4

Constitutional Challenges in the Emotional AI Era

Peggy Valcke, Damian Clifford, and Viltė Kristina Dessers[*]

4.1 INTRODUCTION

Is a future in which our emotions are being detected in real time and tracked, both in private and public spaces, dawning? Looking at recent technological developments, studies, patents, and ongoing experimentations, this may well be the case.[1] In its Declaration on the manipulative capabilities of algorithmic processes of February 2019, the Council of Europe's Committee of Ministers alerts us for the growing capacity of contemporary machine learning tools not only to predict choices but also to influence emotions, thoughts, and even actions, sometimes subliminally.[2] This certainly adds a new dimension to existing computational means, which increasingly make it possible to infer intimate and detailed information about individuals from readily available data, facilitating the micro-targeting of individuals based on profiles in a way that may profoundly affect

[*] The chapter is based on the keynote delivered by P. Valcke at the inaugural conference 'Constitutional Challenges in the Algorithmic Society' of the IACL Research Group on Algorithmic State Market & Society – Constitutional Dimensions', which was held from 9 to 11 May 2019 in Florence (Italy). It draws heavily from the PhD thesis of D. Clifford, entitled 'The Legal Limits to the Monetisation of Online Emotions' and defended at KU Leuven – Faculty of Law on July 3, 2019, to which the reader is referred for a more in-depth discussion.

[1] For some illustrations, see B. Doerrfeld, '20+ Emotion Recognition APIs That Will Leave You Impressed, and Concerned' (Article 2015) https://nordicapis.com/20-emotion-recognition-apis-that-will-leave-you-impressed-and-concerned/ accessed 11 June 2020; M. Zhao, F. Adib and D. Katabi, 'EQ-Radio: Emotion Recognition using Wireless Signals' (Paper 2016) http://eqradio.csail.mit.edu/ accessed 11 June 2020; CB Insights, 'Facebook's Emotion Tech: Patents Show New Ways for Detecting and Responding to Users' Feelings' (Article 2017) www.cbinsights.com/research/facebook-emotion-patents-analysis/ accessed 11 June 2020; R. Murdoch et al., 'How to Build a Responsible Future for Emotional AI' (Research Report 2020) www.accenture.com/fi-en/insights/software-platforms/emotional-ai accessed 11 June 2020. Gartner predicts that by 2022, 10 per cent of personal devices will have emotion AI capabilities, either on-device or via cloud services, up from less than 1% in 2018: Gartner, 'Gartner Highlights 10 Uses for AI-Powered Smartphones' (Press Release 2018) www.gartner.com/en/newsroom/press-releases/2018-03-20-gartner-highlights-10-uses-for-ai-powered-smartphones accessed 11 June 2020.

[2] Committee of Ministers, 'Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes' (Declaration 2019) https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680092dd4b accessed 11 June 2020, para. 8.

https://doi.org/10.1017/9781108914857.005 Published online by Cambridge University Press

their lives.[3] *Emotional artificial intelligence* (further 'emotional AI') and *empathic media* are new buzzwords used to refer to the affective computing sub-discipline and, specifically, to the technologies that are claimed to be capable of detecting, classifying, and responding appropriately to users' emotional lives, thereby appearing to understand their audience.[4] These technologies rely on a variety of methods, including the analysis of facial expressions, physiological measuring, analyzing voice, monitoring body movements, and eye tracking.[5]

Although there have been important debates as to their accuracy, the adoption of emotional AI technologies is increasingly widespread, in many areas and for various purposes, both in the public and private sectors.[6] It is well-known that advertising and marketing go hand in hand with an attempt to exploit emotions for commercial gain.[7] Emotional AI facilitates the systematic gathering of insights[8] and allows for the further personalization of commercial communications and the optimization of marketing campaigns in real time.[9] Quantifying, tracking, and manipulating emotions is a growing part of the social media business model.[10] For example, Facebook is now infamous in this regard due to its emotional contagion[11] experiment where users' newsfeeds were manipulated to assess changes in emotion (to assess whether Facebook posts with emotional content were more engaging).[12] A similar trend has been witnessed in the political sphere – think of the Cambridge

[3] Ibid, para, 6.

[4] A. McStay, *Emotional AI: The Rise of Empathic Media* (SAGE 2018) 3.

[5] For more details, see, e.g., J. Stanley, 'The Dawn of Robot Surveillance' (Report 2019) www.aclu.org/sites/default/files/field_document/061119-robot_surveillance.pdf accessed 11 June 2020 21–25.

[6] Particular employment examples include uses for health care or pseudo-health care (e.g., to detect mood for the purposes of improving mental well-being), road safety (e.g., to detect drowsiness and inattentiveness), employee safety, uses to assess job applicants and people suspected of crimes. See more e.g., A. Fernández-Caballero et al., 'Smart Environment Architecture for Emotion Detection and Regulation' [2016] 64 J Biomed Inform 55; Gartner, '13 Surprising Uses For Emotion AI Technology' (Article 2018) www.gartner.com/smarterwithgartner/13-surprising-uses-for-emotion-ai-technology accessed 11 June 2020; C. Jee, 'Emotion Recognition Technology Should Be Banned, Says an AI Research Institute' (Article 2019) www.technologyreview.com/2019/12/13/131585/emotion-recognition-technology-should-be-banned-says-ai-research-institute/ accessed 11 June 2020; J. Jolly, 'Volvo to Install Cameras in New Cars to Reduce Road Deaths' (Article 2019) www.theguardian.com/business/2019/mar/20/volvo-to-install-cameras-in-new-cars-to-reduce-road-deaths accessed 11 June 2020; Stanley (n 6) 21–24; D. Clifford, 'The Legal Limits to the Monetisation of Online Emotions' (PhD thesis, KU Leuven, Faculty of Law 2019) 12.

[7] Clifford (n 7) 10.

[8] Clifford (n 7) 103.

[9] See, e.g., C. Burr, N. Cristianini, and J. Ladyman, 'An Analysis of the Interaction between Intelligent Software Agents and Human Users' [2018] MIND MACH 735; C. Burr and N. Cristianini, 'Can Machines Read Our Minds?' [2019] 29 MIND MACH 461.

[10] L. Stark and K. Crawford, 'The Conservatism of Emoji: Work, Affect, and Communication' [2015] 1 SM+S, 1, 8.

[11] E. Hatfield, J. Cacioppo, and R. Rapson, 'Emotional Contagion' [1993] Curr Dir Psychol Sci 96.

