IDP
REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Dossier "Europe facing the digital challenge: obstacles and solutions"

Ethics and emerging technologies – facial recognition

Archil Chochia
Tallinn University of Technology (TalTech)

Teele Nässi
Tallinn University of Technology (TalTech)

Date of submission: May 2021
Accepted in: October 2021
Published in: December 2021

Abstract

Emerging technologies and digitalization have an increasing impact on our everyday lives. New technology solutions offer a variety of opportunities to our society, yet the ethical implications of this process have long been discussed by scholars in order to fully understand what the potential ethical risks are. One of such technologies is facial recognition. This article intends to contribute to the above indicated scholarly discussion by analyzing recent developments in the field, focusing on facial recognition.

Keywords

artificial intelligence; AI; digitalization; ethics; ethics of technology; facial recognition

Ética y tecnologías emergentes: reconocimiento facial

Resumen

Las tecnologías emergentes y la digitalización tienen un impacto cada vez mayor en nuestra vida cotidiana. Las nuevas soluciones tecnológicas ofrecen una variedad de oportunidades a nuestra sociedad; sin embargo, las implicaciones éticas de este proceso han sido discutidas durante mucho tiempo por los académicos para comprender completamente cuáles son los potenciales riesgos éticos. Una de estas tecnologías es el reconocimiento facial. Este artículo trata de contribuir a dicha discusión académica analizando los avances recientes en este campo, centrándose en el reconocimiento facial.

Palabras clave

inteligencia artificial; IA; digitalización; ética; ética de la tecnología; reconocimiento facial

Introduction

Ever since technologies have become part of our lives, the discussion on the positive and negative effects of these technologies and the technologization process has been a topic for debate on different levels. This research intends to contribute to such discussion on an academic level, focusing on facial recognition, and is partially based on earlier findings of the authors (please see Joamets & Chochia, 2021). When explaining the complexity of determining an attitude toward technologies, Winston and Edelbach (2011) talk about two distinctive viewpoints – techno-pessimism and techno-optimism. While techno-pessimists focus on the negative aspects of technology and remain sceptical of technological solutions, techno-optimists place emphasis on the benefits that technologies offer to society and remain confident that technological solutions will solve the potential problems of technology.

From the philosophical standpoint, this can be linked to two historical phases of technological analyses: the first being mid-twentieth-century classical hermeneutic critiques that focus on the negative effects on humans caused by modern technologies; and the second being an empirical approach looking at technology rather as socially determined elements through local use. A notable example of the first historical phase is philosopher Jacque Ellul, who believed that technology had developed at such a rapid pace that it could not be controlled by humans and therefore saw it as rather destructive (Ellul, 1964). On the other hand, the second phase approach shifts from general technology to a more nuanced approach, looking at local narratives, examining each technology individually and empirically, viewing it within the values and culture of those societies that use the technology in question (see, e.g., Brey, 2010; Verbeek, 2011). Similarly, to the rest of the branches of philosophy, ethics derives from supposedly simple questions; nevertheless, as John Deigh (2010, p.1) puts it, these questions often "seem simple, yet are ultimately perplexing".

Digitalization has been posing such new questions and, therefore, the ethical implications of digitalization process have long been discussed by scholars. Philosopher Deborah Johnson (2004, p.69) speaks of the information society as a society in which digital technologies shape "human activity and social institutions". Digitalization and emerging technologies affect our lives and are increasingly present in a growing number of fields (see, e.g., Kerikmäe *et al*., 2020). Legal scholars are trying to find the best way to regulate the emerging technologies; also, substantial research is devoted to understanding the implications of emerging technologies on legal systems (Brownsword & Goodwin, 2012, 2018). However, while both of the above approaches can be found in current scholarly discussions on the ethical aspects of technology, the emphasis is on the "continuity of people and technology with the rest of nature" (Parsons, pp. 6-9), while not enough attention is being paid to the widespread use of modern technologies, such as social media, Twitter, augmented reality, smartphones, internet and others, often resulting in moral and ethical issues (Deloitte, n.d.; Jobin *et al*., 2019).

The lack of literacy in digital ethics within our societies is alarming, as Beever *et al*. (2019, pp. 9-25) argue in their book *Understanding Digital Ethics*. They draw attention to the issues of technology control, moral agency, and responsibility, drawing parallels with the famous ethical thought experiment in moral philosophy, the "trolley problem", for example when it comes to autonomous vehicles.

The authors believe that digital ethics is a combination of two literacies: one being a digital literacy-understanding of modern technologies and information, and a second ethical literacy-understanding which is being motivated to act on the emerging ethical issues. And, consequently, in order to achieve a necessary understanding of digital ethics, it is absolutely crucial to possess a sufficient level of both digital literacy and ethical literacy.

