

## Ethical Concerns over Facial Recognition Technology

**Abstract:** The article intends to discuss the impact of facial recognition (FR) technology by critically assessing the divergent viewpoints, expressed by the corporate world and by civil society in the news media, through the discourse analysis of representative textual samples. FR software is one of the most recent developments in the use of biometric data for identification. Its applications, which range from unlocking your smartphone, renting a car and taking an online exam to police monitoring of image databases, are strongly debated on opposite sides. Tech companies extol the level of security of biometric authentication when compared to simple usernames and passwords, claiming the quintessential authenticity of the human face. Voices of civil society and advocacy groups, instead, stress the risk of extended video surveillance and the legal vacuum that surrounds the technology. A main claim is that biometric face recognition is not exempt from bias, error rates and false positives. Besides, though still in a pilot stage, FR development towards the reading of emotions increases anxiety over its power to detect the signals that are wittingly or unwittingly sent in human face-to-face interaction. In the light of this socio-technical controversy, the article aims to reflect on today's man-machine interactional configurations and their ethical impact, as the debate increasingly permeates public discourse.

*Keywords:* artificial intelligence, ethics, man-machine interaction, privacy, surveillance

### 1. Introduction

This article sets out to highlight a few aspects of the ethics debate concerning the use of facial recognition (FR) technology from a discursive perspective,<sup>1</sup> starting from the controversy it has generated since entering the mainstream in the last few years. The topic is a further development in the emerging contribution of discourse studies to the cross-disciplinary big data debate that is affecting all fields of knowledge.<sup>2</sup> It is motivated by a wider interest in the ways in which technology discourses probe into social complexities,<sup>3</sup> especially when contentious issues polarise public opinion, in this case pre-eminently, with conflicting concerns about security and privacy.

In a nutshell, facial recognition emerges from several decades of civilian and military research. Based on software and algorithms, it is capable of analysing digital images and recognising faces in them by crosschecking facial features with a database. After being used for security and surveillance,

---

<sup>1</sup> John Flowerdew and John E. Richardson, eds., *The Routledge Handbook of Critical Discourse Studies* (Abingdon and New York: Routledge, 2018).

<sup>2</sup> For a recapitulation of the debate in the humanities and social sciences and the insights that a linguistically informed analysis can provide, see Maria Cristina Paganoni, *Framing Big Data: A Linguistic and Discursive Approach* (Cham: Palgrave Macmillan/Springer Nature, 2019).

<sup>3</sup> Ian Roderick, *Critical Discourse Studies and Technology: A Multimodal Approach to Analyzing Technoculture* (London: Bloomsbury, 2016).

it has been commercialised as “a mature technology ... achieving a better performance than human”<sup>4</sup> and is now ubiquitous. As vast amounts of data are required to build pattern recognition, FR has been boosted by the use of big data and machine learning.

Several firms now supply this technology and platforms make it available to the public and private sector. Amazon has developed and sells its own software (Rekognition),<sup>5</sup> while Facebook uses DeepFace as a face detector tool.<sup>6</sup> Biometric facial recognition authentication is now a regular household technology with the iPhone X, which deserves its merit of having made consumers comfortable with it. While offering personalised experience for consumers, the uses of FR exceed the mere business and marketing perspective to serve important social needs. In the words of its proponents, FR helps to trace missing children, identifies threats and prevents frauds, crimes, shoplifting and harassment, leading to the arrest of murderers, drug and human traffickers, sexual offenders and terrorists.<sup>7</sup> Proponents also refer to the added feeling of security that the technology may bring. Besides, FR has potential benefits for the visually impaired. In sum, the breadth of FR applications in a number of societal fields reveals the depth of its engagement in the lives of ordinary people.

At the same time, such a widespread technology is at the centre of much controversy. While developers extol its virtues, voices of civil society and advocacy groups express concerns about its social, political and ethical implications. Because of its reliance on sensitive biometric information, FR raises a number of ethical issues and concerns about privacy, human rights and civil liberties<sup>8</sup> that do not go unnoticed by its opponents. Among these concerns, which are now central to the developing field of machine ethics at the intersection of computer science, law and ethics,<sup>9</sup> there are forms of social control including political and religious beliefs, cross-border mobility, gender, ethnic profiling, and non-cooperative, non-consensual photos.<sup>10</sup>

In light of the above, what will be addressed in the following article will position FR technology within the current discussion on the benefits and threats of big data and machine learning, where it belongs. More specifically, the focus of the argumentation will be placed on the dynamics of the emerging ethics debate, in particular as concerns the balance between personal and public security

<sup>4</sup> Issa Traore, Mohammed Alshahrani and Mohammad S. Obaidat, “State of the Art and Perspectives on Traditional and Emerging Biometrics: A Survey”, *Security and Privacy*, 1.6 (2018), 7.