[12] See, e.g., A. Kramer, J. Guillory, and J. Hancock, 'Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks' (Research Article 2014) https://doi.org/10.1073/pnas.1320040111 accessed 11 June 2020. There are also data to suggest that Facebook had offered advertisers the ability to target advertisements to teenagers based on real-time extrapolation of their mood:

Analytica scandal[13] (where data analytics was used to gauge the personalities of potential Trump voters).[14] The aforementioned Declaration of the Council of Europe, among others, points to the dangers for democratic societies that emanate from the possibility to employ algorithmic tools capable of manipulating and controlling not only economic choices but also social and political behaviours.[15]

Do we need new (constitutional) rights, as suggested by some, in light of growing practices of manipulation by algorithms, in general, and the emergence of emotional AI, in particular? Or, is the current law capable of accommodating such developments adequately? This is undoubtedly one of the most fascinating debates for legal scholars in the coming years. It is also on the radar of CAHAI, the Council of Europe's Ad Hoc Committee on Artificial Intelligence, set up on 11 September 2019, with the mission to examine the feasibility and potential elements of a legal framework for the development, design, and application of AI, based on the Council of Europe's standards on human rights, democracy, and the rule of law.[16]

In the light of these ongoing policy discussions, the ambition of this chapter is twofold. First, it will discuss certain legal-ethical challenges posed by the emergence of emotional AI and its manipulative capabilities. Second, it will present a number of responses, specifically those suggesting the introduction of new (constitutional) rights to mitigate the potential negative effects of such developments. Given the limited scope of the chapter, it does not seek to evaluate the appropriateness of the identified suggestions, but rather to provide the foundation for a future research agenda in that direction. The focus of the chapter lies on the *European* legal framework and on the use of emotions for *commercial business-to-consumer purposes*, although some observations are also valid in the context of other highly relevant uses of emotional AI,[17] such as implementations by the public sector, or for the purpose of political micro-targeting, or fake news. The chapter is based on a literature review, including recent academic scholarship and grey literature. Its methodology relies on a legal analysis of how the emergence of emotional AI raises concerns and challenges for 'constitutional' rights and values through the lens of its use in the business to consumer context. With constitutional rights, we do not refer to national

N. Tiku, 'Facebook's Ability to Target Insecure Teens Could Prompt Backlash' (Article 2017) www.wired.com/2017/05/welcome-next-phase-facebook-backlash/ accessed 11 June 2020.

13 See, e.g., L. Stark, 'Algorithmic Psychometrics and the Scalable Subject' (2018) https://static1.squarespace.com/static/59a34512c534a5fe6721d2b1/t/5cb0bdbc4192024cf8e7e587/1555086781059/Stark+-+Algorithmic+Psychometrics+%28pre-print%29.pdf accessed 11 June 2020; Guardian, 'Cambridge Analytica Files' www.theguardian.com/news/series/cambridge-analytica-files accessed 11 June 2020.

14 Stark (n 14).

15 Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes (n 3), para. 8.

16 For more information, see www.coe.int/en/web/artificial-intelligence/cahai. Transparency declaration: one of the co-authors serves as CAHAI's vice-chair.

17 For example, political micro-targeting, fake news. See more Clifford (n 7) 13.

https://doi.org/10.1017/9781108914857.005 Published online by Cambridge University Press

constitutions, but given the chapter's focus on the European level, to the fundamental rights and values as enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms ('ECHR'), on the one hand, and the EU Charter of Fundamental Rights ('CFREU') and Article 2 of the Treaty on European Union ('TEU'), on the other.

4.2 CHALLENGES TO CONSTITUTIONAL RIGHTS AND UNDERLYING VALUES

Protecting the Citizen-Consumer

Emotion has always been at the core of advertising and marketing, and emotion detection has been used in market research for several decades.[18] Consequently, in various areas of EU and national law, rules have been adopted to protect consumers and constrain forms of manipulative practices in business-to-consumer relations. Media and advertising laws have introduced prohibitions on false, misleading, deceptive, and surreptitious advertising, including an explicit ban on subliminal advertising.[19] Consumer protection law instruments shield consumers from aggressive, unfair, and deceptive trade practices.[20] Competition law prohibits exploitative abuses of market power.[21] Data protection law has set strict conditions under which consumers' personal data can be collected and processed.[22] Under contract law, typical grounds for a contract being voidable include coercion, undue influence, misrepresentation, or fraud. The latter, fraud (i.e., the intentional deception to secure an unfair or unlawful gain, or deprive a victim of her legal right) is considered a criminal offence. In the remainder of the text, these rules are referred to as

[18] A well-known video fragment illustrating this (and described by Sunstein in his article , C. Sunstein, 'Fifty Shades of Manipulation' [2016] 1 J. Behavioral Marketing 213) is Mad Men's Don Draper delivering his Kodak Pitch (see at www.youtube.com/watch?v=UrkGsur75Uc). See, e.g., T. Brader, *Campaigning for Hearts and Minds: How Emotional Appeals in Political Ads Work* (University of Chicago Press 2006); E. Mogaji, *Emotional Appeals in Advertising Banking Services* (Emerald Publishing Ltd 2018).

[19] See, e.g., Article 9 of the Parliament and Council Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation, or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) [2010] OJ L 95.

[20] See, e.g., Parliament and Council Directive 2019/2161 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L 328.

[21] Article 102 of the Treaty on the Functioning of the European Union. See Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C 326.

[22] In particular, Parliament and Council Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119. Also see Parliament and Council Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications) [2002] OJ L 201.

'consumer protection law in the broad sense', as they protect citizens as economic actors.

Nevertheless, the employment of emotional AI may justify additional layers of protection. The growing effectiveness of the technology drew public attention following Facebook's aforementioned emotional contagion[23] experiment, where users' newsfeeds were manipulated to assess changes in emotion (to assess whether Facebook posts with emotional content were more engaging),[24] as well as the Cambridge Analytica scandal[25] (where it was used to gauge the personalities of potential Trump voters).[26] There are also data to suggest that Facebook had offered advertisers the ability to target advertisements to teenagers based on real-time extrapolation of their mood.[27] Yet Facebook is obviously not alone in exploiting emotional AI (and emotions) in similar ways.[28] As noted by Stark and Crawford, commenting on the fallout from the emotional contagion experiment, it is clear that quantifying, tracking, and 'manipulating emotions' is a growing part of the social media business model.[29] Researchers are documenting the emergence of what Zuboff calls 'surveillance capitalism'[30] and, in particular, its reliance on behavioural tracking and manipulation.[31] Forms of 'dark patterns' are increasingly detected, exposed, and – to some extent – legally constrained. Dark patterns can be described as exploitative design choices, 'features of interface design crafted to trick users into doing things that they might not want to do, but which benefit the business in question'.[32] In its report from 2018, the Norwegian Consumer Authority called the use by large digital service providers (in particular Facebook, Google, and Microsoft) of such dark patterns an 'unethical' attempt to push consumers towards the least privacy friendly options of their services.[33] Moreover, it questioned whether such practices are in accordance with the principles of data protection by default and data protection by design, and whether consent given under these circumstances can be said to be explicit, informed, and freely given. It stated that '[w]hen digital services employ dark patterns to nudge users towards sharing more personal data, the financial incentive has taken precedence over respecting users' right to choose. The practice of misleading consumers into making certain choices, which may put their privacy at risk, is unethical and exploitative.' In 2019, the French data

[23] Hatfield (n 12).
[24] See, e.g., Kramer (n 13).
[25] Guardian, 'Cambridge Analytica Files' (n 14); Stark (n 14).
[26] Stark (n 14).
[27] Tiku (n 13).
[28] Clifford (n 7) 112.
[29] Stark and Crawford (n 11) 1, 8.
[30] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).
[31] Stark (n 14).
[32] The Norwegian Consumer Council, 'Deceived by Design' (Report 2018) www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/ accessed 11 June 2020 7.
[33] Ibid.

protection authority, CNIL, effectively fined Google for the violation of transparency and information obligations and lack of (valid) consent for advertisements personalization. In essence, the users were not aware of the extent of personalization.[34] Notably, the Deceptive Experiences to Online Users Reduction Act, as introduced by senators Deb Fischer and Mark Warner in the United States (the so-called DETOUR Act), explicitly provided protection against 'manipulation of user interfaces' and offered prohibiting dark patterns when seeking consent to use personal information.[35]

