Universiteit
Leiden
The Netherlands

EU privacy and data protection law applied to AI: unveiling the legal problems for individuals

Häuselmann, A.N.

Citation
Häuselmann, A. N. (2024, April 23). *EU privacy and data protection law applied to AI: unveiling the legal problems for individuals*. Retrieved from https://hdl.handle.net/1887/3747996

Version:	Publisher's Version
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/3747996

Note: To cite this publication please use the final published version (if applicable).

Universiteit Leiden

EU Privacy and Data Protection Law Applied to AI: Unveiling the Legal Problems for Individuals

Andreas Nicolas Häuselmann

EU Privacy and Data Protection Law Applied to AI: Unveiling the Legal Problems for Individuals

Proefschrift

ter verkrijging van

de graad van doctor aan de Universiteit Leiden, op gezag van rector magnificus prof.dr.ir. H. Bijl, volgens besluit van het college voor promoties

te verdedigen op dinsdag 23 April 2024

klokke 15.00 uur

door

Andreas Nicolas Häuselmann

geboren te Schlieren, Zwitserland

Promotoren:	prof. dr. ir. B.H.M. Custers
	prof. dr. G.J. Zwenne
Promotiecommissie:	prof. dr. B.W. Schermer
	dr. G. Malgieri
	prof. dr. N.N. Purtova Msc LL.M. (Universiteit Utrecht)
	prof. dr. A.M. Klingenberg (Rijksuniversiteit Groningen)
	prof. dr. M. Finck LL.M. (Universität Tübingen, Duitsland)

Table of contents

1 Introduction 1

1.1 Context and social relevance 1

1.2 Research question 4

1.3 Methodology 6

1.4 Limitations 8

1.5 Structure 10

2 Artificial Intelligence (AI) 13

2.1 Definitions of AI 13

2.2 AI disciplines 15

2.2.1 Machine learning (ML) 16

2.2.1.1 Supervised machine learning 17

2.2.1.2 Unsupervised machine learning 19

2.2.1.3 Reinforcement learning (RL) 20

2.2.1.4 Artificial Neural Networks and deep learning 21

2.2.2 Natural language processing (NLP) 25

2.2.3 Computer vision (CV) 28

2.2.3.1 Face recognition 29

2.2.3.2 DL and face recognition 31

2.2.4 Affective computing (AC) 32

2.2.4.1 Facial expressions 32

2.2.4.2 Speech in affective computing 35

2.2.4.3 Multimodal approaches 36

2.2.5 Automated reasoning (AR) 37

2.3 Conclusions 39

3 The current legal framework 40

3.1 The fundamental right to privacy 41

3.1.1 Scope 41

3.1.1.1 Private life 42

3.1.1.2 Communications 43

3.1.2 Living instrument doctrine 43

3.2 The fundamental right to data protection 44

3.2.1 Scope 45

3.2.2 Principle of proportionality 45

3.3 General data protection regulation 46

3.3.1 Material scope 47

3.3.1.1 Personal data 47

3.3.1.2 Special categories of personal data 48

3.3.1.3 Processing....50
3.3.2 Personal scope....50
3.3.2.1 Controller....51
3.3.2.2 Processor....51
3.3.3 Principles....52
3.3.3.1 Lawfulness....52
3.3.3.2 Fairness....53
3.3.3.3 Transparency....54
3.3.3.4 Purpose limitation....54
3.3.3.5 Data minimisation....55
3.3.3.6 Accuracy....56
3.3.3.7 Storage limitation....57
3.3.3.8 Integrity and confidentiality....57
3.3.3.9 Data protection by design and default....57
3.3.3.10 Accountability....58
3.3.4 Rights....58
3.3.4.1 Right of access....59
3.3.4.2 Right to rectification....61
3.3.4.3 Right to erasure....62
3.3.4.4 Right to data portability....63
3.3.4.5 Right to object....64
3.3.4.6 Right not to be subject to automated decision making....65
3.4 ePrivacy Directive....68
3.4.1 Material scope....69
3.4.2 Personal scope....70
3.4.3 Specific requirements....71
3.4.3.1 Confidentiality of communications....71
3.4.3.2 Information stored in terminal equipment....71
3.4.3.3 Location data....72
3.5 Conclusions....73
4 Legal problems: principles....75
4.1 Approach....75
4.2 Lawfulness....80
4.2.1 Legal problems: Type 1....80
4.2.2 Legal problems: Type 2....83
4.2.3 Legal problems: Type 3....83
4.3 Fairness....83
4.3.1 Legal problems: Type 1....86