Artificial intelligence (AI) is a field that is developing at a rapid pace and such rapid development has taken the legal and ethical discussion to another level. AI has already replaced humans in many actions performed and this process of "preplacement" is going fast forward (see, e.g., Joamets & Chochia, 2020; Troitiño *et al*., 2020, pp. 303-317). One of the particular areas in this development is Facial Recognition Technology (FRT) and the increasing use of this technology in different areas has provoked discussion due to its close link to human rights, specifically the right to privacy, one of the fundamental human rights. As Naker and Greenbaum (2017, p. 101) explain, "privacy is a precondition for democracy development and freedom. Without privacy, there is no freedom of expression, freedom of religion, or freedom of movement." This research tries to analyze FRT and explain what the human rights-related issue with its usage are.

1. History of facial recognition technology (FRT)

As Welinder (2012, p. 167) explains, facial parameters are extremely useful for identification due to distinction, availability, difficulty to alter, etc. The first scientific facial recognition indications date back to 1884 when an anatomist Welcker compared what was thought to be Raphael's skull with a self-portrait and compared the supposed skull of Kant with his death mask and found that the respective correlations were too good for chance. He used two-dimensional techniques; he provided accurate orthogonal perspective drawings as an outline of the skull and the death mask, and then attempted to superimpose the outlines, while making allowance for the outer tissues (Wilkinson, 2004). After that, there were several anthropologists and anatomists, who tried to perform the facial recognition of early hominids such as Neanderthal and Pithecanthropus, and others of the Stone Age (Verze, 2009, p. 8).

A computer technique for forensic purposes was first developed in the 1980s by Moss and his colleagues at London's University College in the UK. It was based on a system used for cranial reconstructive surgery. The system was developed for 3D surface data acquisition of the human face, involved limited manual intervention, and was subject to minimal human error (Arridge *et al*., 1985, p. 13; Moss, 1987, p. 9). As Gates (2011, p. 3) explains: "The search for automated face perception technologies and new forms of human-machine integration promises to make surveillance systems function more effectively and extend their reach over time and space. But whether these experimental technologies can or should be made to accomplish these goals remains open to debate, one that often plays out in press and policy discussions as a trade-off between 'security' and 'privacy'."

The facial recognition process, as we know it today, begins with the capturing of the face image, also known as the probe image (usually taken from a still or video camera, for example); then the face is being detected and extracted from the larger image (background or other faces); the system will then "normalize" the image in the database and pass it through the recognition software where the possible match will be made between the new image and database images (Introna & Nissenbaum, 2010, p. 11). As Spiesel (2020) explains, Facial recognition is a task-specific technology, which relies on the data obtained by its sensors and an algorithm, and it requires to be trained to perform the matching of the obtained images. By now, FRT is used around the world by different law enforcement agencies to monitor the public space via biometric data collection.

2. Protection of privacy

Protection of privacy is embodied in most human rights instruments, including the Charter of Fundamental Rights of the European Union, the Universal Declaration of Human Rights (UDHR), and the European Convention on Human Rights (ECHR). The General Data Protection Regulation (GDPR), which came into force on 25 May 2018, regulates the main issues about data protection law in the European Union (EU) with modern rules that fit better in a time where technology is evolving at a massive speed. GDPR's core principle is that personal data should not be collected, or processed, more than what is necessary for a certain purpose. As formulated in articles 1 and 2, the regulation protects fundamental rights and freedoms of a natural person and their right to the protection of their personal data. GDPR (art. 9) protects and requires consent for the collection of personal data, particularly sensitive data, including biometrics.

According to GDPR Article 4(14), biometric data is considered personal data resulting from specific technical processing. Biometric data allows confirming the unique identification of natural persons, such as facial images. The GDPR principles also include making clear to individuals when and how facial recognition data are being collected, stored, and used; developing data management practices that consider how individuals are enrolled and what the risks, harms, and benefits of such (in)voluntary enrolment and maintaining the accuracy and integrity of any stored data may be (National Telecommunications and Information Administration, 2016).

Although the GDPR protects individual personal and sensitive data, including biometrics, it remains unclear if facial images always fall under the scope of the GDPR, depending, for example, on the legal justification for processing, because a substantial public interest such as national security or public safety may provide a path for circumventing consent (Buckley & Hunter, 2011, p. 639). As underlined by Jennifer Lynch (2012, p. 14), staff attorney

with the Electronic Frontier Foundation and a researcher on biometrics and facial recognition, "advanced biometrics like face recognition creates additional concerns because the data may be collected in public without a person's knowledge."