It is unlikely, though, that existing consumer protection law (in the broad sense) will be capable of providing a conclusive and exhaustive answer to the question of where to draw the line between forms of permissible persuasion and unacceptable manipulation in the case of emotional AI. On the one hand, there may be situations in which dubious practices escape the scope of application of existing laws. Think of the cameras installed at Piccadilly Lights in London which are able to detect faces in the crowd around the Eros statue in Piccadilly Circus, and 'when they identify a face the technology works out an approximate age, sex, mood (based on whether think you are frowning or laughing) and notes some characteristics such as whether you wear glasses or whether you have a beard'.[36] The cameras have been used during a certain period with the purpose of optimizing the advertising displayed on Piccadilly Lights.[37] Even if such practices of emotional AI in public spaces are not considered in violation of the EU General Data Protection Regulation (given the claimed immediate anonymization of the faces detected), they raise serious question marks from an ethical perspective.[38] On the other hand, the massive scale with which certain practices are deployed may surpass the enforcement of individual rights. The Council of Europe's Parliamentary Assembly expressed concerns that persuasive technologies enable 'massive psychological experimentation and persuasion on the internet'.[39] Such practices seem to

[34] In accordance with the General Data Protection Regulation (n 23): CNIL, 'Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 Pronouncing a Financial Sanction against GOOGLE LLC' (Decision 2019) www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf accessed 11 June 2020.

[35] Deceptive Experiences to Online Users Reduction Act 2019 www.congress.gov/bill/116th-congress/senate-bill/1084/text accessed 11 June 2020; M. Kelly, 'Big Tech's 'Dark Patterns' Could Be Outlawed under New Senate Bill' (Article 2019) www.theverge.com/2019/4/9/18302199/big-tech-dark-patterns-senate-bill-detour-act-facebook-google-amazon-twitter accessed 11 June 2020.

[36] Landsec, 'Archived Privacy Policy Piccadilly Lights' https://landsec.com/policies/privacy-policy/piccadilly-lights-english accessed 11 June 2020.

[37] According to the Archived Privacy Policy Piccadilly Lights (n 37), the data collection ended in September 2018.

[38] A. McStay and L. Urquhart, '"This Time with Feeling?" Assessing EU Data Governance Implications of Out of Home Appraisal Based Emotional AI'. [2019] 24 First Monday 10 https://doi.org/10.5210/fm.v24i10.9457 accessed 11 June 2020.

[39] Council of Europe, Committee on Culture, Science, Education and Media, Rapporteur Mr Jean-Yves LE DÉAUT, 'Technological Convergence, Artificial Intelligence and Human Rights' (Report 2017) www.assembly.coe.int/nw/xml/XRef/XRef-DocDetails-EN.asp?FileId=23531 accessed 11 June 2020 para. 26.

require a collective answer (e.g., by including them in the blacklist of commercial practices),[40] since enforcement in individual cases risks being ineffective in remedying harmful effects on society as a whole.

Moreover, emotional AI is arguably challenging the very underlying rationality-based paradigm imbued in (especially, but not limited to) consumer protection law. Modern legality is characterized by a separation of rational thinking (or reason) from emotion and consumer protection essentially rely on rationality.[41] As noted by Maloney, the law works from the perspective that rational thinking and emotion 'belong to separate spheres of human existence; the sphere of law admits only of reason; and vigilant policing is required to keep emotion from creeping in where it does not belong'.[42] The law is traditionally weighted towards the protection of the verifiable propositional content of commercial communications; however, interdisciplinary research is increasingly recognizing the persuasive effect of the unverifiable content (i.e., images, music)[43] and has long recognized that people interact with computers as social agents and not just tools.[44] It may be reasonably argued that the separation of rationality from affect in the law fails to take interdisciplinary insights into account.[45] In relation to this, the capacity of the current legal framework to cope with the advancements is in doubt. In particular, since the development of emotion detection technology facilitates the creation of emotion-evolved consumer-facing interactions, it poses challenges to the framework which relies on rationality.[46] The developments arguably raise concerns regarding the continuing reliance on the rationality paradigm within consumer protections, and hence consumer self-determination and individual autonomy, as core underlying principles of the legal protections.

Motivating a Constitutional Debate

The need for guidance about how to apply and, where relevant, complement existing consumer protection laws (in the broad sense) in light of the rise of

[40] European Parliament and Council Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L 149, Annex I. D. Clifford, 'Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making, a True Path to the Dark Side?', in L. Edwards, E. Harbinja, and B. Shaffer (eds) *Future Law: Emerging Technology, Regulation and Ethics* (Edinburgh University Press 2020).

[41] D. Clifford, 'The Emergence of Emotional AI Emotion Monetisation and Profiling Risk, Nothing New?', *Ethics of Data Science Conference* (Paper 2020, forthcoming).

[42] T. Maroney, 'Law and Emotion: A Proposed Taxonomy of an Emerging Field' [2019] 30 Law Hum Behav 119.

[43] M. Hütter and S. Sweldens, 'Dissociating Controllable and Uncontrollable Effects of Affective Stimuli on Attitudes and Consumption' [2018] 45 J Consum Res 320, 344.

[44] M. Lee, 'Understanding Perception of Algorithmic Decisions: Fairness, Trust, and Emotion in Response to Algorithmic Management' [2018] 5 BD&S 1, 2.

[45] Clifford (n 7) 82.

[46] In particular, such technologies allow for the development of inter alia content, formats, and products, or indeed entire campaigns that are optimized (i.e., at least at face value) and tailored by emotion insights. Clifford (n 7).

emotional AI motivates the need for a debate at a more fundamental level, looking at constitutional and ethical frameworks. The following paragraphs – revolving around three main observations – focus on the former of these frameworks, and will highlight how emotion detection and manipulation may pose threats to the effective enjoyment of constitutional rights and freedoms.

What's in a Name?

By way of preliminary observation, it should be stressed that, as noted by Sunstein, manipulation has 'many shades' and is extremely difficult to define.[47] Is an advertising campaign by an automobile company showing a sleek, attractive couple exiting from a fancy car before going to a glamorous party 'manipulation'? Do governments – in an effort to discourage smoking – engage in 'manipulation' when they require cigarette packages to contain graphic, frightening health warnings, depicting people with life-threatening illnesses? Is showing unflattering photographs of your opponent during a political campaign 'manipulation'? Is setting an opt-out consent system for deceased organ donation as the legislative default 'manipulation'? Ever since Nobel Prize winner Richard Thaler and Cass Sunstein published their influential book *Nudge*, a rich debate has ensued on the permissibility of deploying choice architectures for behavioural change.[48] The debate, albeit extremely relevant in the emotional AI context, exceeds the scope of this chapter, and is inherently linked to political-philosophical discussions. A key takeaway from Sunstein's writing is that, in a social order that values free markets and is committed to freedom of expression, it is 'exceptionally difficult to regulate manipulation as such'.[49] He suggests to consider a statement or action as manipulative to the extent that it does not sufficiently engage or appeal to people's capacity for reflective and deliberative choice. This reminds us of the notions of consumer self-determination and individual autonomy, which we mentioned previously and which will also be discussed further in this section.