<sup>5</sup> Allison Matyus, “Amazon’s Facial Recognition Updates Can Detect Fear, among Other Emotions”, *Digital Trends* (14 August 2019), [www.digitaltrends.com](http://www.digitaltrends.com): “Amazon announced on Monday improvements to the service that includes better accuracy for gender identification and emotion detection. Amazon said, ‘we have improved accuracy for emotion detection (for all seven emotions: Happy, sad, angry, surprised, disgusted, calm, and confused) and added a new emotion: Fear’”.

<sup>6</sup> After facing a class-action lawsuit over the violation of user privacy with its facial recognition tools, Facebook has very recently made DeepFace an opt-in feature that requires explicit user consent to be activated.

<sup>7</sup> In 2011, FR technology helped to confirm the identity of Osama bin Laden when he was killed in a US raid.

<sup>8</sup> On 14 May 2019, for example, San Francisco became the first American city to ban its police and law enforcement agencies from using facial-recognition systems.

<sup>9</sup> Brent Mittelstadt et al., “The Ethics of Algorithms: Mapping the Debate”, *Big Data & Society*, 3.2 (December 2016), 2: “machine ethics ... investigates how best to design moral reasoning and behaviours into autonomous algorithms as artificial moral and ethical agents”.

<sup>10</sup> Kelly A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York: New York U.P., 2011); Jake Laperruque, “Preserving the Right to Obscurity in the Age of Facial Recognition”, in *The Century Foundation’s Report on Surveillance and Privacy* (20 October 2017), [tcf.org/about](http://tcf.org/about).

versus human rights and civil liberties.<sup>11</sup>

## 2. Methodology and Data Set

Moving from the assumption that our experiences of technology are framed by the ways we discuss and represent it, the issue under analysis is investigated by means of a qualitative toolkit that combines Discourse and Critical Discourse Analysis. Both provide a linguistically informed approach to an understanding of the relationship between language, representations of technology and their ideologies. The approach is interdisciplinary, enriched with insights from the social sciences, in particular in the emerging field of the ethics of artificial intelligence (AI).<sup>12</sup>

For the purpose of this analysis, which is qualitative in nature, textual material was drawn from two main specialised domains, corporate and news discourse, which are emblematic of the ideological polarisation that is currently generated between the technological viewpoint that praises FR, and political, social and civic concerns that express unease about its unregulated use. While AI companies advertise FR, thus somewhat underestimating the risk of ethical breaches, the news media, which amplify the spectrum of societal views, are more prone to depicting its shadows together with its lights.

Corporate sources were selected by searching the phrase ‘top facial recognition companies in 2019’ on the Google search engine and then cross-checking the names thus retrieved in the *Financial Times*, *Forbes*, *Fortune* and *Wired* because of their focus on leading trends in business and tech innovation. At that point, five companies and their respective software were selected, three located in the Asia-Pacific region, SenseTime (SensePass Pro) and Megvii (Face++), in China,<sup>13</sup> and NEC Corporation in Japan, to which Facewatch in the UK and FaceFirst in the US were added. Textual material was drawn from each company’s corporate website and from promotional videos, when available. Microsoft, Google (FaceNet), Apple (FaceID), IBM (i2 FR software), Facebook (DeepFace) and Amazon (Rekognition) were also taken into account, since they have all developed their own facial recognition system, tapping into large data sets of images.

