Evaluating privacy during the COVID-19 public health emergency: the case of facial recognition technologies

Luis Felipe M. Ramos
United Nations University (UNU-EGOV) & JusGov/Universidade do Minho
Rua de Vila Flor 166, 4810-445,
Guimarães, Portugal
lfelipe.sm@gmail.com

ABSTRACT

The present article aims to discuss how governments have turned to biometric technologies to fight the spread of COVID-19, mainly through the adoption of facial recognition technologies, and the risks to people's privacy of inadequate measures to protect their personal data. We have identified seven systems from different countries (i.e., China, France, Israel, Poland, Singapore, South Korea, and Russia) that present some form of facial recognition during their operation and pointed out their functionalities and released information on safeguards for data protection. The data collected so far has shown that, in most countries, the necessary safeguards to protect people's privacy and their personal data in the short-term and long-term, are not receiving sufficient considerations.

CCS CONCEPTS

• **Security and privacy~Human and societal aspects of security and privacy~Privacy protections**
• Applied computing~Law, social and behavioral sciences~Law

KEYWORDS

Biometric Technologies, Facial Recognition, Personal Data, Privacy

ACM Reference format:

Luis Felipe M. Ramos. 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 (ICEGOV 2020), 23-25 September 2020, Athens, Greece*, 4 pages. https://doi.org/10.1145/3428502.3428526

ICEGOV'20, September 23–25, 2020, Athens, Greece

ACM ISBN 978-1-4503-7674-7/20/09…$15.00
https://doi.org/10.1145/3428502.3428526

1. INTRODUCTION

There has been an increase in the adoption of biometric technologies in the last decades, from both the public and the private sectors, and for the most varied finalities.

These technologies are distinguished by the use of personal traits to identify a person or authenticate a transaction performed by a specific person, based on physical (e.g., face, fingerprints, iris, and hand geometry) or behavioral (e.g., signature, gait, and keystroke dynamics) individual characteristics, which can be considered permanent and unique identifiers through the transformation of these characteristics into digital codes to be read by a machine [5],[26],[29].

Numerous applications can benefit from the use of biometric data [18]. Hereupon, biometrics can be used to secure elections [16],[17], provide border security [19],[28], and legal identity [2], among other applications. Concerning the lack of legal identity, which affects more than 1.1 billion people [33], the deployment of biometric identity systems can contribute to solve the issue, and consequently pursue the UN's 2030 SDGs (i.e., Goal 16).

Since the outbreak of the COVID-19 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.Data[2]) 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.

In this context, biometric systems stand out as a critical technology for early detection, patient screening, and public safety monitoring [1]. Many of these novel systems developed to control the spread of infectious diseases have incorporated biometric technologies, such as facial recognition access control

[2] https://www.who.int/godata

systems that can check people's temperature and identification systems that recognize people even if they are wearing protective masks [24], mostly together with artificial intelligence and machine learning technologies. Also, ideas of digital immunity passports, certificates, and applications have been discussed lately among strategies on how to exit from global lockdowns [27],[31].

Most of the deployed systems are based on personal data, such as individual characteristics, mobile phone records, geolocation, and proximity data, and sometimes even sensitive personal data, as personal health records.

Amid the COVID-19 pandemic, many governments started turning to facial recognition technologies to fight the spread of the infection by tracking quarantine evaders or measuring elevated temperatures of potentially infected individuals in crowds.

However, as government surveillance swiftly becomes the norm and facial recognition technology stalks the streets, a quick assessment of some of the proposed solutions started raising concerns on how compliant with the individual right to privacy these systems are.

We can expect that many of these often invasive technological powers to be de-escalated when the threat of COVID-19 is over or even will stop to be useful, but some will likely be maintained, enhanced, and reoriented to other purposes, if not faced with proper regulation.

This context shows that, in most cases, the urge to make these tools available may not have been accompanied by the proper data protection risks assessment, without which it is difficult to know if they are not equipped with adequate safeguards to protect privacy, presenting the potential to violate an individual's privacy and data protection rights [18],[20],[32].

The present work aims to evaluate the context some of the identified digital systems were developed, focusing on their adoption of facial recognition technologies and their concern with personal data protection.

The remainder of this article is organized as follows: Section 2 presents the adopted approach to select the systems and a brief overview of their functionalities and privacy issues. Section 3 presents concluding remarks and a perspective of further works.

2. APPROACH AND RESULTS

Concerning the prevention and control of the COVID-19 pandemic, different systems have been made available for various purposes, such as for digital contact tracing, quarantine and social distancing, big data analytics, and hot spot mapping.

This work focuses on digital systems made available or adopted by governments, and that includes some form of facial recognition technology. Data was collected from public sources online during June 2020, and the systems are presented by countries.

Although so far it was possible to identify seven systems from different countries (i.e., China, France, Israel, Poland, Singapore, South Korea, and Russia), due to space limitations, in this paper, only three are described.

The following sections present a brief description of how the selected systems work and their functionalities, and information on the existence of privacy policy existence, disclosure of data processing purposes, identification of the legal framework allowing the system, or other relevant information on privacy protection.