The GDPR has somewhat regulated the use of biometric data, including FRT, but it is still not certain that the use of such technology always considers people's privacy. According to Omar Tene (2011, p. 21), "the use of biometrics raises privacy risks, including identity theft, function creep, and government surveillance." Buckley and Hunter (2011, p. 639) claim that "the application of facial recognition technology to an individual's facial image constitutes processing of personal data and, therefore, can only take place if a legal justification exists." This indicates that the processing of such data has to fall within the processing conditions set in GDPR article 7, and individuals must be informed of the process according to articles 10 and 11. The EU Agency for Fundamental Rights (FRA) conducted a study on the human rights issues related to FRT, however without guidance on possible legal regulation of the technology (FRA, 2019). The European Commission's White Paper on AI (2020) addresses remote biometric identification and indicates certain high-risk applications, with additional specific requirements.

3. Privacy gaps in facial recognition

The survey, done by German and Switzerland researchers in China, Germany, UK, and USA showed that almost half of all German (48%) and US responders (44%) believe that FRT increases privacy violations, and a majority of Germans (66%) and roughly half of UK and US responders believe that FRT increases surveillance (Steinacker *et al*., 2020, p. 5). More than half of all country responders agree that FRT increases security. Arguably, that is to be expected, because most of the people feel secure, and do not consider their privacy invaded if they see a camera in public areas or for example in shops. Seeing a camera might make individuals feel that if anything should happen to them or their property, someone will immediately notice and send help, if necessary. The analysis also showed that the interpretation of privacy threat is a strong and significant negative predictor of acceptance. In other words, the more a participant perceives the technology as a risk to their privacy, the less likely they are to accept FRT use in public (Steinacker *et al*., 2020, p. 5).

Researchers have raised the issues over privacy violations before. For example, Christopher S. Milligan (1999, p. 299) stated in his research that "in addition to the constitutional issues, there are also social and ethical issues that merit public debate. These questions deal with whether people are willing to live their lives under the watchful lens of a camera and monitor – whether they are able to sacrifice personal autonomy and risk governmental abuse of their data for the sense of safety and order which video surveillance provides". He further explains that "the use of video surveillance and facial recognition technology eliminates some amount of personal privacy and anonymity" (Milligan, 1999, p. 326). Jennifer Lynch (2012, p. 2) says that "face recognition technology, like other biometrics programs that collect, store, share and combine sensitive and unique data poses critical threats to privacy and civil liberties." Brenda Leong (2019, p. 113), director of strategy at the Future of Privacy Forum, continues: "the ethical considerations of where and how to use facial recognition systems even exceed the boundaries of traditional privacy considerations".

Even without security concerns, the presence of FRT severely damages the ability of regular people to maintain their anonymity in the public space. Akin to the evolving right to be forgotten, people ought to have the right to remain anonymous (Naker & Greenbaum, 2017, p. 109). Already in 1999, it was acknowledged that facial recognition and video surveillance technology can be successful in catching criminals and preventing criminal activity (Milligan, 1999, p. 323). However, with all its potential benefits, FRT can pose serious challenges to the right to privacy and data security. It creates problems of unwanted identification, discrimination, and the likely hacking of large datasets of not only faces, but also all the data associated with those faces (Naker & Greenbaum, 2017, p. 122). Bias FRT and discrimination issues against minorities are extensively discussed by Timnit Gebru (2020).

An example of a database using FRT comes from a company called Clearview AI. They have created a research tool, that is used by law enforcement agencies to identify perpetrators and victims of crimes. They provide their service worldwide and their facial recognition database has billions of images, which they have allegedly collected

from open sources. The database can be used by analysts, who can compare the uploaded crime scene images with publicly available images in the database. In their 31st plenary session, the European Data Protection Board (EDPB) raised concerns regarding certain developments in facial recognition technologies and expressed doubts as to whether any Union or Member State law provides a legal basis for using a service such as the one offered by Clearview AI (EDPB, 2020, p. 10). The EDPB was therefore of the opinion that the use of a service such as Clearview AI by law enforcement authorities in the European Union would, as it stands, likely not be consistent with the EU data protection regime. Steinacker *et al*. (2020, p. 1) discovered in their research, that while some of US Governments have banned the use of FRT by city and state agencies, there is currently no federal legislative consensus despite extensive activism for regulation. Neither has the European Commission nor any of the EU Member states explicitly ruled on FRT.