From Manipulation over Surveillance to Profiling Errors

Second, it is important to understand that, in addition to the concerns over its manipulative capabilities, on which the chapter focused so far, emotional AI and

47 Sunstein (n 19).

48 See, e.g., H. Micklitz, L. Reisch and K. Hagen, 'An Introduction to the Special Issue on "Behavioural Economics, Consumer Policy, and Consumer Law"' [2011] 34 J Consum Policy 271 https://doi.org/10.1007/s10603-011-9166-5 accessed 11 June 2020; R. Calo, 'Digital Market Manipulation' [2014] 82 Geo Wash L Rev 995; D. Citron and F. Pasquale, 'The Scored Society: Due Process for Automated Predictions' [2014] 89 Wash L Rev 1 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209 accessed 11 June 2020; H. Micklitz, A. Sibony, and F. Esposito (eds), *Research Methods in Consumer Law* (Edward Elgar 2018).

49 Sunstein (n 19).

its employment equally require to take into consideration potential *harmful affective impacts*, on the one hand, and potential *profiling errors*, on the other. In relation to the former (the latter are discussed later), it is well-known that surveillance may cause a chilling effect on behaviour[50] and, in this way, encroach on our rights to freedom of expression (Article 10 ECHR; Article 10 CFREU), freedom of assembly and association (Article 11 ECRH; Article 12 CFREU), and – to the extent that our moral integrity is at stake – our right to private life and personal identity (Article 8 ECHR; Article 7 CFREU).[51] Significantly, as noted by Calo, '[e]ven where we know intellectually that we are interacting with an image or a machine, our brains are hardwired to respond as though a person were actually there'.[52] The mere observation or perception of surveillance can have a chilling effect on behaviour.[53] As argued by Stanley (in the context of video analytics), one of the most worrisome concerns is 'the possibility of widespread chilling effects as we all become highly aware that our actions are being not just recorded and stored, but scrutinized and evaluated on a second-by-second' basis.[54] Moreover, such monitoring can also have an impact on an individual's ability to 'self-present'.[55] This refers to the ability of individuals to present multifaceted versions of themselves,[56] and thus behave differently depending on the circumstances.[57] Emotion detection arguably adds a layer of intimacy-invasion via the capacity to not only detect emotions as *expressed* but also detect underlying emotions that are being deliberately *disguised*. This is of particular significance, as it not only limits the capacity to self-present but potentially erodes this capacity entirely. This could become problematic if such technologies and the outlined technological capacity become commonplace.[58] In that regard, it is

[50] Clifford (n 42).

[51] See, e.g., the case of *Antović and Mirković* v. *Montenegro* concerning the installation of video surveillance equipment in auditoriums at a university, in which the ECtHR emphasized that video surveillance of employees at their workplace, whether covert or not, constituted a considerable intrusion into their 'private life' (*Antović and Mirković* v. *Montenegro* App no 70838/13 (ECtHR, 28 February 2018) para. 44). See also, e.g., *Liberty and Others* v. *the United Kingdom* App no 58243/00 (ECtHR, 1 July 2008); *Vukota-Bojić* v. *Switzerland* App no 61838/10 (ECtHR, 18 October 2016; *Bărbulescu* v. *Romania* App no 61496/08 (ECtHR, 5 September 2017).

[52] R. Calo, 'The Boundaries of Privacy Harm' (2011) 86 Indiana Law J 1131, 1147.

[53] One should also note surveillance can have a chilling effect even if it is private or public; see N. Richards, 'The Dangers of Surveillance' [2013] 126 Harv Law Rev 1934, 1935: '[W]e must recognize that surveillance transcends the public/private divide. Public and private surveillance are simply related parts of the same problem, rather than wholly discrete. Even if we are ultimately more concerned with government surveillance, any solution must grapple with the complex relationships between government and corporate watchers.'

[54] Stanley (n 6) 35–36.

[55] O. Lynskey, *The Foundations of EU Data Protection Law* (First, OUP 2016) 202, 218.

[56] R. Warner and R. Sloan, 'Self, Privacy, and Power: Is It All Over?' [2014] 17 Tul J Tech & Intell Prop 8.

[57] J. Rachels, 'Why Privacy Is Important' [1975] 4 Philos Public Aff 323, 323–333, 323-333. The author goes on to discuss how we behave differently depending on who we are talking to, and this has been argued as dishonest or a mask by certain authors; but the author disagrees, saying that these 'masks' are, in fact, a crucial part of the various relationships and are therefore not dishonest. See also H. Nissenbaum, 'Privacy as Contextual Integrity' [2004] 79 Wash L Rev 119.

[58] Clifford (n 7) 124; Clifford (n 42).

important to understand that emotional AI can have an impact on an individual's capacity to self-present irrespective of its accuracy (i.e., what is important is that the individual's belief or the mere observation or perception of surveillance can have a chilling effect on behaviour).[59]

The lack of accuracy of emotional AI, resulting in profiling errors and incorrect inferences, presents additional risks of harm,[60] including inconvenience, embarrassment, or even material or physical harm.[61] In this context, it is particularly important that a frequently adopted approach[62] for emotion detection relies on the six basic emotions as indicated by Ekman (i.e., happiness, sadness, surprise, fear, anger, and disgust). However, this classification is heavily criticized as not accurately reflecting the complex nature of an affective state.[63] The other major approaches for detecting emotions, namely the dimensional and appraisal-based approach, also present challenges of their own.[64] As Stanley puts it, emotion detection is an area where there is a special reason to be sceptical, since many such efforts spiral into 'a rabbit hole of naïve technocratic simplification based on dubious beliefs about emotions'.[65] The AI Now Institute at New York University alerts (in the light of facial recognition) that new technologies reactivate 'a long tradition of physiognomy – a pseudoscience that claims facial features can reveal innate aspects of our character and personality' – and emphasizes that contextual, social, and cultural factors play a larger role in emotional expression than was believed by Ekman and his peers.[66] Leaving the point that emotion detection through facial expressions is a pseudoscience to one side, improving the accuracy of emotion detection more generally may arguably require more invasive surveillance to gather more contextual insights and signals, paradoxically creating additional difficulties from a privacy perspective. Building on the revealed circumstances, the risks associated with profiling are strongly related to the fact that the databases being mined for inferences are often 'out-of-context, incomplete or partially polluted', resulting in the risk of

[59] Calo (n 53) 1142–1143.

[60] For example, practical use cases such as the ones in health care or pseudo-health care shed light on the potential for inaccuracy to have damaging effects on the physical and mental well-being of the individual concerned. For details, see, e.g., Clifford (n 42).

[61] Ibid.

[62] AI Now Institute, New York University, 'AI Now Report 20184; (Report 2018), https://ainowinstitute.org/AI_Now_2018_Report.pdf 14.

[63] In this regard, it is interesting to refer to the work of Barret, who views the focus on basic emotions as misguided, as such categories fail to capture the richness of emotional experiences. L. Barrett, 'Are Emotions Natural Kinds?' [2006] 1 Perspectives on Psychological Science 28, as cited by R. Markwica, *Emotional Choices: How the Logic of Affect Shapes Coercive Diplomacy* (Oxford University Press 2018) 18, 72.

[64] Clifford (n 42).

[65] For more details, see Stanley (n 6) 38–39.