The news corpus was manually collected from the web, with “facial recognition” as the search query. It consists of thirty-eight articles, retrieved from the UK and US mainstream press and of eighteen from tech, science and business magazines in English, in the time period spanning from March 2018 to February 2020. The transcripts of two videos on FR uploaded to YouTube by the *Economist*, “Facial Recognition Technology Will Change the Way We Live” on 1 November 2017, and “China: Facial Recognition and State Control” on 24 October 2018 were also added, because of

<sup>11</sup> See Jonathan Shaw, “Exposed: The Erosion of Privacy in the Internet Era”, *Harvard Magazine*, Sept-Oct. (2009), 38-43, and also, Lucas Introna and Helen Nissenbaum, “Facial Recognition Technology: A Survey of Policy and Implementation Issues”, Organisation, Work and Technology Working Paper Series (Lancaster University: The Department of Organisation, Work and Technology, 2010).

<sup>12</sup> See Michael Anderson and Susan Leigh Anderson, “Machine Ethics: Creating an Ethical Intelligent Agent”, *AI Magazine*, 28.4 (2014), 15-26.

<sup>13</sup> The two Beijing-based companies trained their FR technology on MSCeleb, Microsoft’s data set of roughly ten million faces that has now been deleted from the Internet. In October 2019, both SenseTime and Megvii were put on a blacklist of the US Department of Commerce for human rights violations against Xinjiang’s Muslim minorities.

their focus on the technological and the socio-political viewpoint respectively, for a total of fifty-eight items.

Aid to investigate this heterogeneous data set was provided by the use of the ATLAS.ti Cloud, the web-based version of the ATLAS.ti 8 software package for computer-assisted qualitative data analysis.

<sup>14</sup> Its interface and data visualisation facilitate the exploration of (multimodal) textual materials beyond counting occurrences. The way in which the function of coding is implemented allows the researcher great flexibility in highlighting portions of data, creating quotations and associating them with interpretive concepts, i.e. positive and negative connotations of facial recognition. In this case in particular, two functions were found to be useful, first the generation of word clouds in order to identify and code key lexical items and, second, the ability to retrieve these items, which are embedded in wider stretches of text, to highlight the features of discourse semantics to which the CDA approach was applied.

### 3. The Discursive Negotiation of Security and Privacy

As a result of its widespread adoption – from marketing to law enforcement – which was made possible by advancements in machine learning, the ‘virtue signalling’ of FR technology has amplified of late in corporate storytelling. This is to say that the dominant discourse in the global AI industry is orchestrated and strategically deployed to praise (and sell) FR accuracy and security in order to garner approval from stakeholders. As can be seen in examples (a), (b) and (c), the perfective use of the present tense in declarative sentences represents events as complete and bounded, implying that FR companies’ position is legitimate rather than problematic, at least potentially.

- (a) FaceFirst creates safer communities, more secure transactions and great customer experiences. Powered by the FaceFirst computer vision platform, the company uses face recognition and automated video analytics to help retailers, event venues, transportation centers and other organizations prevent crime and improve customer engagement while growing revenue. FaceFirst is highly accurate, fast, scalable, secure and private.<sup>15</sup>
- (b) Simple, secure and affordable, we are the premier choice of retail security companies in the UK. Facewatch is proven to stop crime before it happens.<sup>16</sup>
- (c) NEC’s original biometric authentication technologies in six areas –face recognition, iris recognition, fingerprint/palmprint recognition, voice recognition and ear acoustic authentication – are the best of their class in the world. NEC provides the most suitable solutions to customers’ needs with its biometric authentication technologies. In addition, by combining multiple biometric authentication systems, NEC’s solutions bring about even more robust security.<sup>17</sup>

<sup>14</sup> For its use in computer-assisted qualitative data analysis (CAQDAS), see Susanne Frieze, *Qualitative Data Analysis with ATLAS.ti*, Third Edition (London: Sage, 2019).

<sup>15</sup> FaceFirst, “A Complete Facial Recognition Platform”, [www.facefirst.com](http://www.facefirst.com).

<sup>16</sup> Facewatch, “The UK’s Leading Facial Recognition Security System”, [www.facewatch.co.uk](http://www.facewatch.co.uk).

<sup>17</sup> NEC, “NEC’s Biometric Authentication Technologies”, [www.nec.com](http://www.nec.com).

Far from being isolated, the above quotations, retrieved from the websites of leading AI companies worldwide, can be described as emblematic of a largely uncritical stance, whereby accompanying declarations of high-level ethical principles and self-regulatory codes attempt to build customer trust through persuasive discourse. However, the extent to which these statements are based on verifiable protocols and a more detailed picture of the functioning of this technology in real-world environments is not communicated to stakeholders.