Amnesty International (2020), an organisation whose priority is to help people claim their rights, is also calling for a ban on the use, development, production, sale, and export of facial recognition technology for mass surveillance purposes by the police and other state agencies. The tension between the technology and the right to privacy highlight the dialectic between national security and law enforcement, economic efficiency or public health promoted through the application of facial recognition systems, on the one side, and concerns relating to the potential for disproportionately violating fundamental principles on our society such as the right to personal autonomy, anonymity, to being forgotten, to control one's own personal identifying information, and the person's right to protect the own human body, on the other (Naker & Greenbaum, 2017, p. 100).

During the COVID-19 pandemic, facial recognition was also considered by many as a tool to help fight the virus. Since the outbreak of the pandemic, the adoption or development of digital systems in order to control the spread of the infection, such as contact management software (e.g., the WHO-provided Go.Data2) and to track persons that may have been in contact with the virus (e.g., mobile contact-tracing applications), has attracted the attention of the public administration, private enterprises, and research institutions around the world (Ramos, 2020, p. 176). Professor Silvia Barona Vilar (2020) talks about how the employment of AI technologies, including facial recognition, in an attempt to eradicate the pandemic, shifts the balance between freedom and security towards the latter. Despite the enormous benefits of the technology, privacy-related consequences due to additional security and control measures put up a huge challenge in front of our societies. The Human Rights Watch (2020), along with numerous other organizations, published a joint statement, indicating some conditions that technology-assisted measures to fight the COVID-19 pandemic should meet in order to respect human rights.

Many of these novel systems developed to control the spread of infectious diseases have incorporated biometric technologies, such as facial recognition access control systems that can check people's temperature and identification systems that recognize people even if they are wearing protective masks (Ring, 2020, p. 4). The research carried out in China, France, Israel, Poland, Singapore, South Korea, and Russia about the FRT systems used during the COVID-19 pandemic and the information available on the analyzed systems, did not clarify which measures were being considered to guarantee that the personal data collected was used only to address the spread of COVID-19 and not for additional law enforcement and national security purposes, and it provided no assurance that risk assessments were adopted (Ramos, 2020, p. 178). There are also growing concerns that, once COVID-19 has passed, the data derived from these digital systems could be misused.

The lack of adequate regulations does not provide the certainty that governments will restrict their measures, particularly where there is no specific legislation establishing the rules on the processing, storing, or discarding of the collected data (Ramos, 2020, p. 178). In order to mitigate these risks, the European Commission went ahead and edited guidelines for apps supporting the fight against COVID-19 pandemic in relation to data protection (eHealth Network, 2020). Furthermore, the EDPB (2020) published some guidelines on the use of location data, contact tracing tools, and the processing of personal data. These documents provide valuable insights for facial recognition systems as well, since they enumerate applicable data protection principles and recommendations for this emergency period (Ramos, 2020, p. 179).

FRT is widely considered in different fields to try and use it as a tool to find better solutions. However, research often

points to the existing gaps of such technology and, consequently, to unsatisfactory results. An interesting research is being conducted in the field of experimental psychology, where facial cue is used in emotion recognition and deception detection attempt, but so far it has been concluded that facial cue detection does not aid deception recognition (please see e.g., Zloteanu *et al*., 2021, pp. 910-927).

Sandford and Bindemann (2020, pp. 294-297) talk about the usage of facial recognition in psychology and problems with the results delivered by working with subtle metric differences in facial configuration, concluding that "configuration theory provides limited explanatory power for recognition of familiar faces". Prof. Kosinski's (2021) research focuses on how FRT can determine several characteristics of individuals and argues that even though FRT is often a useful tool to improve human-technology interactions, it could also identify more sensitive data, such as political or sexual orientation, personality.

Using CCTV as a tool to identify individuals with the help of FRT, therefore having a "super recognizer ability" could be a great support to police in its work to fight crime, however, this technology also has its limitations (Davis *et al*., 2018, pp. 350-351). Brandy Dieterle (2021) explains how FRT makes it hard to truly stay anonymous due to the nature of social media engagement and argues that there is a need for more comprehensive research ethics when working with the intimate data of individuals. Such "improved" ethical standards are especially important in social media research, when working on minorities, such as sexual minorities.