[66] AI Now Report 2018 (n 63) 14. For a discussion in the context of emotion detection, see also A. McStay, 'Empathic Media and Advertising: Industry, Policy, Legal and Citizen Perspectives (the Case for Intimacy)' [2016] 3 BD&S 1, 3–6.

false positives and false negatives.[67] This risk remains unaddressed by the individual participation rights approach in the EU data protection framework. Indeed, while the rights of access, correction, and erasure as evident in the EU General Data Protection Regulation may have theoretical significance, the practical operation of these rights requires significant effort and is becoming increasingly difficult.[68] This in turn may have a significant impact on the enjoyment of key fundamental rights and freedoms, such as inter alia the right to respect for private and family life and protection of personal data (Article 8 ECHR; Articles 7–8 CFREU); equality and non-discrimination (Article 14 ECHR; Articles 20–21 CFREU); and freedom of thought, conscience, and religion (Article 9 ECHR; Article 10 CFREU); but also – and this brings us to our third observation – the underlying key notions of *autonomy* and *human dignity*.

Getting to the Core Values: Autonomy and Human Dignity

Both at the EU and Council of Europe level, institutions have stressed that new technologies should be designed in such a way that they preserve human dignity and autonomy – both physical and psychological: 'the design and use of persuasion software and of ICT or AI algorithms . . . must fully respect the dignity and human rights of all users'.[69] Manipulation of choice can inherently interfere with autonomy.[70] Although the notion of autonomy takes various meanings and conceptions, based on different philosophical, ethical, legal, and other theories,[71] for the purposes of this chapter, the Razian interpretation of autonomy is adopted, as it recognizes the need to facilitate an environment in which individuals can act autonomously.[72] According to Razian legal philosophy, rights are derivatives of autonomy[73] and, in contrast with the traditional liberal approach, autonomy

[67] B. Koops, 'On Decision Transparency, or How to Enhance Data Protection after the Computational Turn' in M. Hildebrandt and K. de Vries (eds), *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology* (Routledge 2013) 199.

[68] Koops (n 68) 199.

[69] Parliamentary Assembly, 'Technological Convergence, Artificial Intelligence and Human Rights' (Recommendation 2102 2017) https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726&lang=en accessed 11 June 2020 para. 9.1.5. In relation to bio-medicine, reference can be made to the 1997 Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (also known as 'Oviedo Convention'). At EU level, see, for example, in the area of robotics and AI the European Parliament resolution on civil law rules on robotics: Parliament resolution with recommendations to the Commission 2015/2103(INL) on Civil Law Rules on Robotics [2015] OJ C 252.

[70] P. Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (1st ed., Cambridge University Press 2014).

[71] E. Harbinja, 'Post-Mortem Privacy 2.0: Theory, Law, and Technology' [2017] 31 Int Rev Law Comput Tech 26, 29.

[72] Clifford (n 7) 277.

[73] J. Raz, The Morality of Freedom (Clarendon Press, 1986) 247.

requires more than simple non-interference. Raz's conception of autonomy does not preclude the potential for positive regulatory intervention to protect individuals and enhance their freedom. In fact, such positive action is at the core of this conception of autonomy, as a correct interpretation must allow effective choice in reality, thus at times requiring regulatory intervention.[74] Raz argues that certain regulatory interventions which support certain activities and discourage those which are undesirable 'are required to provide the conditions of autonomy'.[75] According to Raz, '[a]utonomy is opposed to a life of coerced choices. It contrasts with a life of no choices, or of drifting through life without ever exercising one's capacity to choose. Evidently the autonomous life calls for a certain degree of self-awareness. To choose one must be aware of one's options.'[76] Raz further asserts: 'Manipulating people, for example, interferes with their autonomy, and does so in much the same way and to the same degree, as coercing them. Resort to manipulation should be subject to the same conditions as resort to coercion.'[77] Hence the manipulation of choice can inherently interfere with autonomy, and one can conclude that through this lens, excessive persuasion also runs afoul of autonomy.[78]

Autonomy is inherent in the operation of the democratic values, which are protected at the foundational level by fundamental rights and freedoms. However, there is no express reference to a *right to autonomy* or *self-determination* in either the ECHR or the CFREU. Despite not being expressly recognized in a distinct ECHR provision, the European Court of Human Rights (further 'ECtHR') has ruled on several occasions that the protection of autonomy comes within the scope of Article 8 ECHR,[79] which specifies the right to respect for private and family life. This connection has been repeatedly illustrated in the ECtHR jurisprudence dealing with individuals' fundamental life choices, including inter alia in relation to sexual preferences/orientation, and personal and social life (i.e., including a person's interpersonal relationships). Such cases illustrate the role played by the right to privacy in the development of one's personality through self-realization and autonomy (construed broadly).[80] The link between the right to privacy and autonomy is thus strong, and therefore, although privacy and autonomy are not synonyms,[81] it may be reasonably argued that the right to privacy currently offers an avenue for

74 P. Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (1st ed., Cambridge University Press 2014) 25–27; Raz (n 73) 382.

75 Raz (n 74) 420; Clifford (n 7).

76 Raz (n 74) 371; Clifford (n 7).

77 Raz (n 74).

78 Bernal (n 74) 26; Clifford (n 7).

79 For example, in *Pretty* v. *United Kingdom*, the ECtHR found that Article 8 ECHR included the ability to refuse medical treatment and that the imposition of treatment on a patient who has not consented 'would quite clearly interfere with a person's physical integrity in a manner capable of engaging the rights protected under art 8(1) of the Convention'. *Pretty* v. *United Kingdom* App no 2346/02 (ECtHR, 29 April 2002) para. 63.

80 Clifford (n 7) 104.

81 See more, e.g., Clifford (n 7) 104–105.

protection of autonomy (as evidenced by the ECtHR case law).[82] The emergence of emotional AI and the detection of emotions in real time through emotion surveillance challenges the two strands of the right simultaneously, namely (1) privacy as seclusion or intimacy through the detection of emotions and (2) privacy as freedom of action, self-determination, and autonomy via their monetization.[83]

Dignity, similar to autonomy, cannot be defined easily. The meaning of the word is by no means straightforward, and its relationship with fundamental rights is unclear.[84] The Rathenau Institute has touched upon this issue, noting that technologies are likely to interfere with other rights if the use of technologies interferes with human dignity.[85] However, there is little or no consensus as to what the concept of human dignity demands of lawmakers and adjudicators, and as noted by O'Mahony, as a result, many commentators argue that it is at best meaningless or unhelpful, and at worst potentially damaging to the protection of human rights.[86] Whereas a full examination of the substantive content of the concept is outside the scope of this chapter, it can be noted that human dignity, despite being interpreted differently due to cultural differences,[87] is considered to be a *central value* underpinning the entirety of international human rights law,[88] one of the core principles of fundamental rights,[89] and the basis of most of the values emphasized in the ECHR.[90] Although the ECHR itself does not explicitly mention *human dignity*,[91] its importance has been highlighted in several legal sources related to the ECHR,

[82] Ibid, 110.

[83] K. Ziegler, 'Introduction: Human Rights and Private Law – Privacy as Autonomy' in K. Ziegler (ed), *Human Rights and Private Law: Privacy as Autonomy* (1st ed., Hart Publishing 2007). This view is shared by Yeung in her discussion of population-wide manipulation; see K. Yeung, 'A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework (DRAFT)' (Council of Europe 2018) https://rm.coe.int/draft-study-of-the-implications-of-advanced-digital-technologies-inclu/16808ef255 accessed 11 June 2020 29.

[84] See, e.g., D. Feldman, 4;Human Dignity as a Legal Value: Part 14; [1999] Public Law 682, 690.