4.3.2 Legal problems: Type 2 91
4.3.3 Legal problems: Type 3 94
4.4 Transparency 100
4.4.1 Legal problems: Type 1 101
4.4.2 Legal problems: Type 2 106
4.4.3 Legal problems: Type 3 107
4.5 Purpose limitation 120
4.5.1 Legal problems: Type 1 120
4.5.2 Legal problems: Type 2 124
4.5.3 Legal problems: Type 3 125
4.6 Data minimisation 129
4.6.1 Legal problems: Type 1 129
4.6.2 Legal problems: Type 2 131
4.6.3 Legal problems: Type 3 132
4.7 Accuracy 134
4.7.1 Legal problems: Type 1 135
4.7.2 Legal problems: Type 2 142
4.7.3 Legal problems: Type 3 146
4.8 Enhanced protection for ‘special data’ 148
4.8.1 Legal problems: Type 1 150
4.8.2 Legal problems: Type 2 150
4.8.3 Legal problems: Type 3 150
4.9 Confidentiality of communication 168
4.9.1 Legal problems: Type 1 170
4.9.2 Legal problems: Type 2 170
4.9.3 Legal problems: Type 3 170
4.10 Conclusions 177
5 Legal problems: Rights 182
5.1 Approach 182
5.2 Informational privacy 184
5.2.1 Legal problems: Type 1 184
5.2.2 Legal problems: Type 2 187
5.2.3 Legal problems: Type 3 187
5.3 Bodily privacy 188
5.3.1 Legal problems: Type 1 189
5.3.2 Legal problems: Type 2 191
5.3.3 Legal problems: Type 3 191
5.4 Mental privacy 191

5.4.1 Legal problems: Type 1 194
5.4.2 Legal problems: Type 2 198
5.4.3 Legal problems: Type 3 199
5.5 Communicational privacy 199
5.5.1 Legal problems: Type 1 200
5.5.2 Legal problems: Type 2 206
5.5.3 Legal problems: Type 3 206
5.6 Access 207
5.6.1 Legal problems: Type 1 211
5.6.2 Legal problems: Type 2 213
5.6.3 Legal problems: Type 3 224
5.7 Rectification 230
5.7.1 Legal problems: Type 1 232
5.7.2 Legal problems: Type 2 234
5.7.3 Legal problems: Type 3 239
5.8 Erasure 242
5.8.1 Legal problems: Type 1 242
5.8.2 Legal problems: Type 2 246
5.8.3 Legal problems: Type 3 247
5.9 Portability 247
5.9.1 Legal problems: Type 1 248
5.9.2 Legal problems: Type 2 248
5.9.3 Legal problems: Type 3 249
5.10 Objection 252
5.10.1 Legal problems: Type 1 252
5.10.2 Legal problems: Type 2 255
5.10.3 Legal problems: Type 3 255
5.11 Automated decision-making 259
5.11.1 Legal problems: Type 1 260
5.11.2 Legal problems: Type 2 261
5.11.3 Legal problems: Type 3 262
5.12 Conclusions 275
6 Addressing the legal problems 280
6.1 Approach 280
6.2 Fairness principle – the elusiveness problem 284
6.2.1 Setting the scene 284
6.2.2 Solution: interpretation including substantive fairness 289
6.2.3 Conclusion 297

6.3 Enhanced protection for 'special data' – the mental data problem 298
6.3.1 Setting the scene 298
6.3.2 Solution: Introducing a dynamic list for special data 306
6.3.3 Conclusion 308
6.4 Confidentiality – the communication surveillance problem 308
6.4.1 Setting the scene 308
6.4.2 Solution: Regulating human-machine communication 311
6.4.3 Conclusion 316
6.5 Right of access – the trade secrets problem 316
6.5.1 Setting the scene 316
6.5.2 Solution: Introducing a new exception in the TSD 319
6.5.3 Conclusion 324
6.6 Right to rectification – the verifiability standard problem 324
6.6.1 Setting the scene 324
6.6.2 Solution: Amending the right to rectification 330
6.6.3 Conclusion 335
6.7 Automated decision-making – cumulativeness problem 336
6.7.1 Setting the scene 336
6.7.2 Solution: Redrafting the right not to be subject to ADM 337
6.7.3 Conclusion 346
6.8 Conclusions 346
7 Conclusion 349
7.1 Answer to the research question 349
7.2 Recommendations for future legislation 353
7.3 Future research 355

Samenvatting (Dutch summary)… 358
Bibliography 362
Acknowledgments 382
Curriculum Vitae 383

Abbreviations

AC	Affective computing
AI	Artificial Intelligence
ANN	Artificial neural networks
BCI	Brain-computer interfaces
AR	Automated reasoning
DL	Deep learning
CJEU	Court of Justice of the European Union
CNN	Convolutional neural networks
CV	Computer vision
FACS	Facial Action Coding System
GDPR	General Data Protection Regulation
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EUCFR	European Union Charter of Fundamental Rights
ePD	ePrivacy Directive
ML	Machine learning
NLP	Natural language processing
RL	Reinforcement learning
SA	Supervisory authority
TSD	Trade secrets directive