There are also interesting legal precedents; for example, in early 2020, a Dutch court ruled that automated surveillance system violated human rights and ordered its immediate halt. A technology tool was used by the authorities to help them fight benefit and tax fraud, by identifying those individuals who might be committing the wrongdoing. Later in August 2020, The Royal Courts of Justice in London (EWCA Civ 1058, Case No: C1/2019/2670) issued the ruling stating that facial recognition technology violates personal freedoms, invades privacy, and is discriminatory. The court stated that South Wales Police use of Live Automated Facial Recognition technology, which engaged Article 8(1) of the European Convention on Human Rights, was not in accordance with the law for the purposes of Article 8(2) (EWCA Civ 1058, Case No: C1/2019/2670, p. 210). As for the ongoing use of Live Automated Facial Recognition technology, its Data Protection Impact Assessment did not comply with section 64(3)(b) and (c) of the UK Data Protection Act 2018 (A data protection impact assessment must include the following: an assessment of the risks to the rights and freedoms of data subjects and the measures envisaged to address those risks).

The case shows that the use of FRT violated right to privacy, because the appropriate safeguards, which apply to the processing of personal data, including biometric data, where not used. The judges also mentioned that the FRT was supposed to be used to identify and locate people who were suspected of criminality, or wanted by the courts and police, who might pose a risk, or who may be vulnerable, but in this case, the police scanned and identified everyone, and by doing this, violated privacy and data protection rights.

Conclusion

Emerging technologies and the digitalization process in general have an increasing impact on our everyday lives. These technologies bring various opportunities and offer solutions to us in a variety of fields. Professionals in all those fields try to measure the new opportunities and solutions that the use of these technologies would offer, trying to benefit from the technological progress and achieve new levels within these sectors. The opportunities are truly unique, while the process is extremely fast. However, ever since technology has taken an important part of our lives and the lives of our societies, the ethical implications of this process have been discussed by scholars, in order to fully understand what potential ethical risks are there from such "cooperation" between humans and technology.

The discussion on the positive and negative effects of these technologies and the technologization process has been topic for debate on different levels. This research intended to contribute to that debate at the academic level, focusing on facial recognition. A brief analysis of the situation with FRT usage in different fields and the feedback received from the scholars focusing their research on these questions, demonstrates evident gaps in the results delivered by FRT. Provided examples clearly indicate that very frequently there is an actual violation of human rights when

using a facial recognition technology, while often there is a genuine risk. As evidenced by the analysis, there is a lack of clear regulation regarding how, when and for what purposes this technology can be used in specific fields, and until there is one, the technology should not be used, as it is often in violation of human rights or entails clear risks of doing so. There is no argument whether FRT or AI technologies in general, can support our work in different fields and in various ways, extending our abilities and possibilities. However, as Spiesel (2020) puts it, assuming that conscious AI will care for humankind would be a mistake.

The EU has been a pioneer in the world trying to address the complicated issues related to the widespread and rapidly growing usage of modern technologies, including FTR. It has been providing extensive documentation on this topic. The European Commission's *Ethics Guidelines for Trustworthy Artificial Intelligence* is a huge step forward in this direction, in addition to all above-indicated documents, with some of them specifically addressing FRT. However, European efforts remain slow in comparison with how rapidly the technology is developing and used daily. When assessing challenges of regulatory framework on AI ethics, the European Parliamentary Research Service (2020) identified six main risks factors, which included a challenge of "a growing mismatch between the exponential growth of the AI market and a 'delayed' regulatory response."

Questions raised by the researchers from the specific fields where facial recognition has been used as a tool, demonstrate the need to further develop field-specific guidelines to ensure an ethical and human rights friendly employment of such technology. Parfet *et al*. (2020) interestingly compare AI technology to a child, as it needs to be educated and trained before we could rely on the results delivered by it. Just like children learn from their parents and from what their parents teach them, these technologies need to learn from what the data and programmes tell them.

References

AMNESTY INTERNATIONAL (2020). "Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance". In: *Amnesty International* [online]. Available at: https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/ [Accessed: 17 May 2021].

ARRIDGE, S.; MOSS, J. P.; LINNEY, A. D.; JAMES, D. R. (1985). "Three dimensional digitization of the face and skull". In: *Journal of Maxillofacial Surgery*, vol. 13, no. 3, pp. 136-143 [online]. DOI: https://doi.org/10.1016/S0301-0503(85)80034-5

BEEVER, J.; MCDANIEL, R.; STANLICK, N. A. (2019). *Understanding Digital Ethics: Cases and Contexts* [online]. Abingdon: Routledge. DOI: https://doi.org/10.4324/9781315282138

BREY, P. (2010). "Philosophy of technology after the empirical turn". In: *Techné: Research in Philosophy and Technology*, vol. 14, no. 1, pp. 36-48 [online]. DOI: https://doi.org/10.5840/techne20101416

BROWNSWORD, R.; GOODWIN, M. (2012). *Law and the Technologies of the Twenty-First Century* [online]. New York: Cambridge University Press. DOI: https://doi.org/10.1017/CBO9781139047609

BUCKLEY, B.; HUNTER, M. (2011). "Say Cheese! Privacy and facial recognition". In: *Computer Law and Security Review*, vol. 27, vol. 6, pp. 637-640 [online]. DOI: https://doi.org/10.1016/j.clsr.2011.09.011

CLEARVIEW.AI (n.d.). Clearview AI official website [online]. Available at: https://clearview.ai [Accessed: 17 May 2021].