[85] For details, see R. van Est and J. Gerritsen, 'Human Rights in the Robot Age: Challenges Arising from the Use of Robotics, Artificial Intelligence, and Virtual and Augmented Reality' (Rathenau Instituut Expert report written for the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe 2017) www.rathenau.nl/sites/default/files/2018-02/Human%20Rights%20in%20the%20Robot%20Age-Rathenau%20Instituut-2017.pdf accessed 11 June 2020 27–28.

[86] C. O'Mahony, 'There Is No Such Thing as a Right to Dignity' [2012] 10 Int J Const Law 551.

[87] O'Mahony (n 87) 557–558.

[88] O'Mahony (n 87) 552.

[89] Its value is emphasized in a number of international treaties and national constitutional documents. For details, see, e.g., O'Mahony (n 87) 552–553.

[90] See, for instance, *Pretty* v. *United Kingdom (2346/02) [2002] ECHR 423 (29 April 2002)*, where the ECtHR held that the 'very essence of the Convention is respect for human dignity and human freedom' (para. 65). The Universal Declaration of Human Rights – on which the ECHR is based – provides that '[a]ll human beings are born free and equal in dignity and rights' (Article 1). For details, see R. van Est and J. Gerritsen (n 86) 27–28.

[91] Except Protocol No. 13 to the Convention for the Protection of Human Rights and Fundamental Freedoms concerning the abolition of the death penalty in all circumstances.

including the case law of ECtHR and various documents of the CoE.[92] Human dignity is also explicitly recognized as the foundation of all fundamental rights guaranteed by the CFREU,[93] and its role was affirmed by the Court of Justice of the EU (further 'CJEU').[94]

With regard to its substantive content, it can be noted that as O'Mahony argues, perhaps the most universally recognized aspects of human dignity are equal treatment and respect.[95] In the context of emotional AI, it is particularly relevant that although human dignity shall not be considered as a right itself,[96] it is the source of the right to personal autonomy and self-determination (i.e., the latter are derived from the underlying principle of human dignity).[97] As noted by Feldman, there is arguably no human right which is unconnected to human dignity; however, 'some rights seem to have a particularly prominent role in upholding human dignity', and these include the right to be free of inhuman or degrading treatment, the right to respect for private and family life, the right to freedom of conscience and belief, the right to freedom of association, the right to marry and found a family, and the right to be free of discriminatory treatment.[98] Feldman argues that, apart from freedom from inhuman and degrading treatment, these rights are 'not principally directed to protecting dignity and they are more directly geared to protecting the interests in autonomy, equality and respect'.[99] However, it is argued that these interests – autonomy, equality, and respect – are important in providing circumstances in which 'dignity can flourish', whereas rights which protect them usefully serve as a cornerstone of dignity.[100] In relation to this, since the employment of emotional AI may pose threats to these rights (e.g., to the right to respect for private and family life, as illustrated above, or to the right to be free of discriminatory treatment),[101] in essence it may pose threats to human dignity, respectively. To illustrate, one may refer to the analysis of live facial recognition technologies by the EU Agency for Fundamental Rights (further 'FRA'),[102] emphasizing that the processing of facial

[92] R. van Est and J. Gerritsen (n 86) 27–28.

[93] Article 1 of the Charter provides that human dignity is inviolable and shall be respected and protected. See also, e.g., A. Barak, 'Human Dignity as a Framework Right (Motherright)', in A. Barak, *Human Dignity: The Constitutional Value and the Constitutional Right* (Cambridge University Press, 2015) 156–169.

[94] Case C-377/98 *Netherlands* v. *European Parliament and Council of the European Union* [2001] ECR I-7079 paras 70–77.

[95] O'Mahony (n 87) 560.

[96] See, e.g., O'Mahony (n 87); Feldman (n 85).

[97] O'Mahony (n 87) 574.

[98] Feldman (n 85) 688.

[99] Ibid.

[100] Ibid.

[101] For details about interaction between discrimination and dignity, see, e.g., AI Now Report 2018 (n 63) 14; Feldman (n 85) 688.

[102] Although this report focuses on the employment of technologies in the context of law enforcement, certain insights are relevant both for private and public sectors. European Union Agency for Fundamental Rights, 'Facial Recognition Technology: Fundamental Rights Considerations in the

images may affect human dignity in different ways.[103] According to FRA, human dignity may be affected, for example, when people feel uncomfortable going to certain places or events, change their behaviours, or withdraw from social life. The 'impact on what people may perceive as surveillance technologies on their lives may be so significant as to affect their capacity to live a dignified life'.[104] FRA argues that the use of facial recognition can have a negative impact on people's dignity and, relatedly, may pose threats to (rights to) privacy and data protection.[105]

To summarize, the deployment of emotional AI in a business-to-consumer context necessitates a debate at a fundamental, constitutional level. Although it may benefit both businesses and consumers (e.g., by providing revenues and consumer satisfaction respectively), it has functional weaknesses[106] and also begs for the revealed legal considerations. Aside from the obvious privacy and data protection concerns, from the consumer's perspective, individual autonomy and human dignity as overarching values may be at risk. Influencing activities evidently interfere not only with an individual's autonomy and self-determination, but also with the individual's freedom of thought, conscience, and religion.[107] It may be clear, as the CoE's Committee of Ministers has noted, that also in other contexts (e.g., political campaigning), fine-grained, subconscious, and personalized levels of algorithmic

Context of Law Enforcement' (Paper 2019) https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf accessed 11 June 2020.

103 Ibid, 20.

104 Ibid.

105 Ibid, 33. Academic researchers have also argued that facial recognition technologies are to be treated as 'the Plutonium of AI', 'nuclear-level threats', 'a menace disguised as a gift', and an 'irresistible tool for oppression', which shall be banned entirely and without further delay both in public and private sectors . L. Stark, 'Facial Recognition Is the Plutonium of AI' (Article 2019) https://xrds.acm.org/article.cfm?aid=3313129 accessed 11 June 2020; E. Selinger and W. Hartzog, 'What Happens When Employers Can Read Your Facial Expressions?' (Article 2019) www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html accessed 11 June 2020; W. Hartzog, 'Facial Recognition Is the Perfect Tool for Oppression' (Article 2018) https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 accessed 11 June 2020; E. Selinger, 'Amazon Needs to Stop Providing Facial Recognition Tech for the Government' (Article 2018) https://medium.com/s/story/amazon-needs-to-stop-providing-facial-recognition-tech-for-the-government-795741a016a6 accessed 11 June 2020; E. Selinger, 'Why You Can't Really Consent to Facebook's Facial Recognition' (Article 2019) https://onezero.medium.com/why-you-cant-really-consent-to-facebook-s-facial-recognition-6bb94ea1dc8f accessed 11 June 2020. It remains to be seen whether legislators will adopt specific rules on face recognition technologies. Although the European Commission apparently contemplated a temporary five-year ban on facial recognition, the final version of its White Paper on Artificial Intelligence of 19 February 2020 no longer draws such a hard line (COM (2020) 65 final); see J. Espinoza, 'EU Backs Away from Call for Blanket Ban on Facial Recognition Tech' (Article 2020) www.irishtimes.com/business/innovation/eu-backs-away-from-call-for-blanket-ban-on-facial-recognition-tech-1.4171470 accessed 15 June 2020. California recently adopted a Bill, referred to as the Body Camera Accountability Act, which (if signed into law) would ban the use of facial recognition software in police body cameras. See R. Metz, 'California Lawmakers Ban Facial-Recognition Software from Police Body Cams' (Article 2019) https://edition.cnn.com/2019/09/12/tech/california-body-cam-facial-recognition-ban/index.html accessed 11 June 2020.

