
Jean HERVEG	

CHAPTER 1 ICT GOVERNANCE

The European Data Protection Regulation and Information Governance	13
---------------------------------------------------------------------------	----

Herbert BURKERT

1. – The Broader Context	13
2. – The Regulation in the Context of Information Governance	16
2.1. Information Governance, the Regulation and Law	17
2.2. Information Governance, the Regulation and Information Policy	18
2.3. Information Governance, the Regulation and Comprehensiveness	21
2.4. Summary: The Regulation in the Context of Information Governance	23
3. – The Future of Information Governance	24
Mapping	24
Inventories	25
Technology Awareness	25
Feed-back and Learning	25
Evaluative Framework	26
Global Perspective	26
Concluding Remark	26

The European Group on Ethics in Science and New Technologies and Data Protection in the EU	29
Herman Nys	
Introduction	29
1. – Opinion n° 13 of 30 July 1999 on ethical questions in the information society	29
2. – Opinion n° 20 of 16 March 2005 on the ethical aspects of ICT implants in the human body	31
3. – Opinion n° 26 of 22 February 2012 on ethics of information and communication technologies	33
4. – Opinion n° 28 of 20 May 2014 on ethics of security and surveillance technologies	36
5. – Opinion n° 29 of 13 October 2015 on the ethical implications of new health technologies and citizen participation	37
6. – Opinion n° 30 of 19 December 2018 on Future of Work, Future of Society	40
Conclusion	41

CHAPTER 2

COMMODIFICATION AND COMPETITION

Paying with Personal Data: Between Consumer and Data Protection Law	45
Antoine DELFORGE	
Introduction	45
1. – Applicability of EU Consumer Law	47
2. – Transparency Obligation About the Commercial Reuse of Personal Data	50
3. – Analysis of the GDPR Legal Bases	54
a. Necessity for the performance of the contract to which the data subject is party	55
b. Legitimate Interests of the Data Controller	56
c. Data Subject's Consent	57
4. – Termination of the Contract and Withdrawal of the Consent	60

5. – Assessing the Fairness of the Contractual Relationships	62
Conclusion	64
The GDPR: A Shield to a Competition Authority's Data Sharing Remedy?	67
Thomas TOMBAL	
Abstract	67
Introduction	68
I. – Lawful basis for the data sharing	72
A. Lawful basis for the data holder	73
1. Consent	75
2. Necessary for the compliance with a legal obligation to which the data holder is subject	77
B. Lawful basis for the data recipient	79
1. Consent	80
2. Necessary for the purposes of the legitimate interests pursued by the data recipient	81
C. Findings	83
II. – Compliance with the general principles of personal data protection	85
III. – Need for competition and data protection authorities to collaborate	87
Conclusion	88
References	90

CHAPTER 3

SECRET SURVEILLANCE

The Half-Way Revolution of the European Court of Human Rights or the 'Minimum' Requirements of 'Law'	97
Bart VAN DER SLOOT	
Introduction	97
1. – Accessibility of the domestic law	101
2. – Scope of application of secret surveillance measures	102

3. – The duration of secret surveillance measures	104
4. – Procedures for processing the data	106
5. – Authorisation procedures	107
6. – Ex post supervision of the implementation of secret surveillance measures	111
7. – Conditions for communicating data to and receiving data from other parties	113
8. – Notification of interception of communications	114
9. – Available remedies	116
Conclusion	117

CHAPTER 4
WHISTLEBLOWING

Whistleblowing: Threat or Safeguard for Data Protection in the Digital Era?	129
Amélie LACHAPELLE	
Introduction	129
I. – Whistleblowing in the Digital Era	130
A. A New Way of Blowing the Whistle	131
B. A New Way of Thinking about Whistleblowing	132
II. – GDPR, a Limit to Whistleblowing	133
A. A Key Component of European Whistleblower Protection	134
B. Whistleblowing Compliance with Data Protection	135
1. The Lawfulness of Processing of Personal Data	136
2. The Principles relating to Processing of Personal Data	139
3. The Data Subject's Rights	142
III. – GDPR, an Incentive to Blowing Whistle	143
A. The New Faces of Compliance	144
B. The Open Door to Whistleblowing	146
Conclusion	148