- (d) We work to ensure that new technologies incorporate considerations of user privacy and where possible enhances it.... Sensitive data stays on the device, while the software still adapts and gets more useful for everyone with use.<sup>18</sup>
- (e) SenseTime aims to develop AI technologies that advance the world's economies, society and humanity for a better tomorrow.... We have made a number of technological breakthroughs, one of which is the first ever computer system in the world to achieve higher detection accuracy than the human eye.... Today, our technologies are trusted by over 700 customers and partners around the world to help address real world challenges.<sup>19</sup>

According to more skeptical views in digital ethics, it would seem that “the current conversation about algorithms absolves firms”.<sup>20</sup> Rhetorical adroitness oversimplifies the issue of trust, deflecting responsibility for what the AI industry designs, produces and commercialises, while corporate self-regulation leads to a fragmented landscape of ethical decisions, for example about how to protect biometric data when stolen.<sup>21</sup> In sum, a major limitation of AI companies' ethical approach lies in the fact that it fails to effectively address normative and political disagreement, from privacy law to human rights,<sup>22</sup> under the pressure of overriding business interests and the fast-changing scenario of AI implementation.

### 3.1 *A powerful technology and a booming industry in a data-driven world*

Among the keywords that were singled out to describe the winning features of FR in corporate discourse and in the news media we find lexical items and phrases that verge on the hyperbolic and stress the fast rise and ‘broader use’ of this ‘powerful technology’ and ‘booming industry’ with a ‘huge impact’. As expected, the type of narrative these words contribute to constructing is that of

---

<sup>18</sup> Google AI, “Our Approach to Facial Recognition”, <https://ai.google/responsibilities>.

<sup>19</sup> SenseTime, “About Us”, [www.sensetime.com](http://www.sensetime.com).

<sup>20</sup> Kirsten Martin, “Ethical Implications and Accountability of Algorithms”, *Journal of Business Ethics*, 160.4 (December 2019), 835-850.

<sup>21</sup> Luciano Floridi, “Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical”, *Philosophy & Technology*, 32.2 (June 2019), 185-193. In his article Floridi, who is Professor of Philosophy and Ethics of Information and Director of the Digital Ethics Lab of the Oxford Internet Institute, discusses five unethical risks in translating principles into practice: ethics shopping, ethics bluewashing, ethics lobbying, ethics dumping and ethics shirking (186). He argues that “shortcuts, postponements, or quick fixes do not lead to better ethical solutions but to more serious problems, which become increasingly difficult to solve the later one deals with them” (192).

<sup>22</sup> Brent Mittelstadt, “Principles Alone Cannot Guarantee Ethical AI”, *Nature Machine Intelligence*, 1 (November 2019), 501-507.

technological determinism, and is discursively reinforced by ergative verbs, like ‘expand’, ‘grow’, ‘increase’, ‘quadruple’, ‘spread’, and ‘widen’, used in intransitive constructions.<sup>23</sup> In (f) and (g), for example, the ascent of this biometric application is portrayed as a self-generating process that is endowed with autonomous life and strength and somehow inevitable and unstoppable once it has been hatched.

(f) From law enforcement to banking and from retail to healthcare, the market for facial recognition technology is expected to quadruple in size.... The appetite for facial recognition is growing fast for sound commercial reasons across a whole host of sectors in the UK, particularly retail and travel.<sup>24</sup>

(g) Facial recognition technology has spread prodigiously.<sup>25</sup>

In fact, it is not difficult to recognise a discursive variation and an expansion of the “Data Is Power” statement in the conventionality of this narrative. The refrain has been defining the big data ecosystem and economy since the last decade of the twentieth century.<sup>26</sup> What should be read between the lines, nonetheless, is that rapid advancements in artificial intelligence and machine learning are bringing about unpredictable and underestimated outcomes (example h), that go much beyond tagging faces in uploaded images on social media platforms and the convenience of unlocking smartphones.<sup>27</sup>

(h) As face-recognition technology spreads, so do ideas for subverting it.... Powered by advances in artificial intelligence (AI), face-recognition systems are spreading like knotweed.<sup>28</sup>

In other words, what the news media capture and amplify is a not unusual phenomenon. Technological innovation outpaces the ability of laws and regulations to keep up and the legal vacuum that follows pushes the ethics debate into the limelight. It means that, while data scientists address algorithms mostly as mathematical constructs in the seclusion of computer labs, the need for an ethical approach arises empirically in the public arena, at the discursive conflation “between formal definitions and popular usage of ‘algorithm’”.<sup>29</sup>

Because of its ubiquity and invasiveness, which derive from the power of digital technologies to create new and unplanned contexts and environments,<sup>30</sup> FR is now blamed for being instrumental to

<sup>23</sup> Michael A.K. Halliday, *An Introduction to Functional Grammar*, Fourth Edition, revised by Christian M.I.M. Matthiessen (Abingdon and New York: Routledge, 2014).