COUNCIL OF EUROPE (1950). *European Convention for the Protection of Human Rights and Fundamental Freedoms* [online]. Available at: https://www.refworld.org/docid/3ae6b3b04.html [Accessed: 17 May 2021].

DAVIS, J. P.; FORREST, C.; TREML, F.; JANSARI, A. (2018). "Identification from CCTV: Assessing police super-recogniser ability to spot faces in a crowd and susceptibility to change blindness". In: *Appl Cognit Psychol*, no. 32, pp. 337-353 [online]. DOI: https://doi.org/10.1002/acp.3405

DEIGH, J. (2010). *An Introduction to Ethics* [online]. New York: Cambridge University Press. DOI: https://doi.org/10.1017/CBO9780511750519

DELOITTE (n.d.). *Europe's "Trustworthy AI" meets AI Ethics. The ethics of AI* [online]. Available at: https://www2.deloitte.com/nl/nl/pages/risk/articles/europes-trustworthy-ai-meets-ai-ethics.html [Accessed: 27 April 2021].

DIETERLE, B. (2021). "People As Data?: Developing an Ethical Framework for Feminist Digital Research". In: *Computers and Composition*, vol. 59 [online]. DOI: https://doi.org/10.1016/j.compcom.2021.102630

EHEALTH NETWORK (2020). "Mobile Applications to Support Contact Tracing in the EU's Fight against COVID-19" [online]. Available at: https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-19_apps_en.pdf [Accessed: 17 May 2021].

ELLUL, J. (1964). *The Technological Society*. New York: Vintage Books.

EUROPEAN COMMISSION (2020). "White Paper on Artificial Intelligence-A European approach to excellence and trust" [online]. Available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf [Accessed: 20 September 2021].

EUROPEAN DATA PROTECTION BOARD (EDPB) (2020). "Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak" [online]. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf [Accessed: 17 May 2021].

EUROPEAN PARLIAMENTARY RESEARCH SERVICE (2020). "European framework on ethical aspects of artificial intelligence, robotics and related technologies. European Added Value Assessment" [online]. Available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)654179 [Accessed: 23 September 2021].

EUROPEAN UNION (2012). *Charter of Fundamental Rights of the European Union*, 2012/C 326/02 [online]. Available at: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:12012P/TXT [Accessed: 17 May 2021].

EUROPEAN UNION (2016). *EU General Data Protection Regulation (GDPR)*. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN [Accessed: 17 May 2021].

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA) (2019). *Facial recognition technology: fundamental rights considerations in the context of law enforcement* [online]. Available at: https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law [Accessed: 20 September 2021].

GATES, K. A. (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* [online]. 2nd. ed. NYU Press. DOI: https://doi.org/10.18574/nyu/9780814732090.001.0001

GEBRU, T. (2020). "Race and gender". In: *The Oxford handbook of ethics of AI*, pp. 251-269 [online]. DOI: https://doi.org/10.1093/oxfordhb/9780190067397.013.16

HUMAN RIGHTS WATCH (2020). "Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights" [online]. Available at: https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight [Accessed: 17 May 2021].

INTRONA, L.; NISSENBAUM, H. (2010). "Facial Recognition Technology A Survey of Policy and Implementation Issues". In: *Organisation, Work and Technology Working Paper Series*. Lancaster: The Department of Organisation, Work and Technology of Lancaster University Management School.

JOAMETS, K.; CHOCHIA, A. (2020). "Artificial intelligence and its impact on labour relations in Estonia". In: *Slovak Journal of Political Sciences*, vol. 20, no. 2, pp. 255-277 [online]. DOI: http://doi.org/10.34135/sjps.200204 https://doi.org/10.34135/sjps.200204

JOAMETS, K.; CHOCHIA, A. (2021). "Access to Artificial Intelligence for Persons with Disabilities: Legal and Ethical Questions Concerning the Application of Trustworthy AI". In: *Acta Baltica Historiae et Philosophiae Scientiarum*, vol. 9, no. 1, pp. 51-66 [online]. DOI: https://doi.org/10.11590/abhps.2021.1.04