CHAPTER 5**SOCIAL MEDIAS, WEB ARCHIVING & JOURNALISM**

To Scrape or Not to Scrape? The Lawfulness of Social Media Crawling under the GDPR	151
Catherine ALTOBELLI, Nikolaus FORGÓ, Emily JOHNSON & Antoni NAPIERALSKI	
Introduction	151
1. – Type and Formats of Personal Data on Social Media	152
2. – Personal Data Collection Techniques on Social Media Platforms	156
3. – Different legislative approaches for processing for research purposes	157
4. – Lawfulness of Social Media Crawling	159
4.1. Lawfulness of Primary Processing by Social Media Platform	160
4.1.1. Consent	161
4.1.2. Performance of a contract	161
4.1.3. Legitimate interests	162
4.1.4. Special Categories of Personal Data	164
4.1.5. Outcome of Lawfulness Analysis	166
4.2. Lawfulness of Social Media Crawling as Further Processing	166
4.2.1. Compatibility of Crawling Purposes	168
4.2.2. Crawling for Research (Purposes)	170
4.2.3. Incompatibility of Crawling Purposes	173
Conclusion	174
Bibliography	175
Web Archiving in the Public Interest from a Data Protection Perspective	181
Alejandra MICHEL	
Introduction	181
I. – Web archiving in the public interest: a major societal challenge	182
II. – Application of GDPR provisions to web archiving activities	184
III. – Scope and meaning of the derogatory regime for personal data processing for archiving purposes in the public interest	186

IV. – Exemptions for archiving purposes in the public interest	189
A. A necessary pre-condition: the establishment of appropriate safeguards	189
B. Exemptions directly provided by the GDPR	191
C. Exemptions provided by Union or national law	194
V. – Appropriate safeguards and specificities of the Belgian law	195
A. Appropriate safeguards for data subjects' rights and freedoms	196
B. Specificities for the dissemination and the communication of personal data processed for archiving purposes in the public interest	198
Conclusion	199
Processing of personal data for “journalistic purposes”	201
Cécile DE TERWANGNE & Alejandra MICHEL	
Introduction	201
I. – The interconnected society and the advent of neo-journalism	202
II. – The notion of “journalistic purposes”	204
A. The functional approach of the journalistic activity	205
B. Assimilation of journalistic purposes to the freedom of expression	208
C. The requirement of a public debate/general interest condition	210
III. – Exemptions for personal data processing for journalistic purposes	212
IV. – Belgian Data Protection Act	216
A. Definition of processing for journalistic purposes	216
B. Exemptions and Derogatory Regime	221
1. Consent	221
2. Special categories of personal data	222
3. Data subject's rights	223
4. Obligations of the controller or processor	226
5. Transborder data flows	227
6. Powers of the supervisory authority	227
Conclusion	227

CHAPTER 6

AUTOMATED INDIVIDUAL DECISION-MAKING

The GDPR and Automated Individual Decision-Making: Fair Processing v. Fair Result	233
Manon KNOCKAERT	
Introduction	233
I. – Preliminary remark on Article 22	234
II. – The General Data Protection Regulation and the fair processing	236
1. Privacy by design as a way to ensure an effective fair processing in automated decision-making	237
2. Security as an integral component of a fair processing	238
III. – The General Data Protection Regulation and the fair results	242
IV. – Indirect remedies: the right to object and the concept of fairness	246
1. Convention 108+ and Article 29 Working Party: the right to explanation as a part of the right to object	246
2. The concept of Fairness in the results obtained by automated decision-making systems	248
Conclusion	250

CHAPTER 7

DATA SECURITY

Risk as the Cornerstone of Information Security and Data Protection	255
Jean-Noël COLIN	
Introduction	255
1. – Information System Security	257
1.1. Defining the Information System	257
1.2. Defining security	258
1.3. Threats and attack vectors	260
2. – A risk-based approach for managing security	262

3. – Protecting the IS	266
3.1. Principles	266
3.2. A layered approach	267
Conclusion	269
How to Deal with the Human Factor in Information Security?	271
Charlotte DURIEUX, Alain EJZYN & Anne ROUSSEAU	
Introduction	271
I. – The problematic of information security	272
1. Organizational culture	273
1.1. Link between organizational culture and information security culture	273
1.2. An information security culture	275
1.3. Information security policies	276
2. Management	277
3. Individual behaviours	278
3.1. Information psychology and beliefs	279
3.2. Usability & design of mechanisms	280
3.3. Raising awareness	281
II. – Discussion and proposed research framework	282
III. – Limits	283
Bibliography	284
“Technical and Organisational Measures” – A Systematic Analysis of Required Data Protection Measures in the GDPR	289
Dag Wiese SCHARTUM	
Introduction	289
1. – Overview of articles of the GDPR imposing measures	291
2. – Which types of measures could be comprised?	294
3. – Interaction and dependencies	299
4. – A more complete approach	302
Conclusion	305