<sup>24</sup> Natasha Bernal, “Facial Recognition: Future of Business or Ethical Nightmare?”, *The Telegraph* (28 November 2018), [www.telegraph.co.uk](http://www.telegraph.co.uk).

<sup>25</sup> Ian Sample, “What Is Facial Recognition – and How Sinister Is It?”, *The Guardian* (29 July 2019), [www.theguardian.com](http://www.theguardian.com).

<sup>26</sup> Paganoni, *Framing Big Data*, 5.

<sup>27</sup> Niloufer Selvadurai, “Not Just a Face in the Crowd: Addressing the Intrusive Potential of the Online Application of Face Recognition Technologies”, *International Journal of Law and Information Technology*, 23.3 (Autumn 2015), 187-218.

<sup>28</sup> *The Economist*, “Fooling Big Brother” (15 August 2019), [www.economist.com](http://www.economist.com).

<sup>29</sup> Mittelstadt et al., “The Ethics of Algorithms”, 2.

<sup>30</sup> “The ethical impact of the digital transcends its design and uses. This is because digital technologies transform the reality in which we live by creating a new environment, new forms of (artificial) agency, and new affordances for our interactions with them”, Carl Öhman and David Watson, “Digital Ethics: Goals and Approaches”, in Carl Öhman and David Watson, eds., *The 2018 Yearbook of the Digital Ethics Lab* (Cham: Springer Nature, 2019), 2.

potentially unlawful public surveillance. Concurrently, government regulations are invoked to restrain its uses (examples i, j and k).

- (i) The extraordinary intrusiveness of facial recognition should not be underestimated.<sup>31</sup>
- (j) The technology's deployment has quickly outpaced regulation.... The potential for weaponization and abuse of facial-analysis technologies cannot be ignored.<sup>32</sup>
- (k) Hannah Couchman, advocacy and policy officer at Liberty says ... "We are still horrified to see how quickly this technology is expanding in use throughout the private sector into retail environments".<sup>33</sup>

A case in point of how FR may take a disproportionately dystopian turn is provided by the Chinese government, in its effort to establish a police state. We learn that Chinese police employ FR to fine jaywalkers in the street and show their faces on giant screens in order to shame the pedestrians into compliance. Even worse, in the autonomous region of Xinjiang, in north-west China, authorities have been scanning the facial features of hundreds of thousands of Muslim Uighurs since 2017, while enforcing arbitrary detention and political re-education, allegedly to prevent terrorism on a religious basis. Thus, the Uighur community suffers mass surveillance and persecution that are assisted by state-of-the-art FR technology.

- (l) AI companies such as CloudWalk, Yitu and SenseTime have partnered with the Chinese government to roll out facial recognition and predictive policing, particularly among minority groups such as the Uighur Muslims.<sup>34</sup>

True, the scary technology-aided violation of human rights now occurring in China is not the kind of political landscape that normally concerns human rights activists and civil society in more democratic countries. Nonetheless, "China's surveillance dragnet"<sup>35</sup> and brutal treatment of minorities, reported by outraged Western media (including a considerable section of the textual materials under analysis) and recently condemned by the UN, have further raised awareness about the importance of "watching the watchers".<sup>36</sup>

More generally, "the debate on the ethical impact and implications of digital technologies has reached the front pages of newspapers"<sup>37</sup> also in Western democracies, where incidents such as the

---

<sup>31</sup> Cynthia Wong, "We Underestimate the Threat of Facial Recognition Technology at Our Peril", *The Guardian* (17 August 2018), [www.theguardian.com](http://www.theguardian.com).

<sup>32</sup> Drew Harwell, "Amazon's Facial-Recognition Software Has Fraught Accuracy Rate, Study Finds", *The Washington Post* (27 January 2019), [www.washingtonpost.com](http://www.washingtonpost.com).