JOBIN, A.; IENCA, M.; VAYENA, E. (2019). "The global landscape of AI ethics guidelines". In: *Nature Machine Intelligence*, vol. 1, pp. 389-399 [online]. DOI: https://doi.org/10.1038/s42256-019-0088-2

JOHNSON, D. (2004). "Computer ethics". In: FLORIDI, L. (ed.). *The Blackwell Guide to the Philosophy of Computing and Information*, pp. 65-75 [online]. New York: Blackwell. DOI: https://doi.org/10.1002/9780470757017.ch5

KERIKMÄE, T.; HOFFMANN, T.; CHOCHIA, A. (2018). "Legal technology for law firms: determining roadmaps for innovation". In: *Croatian International Relations Review*, vol. 24, no. 81, pp. 91-112 [online]. Available at: https://hrcak.srce.hr/199994 [Accessed: 28 November 2021].

KERIKMÄE, T.; SOLARTE-VASQUEZ, M. C.; RUDANKO, M.; TROITIÑO, D. R. (eds.) (2020). *Inteligencia artificial: de la discrepancia regional a las reglas universales. Integración de percepciones políticas, económicas y legales*. Pamplona: Thomson Reuters.

KOSINSKI, M. (2021). "Facial recognition technology can expose political orientation from naturalistic facial images". In: *Sci Rep*, no. 11, 100 [online]. DOI: https://doi.org/10.1038/s41598-020-79310-1

LEONG, B. (2019). "Facial recognition and the future of privacy: I always feel like...somebody's watching me". In: *Bulletin of the Atomic Scientists*, vol. 75, no. 3, pp. 109-115 [online]. DOI: https://doi.org/10.1080/00963402.2019.1604886

LYNCH, J. (2012). "What Facial Recognition Technology Means for Privacy and Civil Liberties". In: *Senate Committee on the Judiciary* [online]. DOI: https://doi.org/10.2139/ssrn.2134497

MILLIGAN, C. S. (1999). "Facial recognition technology, video surveillance, and privacy". In: *Southern California Interdisciplinary Law Journal*, vol. 9, no. 1, pp. 295-334.

MOSS, J. P.; LINNEY, A. D.; GRINDROD, S. R.; ARRIDGE, S. R.; CLIFTON, J. S. (1987). "Three-dimensional visualization of the face and skull using computerized tomography and laser scanning techniques". In: *European Journal of Orthodontics*, vol. 9, no. 4, pp. 247-253 [online]. DOI: https://doi.org/10.1093/ejo/9.4.247

NAKER, S.; GREENBAUM, D. (2017). "Now you see me: Now you still do: Facial recognition technology and the growing lack of privacy". In: *Boston University Journal of Science and Technology Law*, vol. 23, no. 1, pp. 88-122.

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (2016). "Privacy Best Practices Recommendations for Commercial Facial Recognition Use" [online]. Available at: https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf [Accessed: 17 May 2021].

PARFETT, A.; TOWNLEY, S.; ALLERFELDT, K. (2020). "AI-based healthcare: a new dawn or apartheid revisited?". In: *AI & Society* [online]. DOI: https://doi.org/10.1007/s00146-020-01120-w

PARSONS, T. D. (2019). *Ethical Challenges in Digital Psychology and Cyberpsychology* [online]. Cambridge: Cambridge University Press. DOI: https://doi.org/10.1017/9781108553384

RAMOS, L. F. (2020). "Evaluating privacy during the COVID-19 public health emergency: the case of facial recognition technologies". In: *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*, pp. 176-179 [online]. New York: Association for Computing Machinery. DOI: https://doi.org/10.1145/3428502.3428526

RING, T. (2020). "Face ID Firms Battle Covid-19 as Users Shun Fingerprinting". In: *Biometric Technology Today*, vol. 4, pp. 1-2 [online]. DOI: https://doi.org/10.1016/S0969-4765(20)30042-4

ROYAL COURT OF JUSTICE (2019). *R (Bridges) vs. CC South Wales & ors*. EWCA Civ 1058, Case No: C1/2019/2670 [online]. Available at: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf [Accessed: 14 May 2021].

SANDFORD, A.; BINDEMANN, M., (2020). "Discrimination and recognition of faces with changed configuration". In: *Mem Cogn*, no. 48, pp. 287-298 [online]. DOI: https://doi.org/10.3758/s13421-019-01010-7

SPIESEL, C. (2020). "Technology's Black Mirror: Seeing, Machines, and Culture". In: *Int J Semiot Law* [online]. DOI: https://doi.org/10.1007/s11196-019-09679-4

STEINACKER, L.; MECKEL, M.; KOSTKA, G.; BORTH, D. (2020). "Facial Recognition: A cross-national Survey on Public Acceptance, Privacy, and Discrimination". In: *Law and ML Workshop*.