106 See, e.g., Stanley (n 6); Barrett (n 64); Feldman (n 85).

107 R. van Est and J. Gerritsen (n 86) 23.

persuasion may have significant effects on the cognitive autonomy of individuals and their right to form opinions and take independent decisions.[108] As a result, not only the exercise and enjoyment of individual human rights may be weakened, but also democracy and the rule of law may be threatened, as they are equally grounded on the fundamental belief in the equality and *dignity* of all humans as *independent* moral agents.[109]

4.3 SUGGESTIONS TO INTRODUCE NEW (CONSTITUTIONAL) RIGHTS

In the light of the previously noted factors, it comes as no surprise that some authors have discussed or suggested the introduction of some novel rights, in order to reinforce the existing legal arsenal.[110] Although both autonomy and dignity as relevant underlying values and some relevant rights such as right to privacy, freedom of thought, and freedom of expression are protected by the ECHR, some scholars argue that the ECHR does not offer sufficient protection in the light of the manipulative capabilities of emotional AI.[111] The subsequent paragraphs portray, in a non-exhaustive manner, such responses that concern the introduction of some new (constitutional) rights.

A first notable (American) scholar is Shoshana Zuboff, who has argued (in a broader context of *surveillance capitalism*)[112] for the 'right to the future tense'. As noted by Zuboff, 'we now face the moment in history when the elemental right to future tense is endangered' by digital architecture of behavioural modification owned and operated by 'surveillance capital'.[113] According to Zuboff, current legal frameworks as mostly centred on privacy and antitrust have not been sufficient to prevent undesirable practices,[114] including the exploitation of technologies for manipulative purposes. The author argues for the laws that reject the fundamental legitimacy of certain practices,

> including the illegitimate rendition of human experience as behavioral data; the use of behavioural surplus as free raw material; extreme concentrations of the new means of production; the manufacture of prediction products; trading in behavioral futures; the use of prediction products for third-party operations of modification, influence and control; the operations of the means of behavioural modification; the

[108] Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes (n 3), para. 9.
[109] Ibid.
[110] See, e.g., Yeung (n 84); Zuboff (n 31); J. Bublitz, 'My Mind Is Mine!? Cognitive Liberty as a Legal Concept' in E. Hildt and A. Franke (eds), *Cognitive Enhancement: An Interdisciplinary Perspective* (Springer Netherlands 2013).
[111] Yeung (n 84) 79–80.
[112] Zuboff (n 31).
[113] Ibid., 332.
[114] Ibid., 344.

https://doi.org/10.1017/9781108914857.005 Published online by Cambridge University Press

accumulation of private exclusive concentrations of knowledge (the shadow text); and the power that such concentrations confer.[115]

While arguing about the rationale of the so-called right to the future tense, the author relies on the importance of free will (i.e., Zuboff argues that in essence manipulation eliminates the freedom to will). Consequently, there is no future without the freedom to will, and there are no subjects but only 'objects'.[116] As the author puts it, 'the assertion of freedom of will also asserts the right to the future tense as a condition of a fully human life'.[117] While arguing for the recognition of such a right as a human right, Zuboff relies on Searle, who argues that elemental rights are crystallized as formal human rights only at that moment in history when they come under systematic threat. Hence, given the development of surveillance capitalism, it is necessary to recognize it as a human right. To illustrate, Zuboff argues that no one is recognizing, for example, a right to breathe because it is not under attack, which cannot be said about the right to the future tense.[118]

German scholar Jan Christoph Bublitz argues for the 'right to cognitive liberty' (phrased alternatively a 'right to mental self-determination'), relying in essence on the fact that the right to freedom of thought has been insignificant in practice, despite its theoretical importance.[119] Bublitz calls for the law to redefine the right to freedom of thought in terms of its theoretical significance in light of technological developments capable of altering thoughts.[120] The author argues that such technological developments require the setting of normative boundaries 'to secure the freedom of the *forum internum*'.[121]

In their report for the Council of Europe analyzing human rights in the robot age, Dutch scholars Rinie van Est and Joost Gerritsen from the Rathenau Institute suggest reflecting on two novel human rights, namely, the right to not be measured, analyzed or coached and the right to meaningful human contact.[122] They argue that such rights are indirectly related to and aim to elaborate on existing human rights, in particular, the classic privacy right to be let alone and the right to respect for family life (i.e., the right to establish and develop relationships with other human beings).[123] While discussing the rationale of a potential right not to be measured, analyzed, or coached, they rely on scholarly work revealing detrimental effects of ubiquitous monitoring, profiling or scoring, and

[115] Ibid.
[116] Ibid, 332, 336–337.
[117] Ibid.
[118] Ibid, 332; J. Searle, *Making the Social World: The Structure of Human Civilization* (Oxford University Press 2010).
[119] Bublitz (n 111).
[120] J. Bublitz, 'Freedom of Thought in the Age of Neuroscience' [2014] 100 Archives for Philosophy of Law and Social Philosophy 1; Clifford (n 7) 286.
[121] Ibid, 25.
[122] R. van Est and J. Gerritsen (n 86) 43–45; Clifford (n 7) 287.
[123] R. van Est and J. Gerritsen (n 86) 43.

persuasion.[124] They argue that what is at stake given the technological development is not only the risk of abuse but the right to remain anonymous and/or the right to be let alone, 'which in the robot age could be phrased as the right to not be electronically measured, analyzed or coached'.[125] However, their report ultimately leaves it unclear whether they assume it is necessary to introduce the proposed rights as new formal human rights. Rather, it calls for the CoE to clarify how these rights – the right to not be measured, analyzed, or coached, and the right to meaningful human contact – could be included within the right to privacy and the right to family life respectively.[126] In addition to considering potential novel rights, the Rathenau report calls for developing fair persuasion principles, 'such as enabling people to monitor the way in which information reaches them, and demanding that firms must be transparent about the persuasive methods they apply'.[127]

According to UK scholar Karen Yeung, manipulation may threaten individual autonomy and the 'right to cognitive sovereignty'.[128] While arguing about the rationale of such a right, Yeung relies on the importance of individual autonomy and on the Razian approach comparing manipulation to coercion,[129] as discussed previously. In addition, Yeung relies on Nissenbaum, who observes that the risks of manipulation are even more acute in a digital world involving 'pervasive monitoring, data aggregation, unconstrained publication, profiling, and segregation', because the manipulation that deprives us of autonomy is more subtle than the world in which lifestyle choices are punished and explicitly blocked.[130] When it comes to arguing about the need to introduce a new formal human right, Yeung notes that human dignity and individual autonomy are not sufficiently protected by Articles 8, 9, and 10 of the ECHR; however, the study in question does not provide detailed arguments in that regard. The author also refrains from elaborating on the content of such a right.[131]

Some novel rights are discussed at the institutional level as well. For example, the CoE's Parliamentary Assembly has proposed working on guidelines which would cover, among other things, the recognition of some new rights, including the right not to be manipulated.[132]

Further research is undoubtedly necessary to assess whether the current legal framework is not already capable of accommodating the developments properly.