<sup>33</sup> Natasha Bernal, "Why We Should All Be Worried about Britain's Facial Recognition Experiment", *The Telegraph* (1 February 2019), [www.telegraph.co.uk](http://www.telegraph.co.uk).

<sup>34</sup> *The Financial Times*, "How Big Tech Is Struggling with the Ethics of AI" (29 April 2019), [www.ft.com](http://www.ft.com).

<sup>35</sup> Emma Graham-Harrison and Juliette Garside, "Revealed: Power and Reach of China's Surveillance Dragnet", *The Guardian* (24 November 2019).

<sup>36</sup> Hannah Devlin, "'We Are Hurtling towards a Surveillance State': The Rise of Facial Recognition Technology", *The Guardian* (5 October 2019), [www.theguardian.com/technology](http://www.theguardian.com/technology).

<sup>37</sup> Floridi, "Translating Principles into Practice", 185.

2018 Cambridge Analytica Scandal and Amazon’s secret AI recruiting tool that showed that recruiting processes were biased against women have awakened public consciousness to the social and political consequences of unregulated data-driven technology.<sup>38</sup>

### 3.2 Lack of consent, algorithmic bias, loss of privacy

The awareness that FR is expanding in largely uncharted territory explains why the news media frequently mention legal terms and concepts in its coverage, as well as references to the First Amendment in the US<sup>39</sup> and the GDPR for Europe. A first major issue remains that of the legal basis for the collection of biometric data, ‘affirmative’ user consent and the right to anonymity in public, which is no longer ‘granted’ nor ‘guaranteed’.

(m) What makes facial recognition different from other biometrics is that it’s very easy to collect from a person without their noticing.<sup>40</sup>

In the highly competitive digital economy, data are ‘gathered’ without consent, ‘pilfered’ and ‘stolen’ through ‘covert trickery’. Faces are ‘tracked’ within seconds and “in secret” since, unlike fingerprints and DNA samples, FR does not require much physical proximity. Current general data protection laws, however, require explicit consent to collect personal data. One of the reasons for this mandate is that data aggregation into a virtual identity may become ethically significant. It means that adding up sensitive information (political and religious affiliations, consumption patterns, health habits etc.), gleaned from the Internet, may potentially lead to predictive privacy harms for individuals and groups.

Furthermore, gender and racial bias, mistaken identities, false positives and identity theft are listed as actual risks (example n). At the lexical level, this anxiety is further conveyed by terms like ‘alter’, ‘discriminate’, ‘error rates’, ‘misassign’, ‘misclassify’, ‘misidentify’, ‘mistake’, ‘obscure’, ‘skew/skewed’ that are charged with negative associations. What is felt as a paradox in the ethics debate over FR is that algorithms, which should correct human fallibility, end up enhancing it and making individuals and communities more vulnerable, threatening human rights and civil liberties.

(n) Last year, the American Civil Liberties Union (ACLU) found that Amazon’s Rekognition software wrongly identified 28 members of Congress as people who had previously been arrested. It disproportionately misidentified African-Americans and Latinos (*Guardian*, 29 July 2019).<sup>41</sup>

Lastly, the news media voice the fear that loss of anonymity in public spaces may curb public

<sup>38</sup> “The resulting gap between the design and operation of algorithms and our understanding of their ethical implications can have severe consequences affecting individuals as well as groups and whole societies”, Mittelstadt et al., “The Ethics of Algorithms”, 2.

<sup>39</sup> See example (n) below.

<sup>40</sup> Jenny Jones, “Why I’m Fighting Police Use of Big Brother-Style Facial Recognition Technology”, *The Telegraph* (3 August 2018), [www.telegraph.co.uk/technology](http://www.telegraph.co.uk/technology).

<sup>41</sup> Sample, “What Is Facial Recognition”.

protest, political participation and legitimate dissent through the unlawful targeting of activists due to the constant surveillance that is augmented by facial recognition technology. Concurrently, the ubiquity of networked cameras will result in the privatisation of public urban spaces and “geofencing”, i.e. defining a virtual boundary around a real-world geographical area.