CHAPTER 8

PRIVACY BY DESIGN

Privacy-by-Design in Intelligent Infrastructures	309
Manon KNOCKAERT, Maryline LAURENT, Lukas MALINA, Raimundas MATULEVIČIUS, Marinella PETROCCHI, Mari SEEBA, Qiang TANG, Aimilia TASIDOU, Jake TOM	
Introduction	309
1. – Key Data Protection elements in Intelligent Infrastructures	312
2. – Intelligent Infrastructures Environment	323
2.1. Key components	323
2.2. Parking Reservation Generation Scenario	326
3. – Personal Data Protection and Intelligent Infrastructures: the added-value of Privacy Enhancing Technologies	328
3.1. Overview of current Privacy Enhancing Technologies to support GDPR principles	328
3.2. Summary	333
3.3. Illustration of Personal Data Managing in Parking Reservation Generation Scenario	334
3.4. Illustration for privacy policies: a language-based approach for Editing, Analysis, and Enforcement of privacy requirements	339
Conclusion	343

CHAPTER 9

HEALTH, AI, SCIENTIFIC RESEARCH & POST-MORTEM PRIVACY

Health Care Data in the U.S., the GDPR Exemplar and the Challenge of AI	347
Nicolas TERRY	
Introduction	347
I. – U.S. Data Protection's Failure to Adjust for Emerging Technologies	348
II. – The Challenge of Health Data Protection	349
III. – The Regulatory Challenges of AI	353

IV. – What is the Salient Question, Data Protection or Social Goods?	358
V. – Are New or Proposed U.S. Laws the Answer?	361
Conclusion	363
Artificial Intelligence and Discrimination Based on Prediction of Future Illness	365
Sharona HOFFMAN and Mariah DICK	
Introduction	365
I. – What Is Artificial Intelligence?	366
A. Definitions	366
B. Practical Applications	367
II. – Employers and AI	370
III. – Current Data Protection and Anti-Discrimination Laws	372
A. United States Law	372
1. The HIPAA Privacy Rule	372
2. The Americans with Disabilities Act	373
3. Other Relevant Laws: The Genetic Information Nondiscrimination Act and State Laws	374
B. European Law	375
1. The General Data Protection Regulation	375
2. Anti-Discrimination Laws	376
3. Genetic Discrimination Laws	377
IV. – Recommendations	377
A. Expanding Disability Discrimination Protections	378
B. Requiring Disclosure of AI Use	378
Conclusion	379
Artificial Intelligence in Healthcare and the Impact of COVID-19	381
Stefaan CALLENS & Guillaume POMES	
Introduction	381
1. – Some concepts	382
2. – AI in healthcare and the combat of COVID-19	383
3. – Opportunities and concerns of AI	385

4. – The impact of COVID-19 on healthcare and on AI	388
A. Impact of COVID-19 on healthcare	388
B. Impact of COVID-19 on AI	390
Conclusion	394
The Processing of Personal Data for Scientific Research Purposes in Medicine. Some Aspects of the General Data Protection Regulation: Between Law and Ethics	395
Carla BARBOSA	
1. – General Data Protection Regulation (GDPR) and scientific research	395
2. – Health scientific research	397
3. – Consent, secondary use, and biobanks – GDPR solutions	398
4. – The future	401
Conclusion	404
References	406
Invigorating the Principles of Consent and Data Privacy in the Medical Field through Gamification and Genome Donation	409
Hortense GALLOIS, Yann JOLY, Vincent GAUTRAIS	
Introduction	409
1. – Informed consent and health data sharing under Quebec law	412
1A. Consent and patient protection	412
1B. Consent and privacy protection	416
2. – Moving away from informed consent	418
2A. Building the right safeguards around data sharing: protecting privacy by going beyond autonomy	418
2A1. Documentation	419
2A2. Third party control	422
2B. Developing new consent models built on shared decision-making, dynamic and broad consents	424
3. – Fostering data sharing through innovative frameworks	427
3A. Gamification	427
3B. Genome donation	429
Conclusion	432

What About Post-Mortem Digital Privacy and Personal Health Data Protection?	433
Gauthier CHASSANG	
Abstract	433
Introduction	434
I. – Post-mortem digital privacy and personal health-related data in International and EU Law	436
A. No explicit recognition of an individual right to post-mortem digital privacy	436
B. Clues in favour of a limited and implicit post-mortem digital privacy protection through interpretation of current provisions applying to personal health data uses	442
II. – Examples of post-mortem digital privacy regulatory approaches covering personal health-related data	452
A. Example of self-regulations based on the autonomous choices of living data subjects	452
B. The French example of a national legislation merging autonomous and delegated post-mortem privacy management	456
Conclusion	459

PROSPECTIVE VIEW

Data protection or privacy?	463
Yves POULLET	