[124] For reference see R. van Est and J. Gerritsen (n 86) 43–44.
[125] Ibid, 44.
[126] Ibid, 43–45.
[127] Rathenau Institute argues that such principles could be developed by the Council of Europe. R. van Est and J. Gerritsen (n 86) 26.
[128] Yeung (n 84) 79.
[129] Ibid, 79.
[130] Yeung (n 84); H. Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford Law Books 2010) 83.
[131] Yeung (n 84) 79–80.
[132] Parliamentary Assembly (n 70).

https://doi.org/10.1017/9781108914857.005 Published online by Cambridge University Press

While the introduction of novel constitutional rights may indeed contribute to defining normative beacons, we should at the same time be cautious not to dilute the significance of constitutional rights by introducing new ones that could, in fact, be considered as manifestations of existing constitutional rights.[133] Hence, it is particularly important to delineate, as noted by Clifford, between primary and secondary law, and to assess the capabilities of the latter in particular.[134] In other words, it is necessary to exercise restraint and consider what already exists and also to delineate between rights and the specific manifestation of these rights in their operation and/or in secondary law protections (i.e., derived sub-rights). For example, key data subject rights like the right to erasure, object, access, and portability are all manifestations of the aim of respecting the right to data protection as balanced with other rights and interests. Admittedly, while the right to data protection has been explicitly recognized as a distinct fundamental right in the CFREU, this is not the case in the context of the ECHR, where the ECtHR has interpreted the right to privacy in Article 8 ECHR as encompassing informational privacy.[135] The rich debate on the relation between the right to privacy and the right to data protection, and how this impacts secondary law like the GDPR and Convention 108+, clearly exceeds the scope of this chapter.[136]

4.4 BLUEPRINT FOR A FUTURE RESEARCH AGENDA

The field of affective computing, and more specifically the technologies capable of detecting, classifying, and responding to emotions – in this chapter referred to as

[133] Clifford (n 7) 287. This reminds us of the discussion about the positioning of consumer rights as fundamental rights; see, e.g., S. Deutch, 'Are Consumer Rights Human Rights? (Includes Discussion of 1985 United Nations Guidelines for Consumer Protection)' [1994] 32 Osgoode Hall Law Journal. For a general criticism of the creation of new human rights, see Ph. Alston, 'Conjuring up New Human Rights: A Proposal for Quality Control' [1984] 78 The American Journal of International Law 607.

[134] Clifford (n 7) 287.

[135] See, for instance, *Satakunnan Markkinapörssi OY and Satamedia OY* v. *Finland [2017] ECHR 607*, para. 137, in which the ECtHR derived a (limited form of) right to informational self-determination from Article 8 ECHR.

[136] For further reference, see Clifford (n 7) 124–133, and references there to M. Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the CJEU's Constitutional Reasoning' [2019] 20 German Law Journal; O. Lynskey, 'Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order' [2014] 63 International & Comparative Law Quarterly 569; H. Hijmans, *The European Union as Guardian of Internet Privacy* (Springer International Publishing 2016); G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer International Publishing 2014); G. González Fuster and R. Gellert, 'The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right' [2012] 26 *International Review of Law, Computers & Technology* 73; J. Kokott and C. Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' [2013] International Data Privacy Law; S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, and S. Nouwt (eds) *Reinventing Data Protection?* (Springer 2009).

emotional AI – hold promises in many application sectors, for instance, for patient well-being in the health sector, for road safety, consumer satisfaction in retail sectors, and so forth. But, just like most (if not all) other forms of artificial intelligence, emotional AI brings with it a number of challenges and calls for assessing whether the existing legal frameworks are capable of accommodating the developments properly. Due to its manipulative capabilities, its potential harmful affective impact and potential profiling errors, emotional AI puts pressure on a whole range of constitutional rights, such as the right to respect for private and family life, non-discrimination, and freedom of thought, conscience, and religion. Moreover, the deployment of emotional AI poses challenges to individual autonomy and human dignity as underlying values underpinning the entirety of international human rights law, as well as to the underlying rationality-based paradigm imbued in law.

Despite the constitutional protection already offered at the European level, some scholars argue, in particular in the context of the ECHR, that this framework does not offer sufficient protection in light of the manipulative capabilities of emotional AI. They suggest (contemplating or introducing) novel rights such as the right to the future tense; the right to cognitive liberty (or, alternatively, the right to mental self-determination); the right to not be measured, analyzed, or coached; the right to cognitive sovereignty; and the right not to be manipulated.

At the same time, it should be noted that the field of constitutional law (in this chapter meant to cover the field of European human rights law) is a very dynamic area that is further shaped through case law, along with societal, economic, and technological developments. The way in which the ECtHR has given a multifaceted interpretation of the right to privacy in Article 8 ECHR is a good example of this.

This motivates the relevance of further research into the scope of existing constitutional rights and secondary sub-rights, in order to understand whether there is effectively a need to introduce new constitutional rights. A possible blueprint for IACL's Research Group 'Algorithmic State, Society and Market – Constitutional Dimensions' could include

- empirical research into the effects of fine-grained, subconscious, and personalised levels of algorithmic persuasion based on affective computing (in general or for specific categories of vulnerable groups, like children[137]);
- interdisciplinary research into the rise of new practices, such as the trading or renting of machine learning models for emotion classification, which may escape the traditional legal protection frameworks;[138]

[137] See, in this regard, for instance, V. Verdoodt, 'Children's Rights and Commercial Communication in the Digital Era', KU Leuven Centre for IT & IP Law Series, n 10, 2020.

[138] See, for instance, M. Veale, R. Binns, and L. Edwards, 'Algorithms That Remember: Model Inversion Attacks and Data Protection Law' [2018] 376 Philosophical Transactions of the Royal Society A3.

https://doi.org/10.1017/9781108914857.005 Published online by Cambridge University Press

- doctrinal research into the scope and limits of existing constitutional rights at European level in light of affective computing; Article 9 ECHR and Article 8 CFREU seem particularly interesting from that perspective;
- comparative research, on the one hand, within the European context into constitutional law traditions and interpretations at the national level (think of Germany, where the right to human dignity is explicitly recognised in Article 1 Grundgesetz, versus Belgium or France, where this is not the case), and on the other hand, within the global context (comparing, for instance, the fundamental rights orientated approach to data protection in the EU and the more market-driven approach in other jurisdiction such as the US and Australia[139]); and
- policy research into the level of jurisdiction, and type of instrument, best suited to tackle the various challenges that emotional AI brings with it. (Is there, for instance, a need for a type of 'Oviedo Convention' in relation to (emotional) AI?)

At the beginning of this chapter, reference was made to the CoE's Declaration on the Manipulative Capabilities of Algorithmic Processes of February 2019.[140] In that Declaration, the Committee of Ministers invites member States to

> initiat[e], within appropriate institutional frameworks, open-ended, informed and inclusive public debates with a view to providing guidance on where to draw the line between forms of permissible persuasion and unacceptable manipulation. The latter may take the form of influence that is subliminal, exploits existing vulnerabilities or cognitive biases, and/or encroaches on the independence and authenticity of individual decision-making.

Aspiring to deliver a modest contribution to this much-needed debate, this chapter has set the scene and hopefully offers plenty of food for thought for future activities of the IACL Research Group on Algorithmic State Market & Society – Constitutional Dimensions.

[139] Clifford (n 7) 331.
[140] Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes (n 3), para. 9.

https://doi.org/10.1017/9781108914857.005 Published online by Cambridge University Press