TENE, O. (2011). "Privacy: The new generations". In: *International Data Privacy Law*, vol. 1, no. 1, pp. 15-27 [online]. DOI: https://doi.org/10.1093/idpl/ipq003

THE GUARDIAN (2020). "Welfare surveillance system violates human rights, Dutch court rules" [online]. Available at: https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules [Accessed: 14 May 2021].

TROITIÑO, D. R.; KERIKMÄE, T.; SHUMILO, O.; RAMÍREZ BARBOSA, P. A. (2020). "El libro blanco sobre inteligencia artificial: análisis y comentarios sobre mercado, valores y cooperación europea". In: KERIKMÄE, T.; SOLARTE-VASQUEZ, M. C.; RUDANKO, M.; TROITIÑO, D. R. (eds.). *El Parlamento Europeo y la necesidad de una legislación común en un marco europeo de la inteligencia artificial. Inteligencia artificial: de la discrepancia regional a las reglas universales. Integración de percepciones políticas, económicas y legales*, pp. 303-317. Pamplona: Thomson Reuters.

UNITED KINGDOM (2018). "UK Data Protection Act" [online]. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [Accessed: 17 May 2021].

UNITED NATIONS (1948). "Universal Declaration of Human Rights" [online]. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights [Accessed: 17 May 2021].

VERBEEK, P.-P. (2011). *Moralizing Technology, Understanding and Designing the Morality of Things* [online]. Chicago: University of Chicago Press. DOI: https://doi.org/10.7208/chicago/9780226852904.001.0001

VERZE, L. (2009). "History of facial recognition". In: *Acta Biomed*, vol. 80, pp. 5-12.

VILAR, S. B. (2020). "La sociedad postcoronavirus con big data, algoritmos y vigilancia digital, ¿excusa por motivos sanitarios?, ¿y los derechos dónde quedan?". *Revista Boliviana de Derecho*, no. 30, pp. 14-39.

WELINDER, Y. (2012). "A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks". In: *Harvard Journal of Law and Technology*, vol. 26, no. 1, pp. 166-237.

WILKINSON, C. (2004). "Forensic facial reconstruction". Cambridge University Press.

WINSTON, M.; EDELBACH, R. (2011). *Society, Ethics and Technology* [online]. Belmont, CA: Wadsworth Publishing. DOI: https://doi.org/10.1017/CBO9781107340961

ZLOTEANU, M.; BULL, P.; KRUMHUBER, E. G.; RICHARDSON, D. C. (2021). "Veracity judgement, not accuracy: Reconsidering the role of facial expressions, empathy, and emotion recognition training on deception detection". In: *Quarterly Journal of Experimental Psychology*, vol. 74, no. 5, pp. 910-927 [online]. DOI: https://doi.org/10.1177/1747021820978851

Recommended citation

CHOCHIA, Archil; NÄSSI, Teele (2021). "Ethics and emerging technologies – facial recognition". *IDP. Internet, Law and Politics E-Journal*. No. 34. UOC [Accessed: dd/mm/aa]
http://dx.doi.org/10.7238/idp.v0i34.387466

About the authors

Archil Chochia
Tallinn University of Technology (TalTech)
archil.chochia@taltech.ee
Department of Law
Tallinn University of Technology
Ehitajate tee 5, Tallinn 19086, Estonia

Senior Researcher at TalTech Law School of Tallinn University of Technology. Dr. Chochia obtained his doctoral degree from Tallinn University of Technology in 2013. He has more than 90 academic publications and is a co-editor of the books *Political and Legal Perspectives of the EU Eastern Partnership Policy* (Springer, 2016), *Brexit: History, Reasoning and Perspectives* (Springer, 2018) and *Russian Federation in the Global Knowledge Warfare – Influence Operations in Europe and Its Neighbourhood* (Springer, 2021). Archil is a managing editor of *TalTech Journal of European Studies*. His research fields of interest are law and technology, ethical aspects of digitalization, alternative dispute resolution, EU integration, EU Neighbourhood Policy. Archil is a Senior Fellow of Weinstein International Foundation.

ORCID: https://orcid.org/0000-0003-4821-297X

Teele Nässi
Tallinn University of Technology (TalTech)
teenas@taltech.ee

Master level student at TalTech Law School of Tallinn University of Technology, Estonia. Ms. Nässi has obtained her diploma, BA in Law, from TalTech Law School of Tallinn University of Technology in 2012. Currently, Ms. Nässi works for local government as a lawyer, while she previously worked as a clerk at the Harju County court for five years.