- (o) Civil liberties experts warn that it can also be used to secretly identify people – potentially chilling Americans’ ability to speak freely or simply go about their business anonymously in public.<sup>42</sup>

It appears that the next step, still in its pilot stage and not free from contention,<sup>43</sup> will be emotion AI and artificial empathy. In this case, algorithms are trained to read facial expression and body language, all signals that are intentionally or unwittingly sent in interaction.<sup>44</sup> Arguably, the major anthropological change that will follow will see quintessentially human acts transferred to machines,<sup>45</sup> while the Internet of Things will become bidirectional because of the flow of man-machine interaction.

It is also worth noticing that the discursive unfolding of the ethics debate over FR in public discourse sees the involvement of experts that ‘argue’, ‘explain’, ‘question’, ‘say’, ‘suggest’ and ‘warn’. Expert opinion that we find embedded in texts addressed to a general audience aims to translate specialised knowledge straight from the computer lab and to provide a theoretical framework for the lay public<sup>46</sup> that is empirically engaged in the understanding of technology and demands explanations and regulations.

- (p) Ultimately, experts say the field is still nascent, and a joint approach between the private and public sectors is required to build consensus.<sup>47</sup>

Taking our textual selection as a small but meaningful sample of the ways in which the ethics debate is empirically emerging in the conversation between the private and public sector, we cannot dismiss its discursive polarisation but we also notice the orientation towards a more flexible approach to technology (example p), but only if in reasonable compliance with democratic values.

#### 4. Concluding Remarks

The analysis has focused on the current discursive unfolding of the ethical implications of FR technology by reflecting upon the divergent viewpoints of the AI corporate world and voices from

<sup>42</sup> Natasha Singer, “Amazon Is Pushing Facial Technology That a Study Says Could Be Biased”, *The New York Times* (24 January 2019), [www.nytimes.com](http://www.nytimes.com).

<sup>43</sup> Douglas Heaven, “Why Faces Don’t Always Tell the Truth about Feelings”, *Nature* (26 February 2020), [www.nature.com](http://www.nature.com).

<sup>44</sup> Emotion Research Lab, “Moods or States of Mind Have Come to Stay”, [emotionresearchlab.com/blog](http://emotionresearchlab.com/blog).

<sup>45</sup> The blurring divide between biological and synthetic humans is the main theme of Ian McEwan’s new novel, *Machines like Me* (London: Cape, 2019). See also Rosi Braidotti, *The Posthuman* (Cambridge: Polity Press, 2013).

<sup>46</sup> See Giuliana Garzone, “News Production and Scientific Knowledge: Exploring Popularization as a Process”, in Giancarmine Bongo and Giuditta Caliendo, eds., *The Language of Popularization: Die Sprache der Popularisierung* (Bern: Peter Lang, 2014), and Marina Bondi et al., eds., *Discourse In and Through the Media: Recontextualizing and Reconceptualizing Expert Discourse* (Newcastle upon Tyne: Cambridge Scholars Publishing, 2015).

<sup>47</sup> *The Financial Times*, “How Big Tech Is Struggling with the Ethics of AI”.

civil society in the UK and the US, as they are reported and amplified in the news media. The hybridisation of expert, corporate and popular views is, after all, what lay people are regularly exposed to when they try to respond to the fast advancements of technological innovation.

As has been seen, the ethics debate over FR technology involves a complex set of issues that have come to the forefront in public discourse, and consequently in the news media, under the pressure of the fast implementation of machine learning in a variety of societal contexts, at times with unexpected and unpleasant outcomes. Strongly favoured by the global AI industry, this process has generated benefits for society in terms of security, safety and a better consumer experience, as promised by FR developers. However, it has also given rise to forms of bias, discrimination, predictive profiling and threats to basic human rights and civil liberties, up to political repression, as the one suffered by the Uighur people in China.

Quite expectedly, the AI industry adopts a narrative of technological progress largely oblivious to the far-reaching anthropological, political and social consequences of AI, while the news media report on the more problematic sides of AI. Nonetheless, this is evolving into an interesting phenomenon, an emerging public debate that is striving to forge a manageable digital ethics, putting algorithms and their ethical import under scrutiny.

As characteristic of the nonlinear reception of technological innovation within the complexities of science-society relations, the ethics debate is discursively polarised between expectations and threats, benefits and risks, but also empirically engaged in the discursive negotiation of the same. By itself, this collective attempt is what makes FR technology more human.