The Human Rights Watch, along with numerous other organizations, published a joint statement, indicating some conditions that technology-assisted measures to fight the COVID-19 pandemic should present, in order to respect human rights [13]:

- Be lawful, necessary, proportionate, transparent, and justified by legitimate public health objectives
- Be time-bound and only continue for as long as necessary to address the pandemic
- Be limited in scope and purpose, used only for the purposes of responding to the pandemic
- Ensure sufficient security of any personal data that is collected
- Mitigate any risk of enabling discrimination or other rights abuses against marginalized populations
- Be transparent about any data-sharing agreements with other public or private sector entities
- Incorporate protections and safeguards against abusive surveillance and give people access to effective remedies
- Provide for free, active, and meaningful participation of relevant stakeholders in data collection efforts

In this work, we will use these conditions to evaluate the selected digital systems on the existence of adequate safeguards for privacy protection.

2.1. China

In China, a set of applications named "Health Code Apps" were developed by private companies and adopted by authorities in cities and provinces across China. Their operation is based on an established tradition of population surveillance and control [6].

After installing the application, the user must fill in their personal information, including their ID number, residence address, and information on whether they have been with people carrying the virus, and symptoms they may be presenting. Based on that information, the app displays one of three colors: green means the user can go anywhere, yellow and red mean seven and 14 days of quarantine, respectively. There are reports that the app also collects and shares with law enforcement authorities people's location data without their consent.

The color determined by the application has a far-reaching impact on its hundreds of million users, as the local authorities across the country require people to show their app when they use public transportation, go shopping, or move across residential areas and the subway. Citizen's capability to move, work, and even obtain basic goods and medical assistance is dependent on the app's color scheme. Some residential area's access control systems are based on facial recognition technology, giving permission only those people with green code to enter, indicating that these systems are linked [23].

The Zhejiang provincial government – the first to adopt this type of application – has promulgated a set of standards for the

app, outlining broad and ambiguous categorization criteria. However, it is not clear how the companies involved in the development of the apps designed them and which criteria are considered for categorizing people. Other local governments have been authorized to establish their own rules for implementing these criteria in their districts. Without further insight into the app's inner workings, it is hard for people to make sense of the color they are assigned, or what circumstances might trigger a change in color [4].

2.2. Russia

In Russia's capital, Moscow, a mobile application named "Social Monitoring" was developed to track coronavirus patients' movement. All patients ordered to quarantine at their homes are obliged to install the app. It follows an issued decree stipulating that anyone, including children, displaying symptoms of respiratory disease should, just like those who have tested positive for Covid-19, undergo a two-week self-quarantine period [14]. The app requests all kinds of permissions possible, including access to the user's call records, camera, storage, location data, network information, and sensors [25]. The users are also requested to provide selfies to prove they are at home, through notifications sent at random times, which, in addition to the implementation of one of the world's largest surveillance camera systems provided with facial recognition technology, are being used by authorities for law enforcement purposes, as well as the tracking of foreign nationals under observation for coronavirus, ensuring that everyone placed under self-quarantine stays off the streets, and the identification of individuals attending rallies and protests [12],[15]. Although not disclosing information on the processing of personal data and the adopted safeguards for its protection, Russia's legal system has dismissed lawsuits alleging that it violates individuals' privacy rights [22].

2.3. France

Although it was one of the hardest-hit countries in overall infections and deaths related to COVID-19[3], which resulted in one of the most rigorous lockdowns in Europe, France adopted one of the least invasive biometric systems to control the easing of restrictions.

Video surveillance systems were equipped with artificial intelligence algorithms in the public transport in Paris, and in outdoor markets and buses in Cannes, to allow the identification of persons wearing masks and their adherence to social distancing measures [3].

However, the objective of these systems is not to perform digital surveillance over the citizens, but to aggregate anonymous statistics on how many people are wearing masks on different regions, in order to better distribute protective gear, such as masks and hand sanitizers, and provide more testing, helping authorities anticipate future outbreaks of COVID-19 [11].

The system works locally, not sending data to any centralized server. It provides authorities with statistics generated every 15 minutes, which can only have access to a dashboard that displays the proportion of people with masks [30].

The company responsible for the system development discloses its confidentiality policy, pointing out the purposes of the data processing and other relevant information on privacy and personal data protection[4].

3. CONCLUSION AND FURTHER WORK

Since the beginning of the COVID-19 pandemic, many digital tools have been suggested to rapidly expand bodily and health surveillance systems under public health guise. In various countries, the development and deployment of such tools have been accompanied by temporary legal frameworks designed to support its adoption until a legislative framework is developed.

However, there are growing concerns that when COVID-19 has passed, data gleaned 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 the collected data.

The data collected so far has shown that, in most countries, it is not clear that sufficient considerations are being given to the safeguards necessary to protect people and their data in the short-term and long-term. The information available on the analyzed systems does not clarify which measures are being considered to guarantee the personal data collected is used only to address the spread of Covid-19 and not for additional law enforcement and national security purposes, and do not provide assurance that risks assessments were adopted.

Also, many countries have collaborated directly with private companies to developed digital solutions according to their requirements, without the supervision of legislative institutions and in the absence of public discussion, not showing how these systems meet even the most basic thresholds of legality, proportionality, accountability, necessity, legitimacy, or safeguarding.

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 [7],[8]. At the same time, the European Data Protection Board (EDPB) published some guidelines on the use of location data, contact tracing tools, and the processing of personal data [9],[10]. These documents provide valuable insights for facial recognition systems as well since they enumerate applicable data protection principles and recommendations for this emergency period.

Despite that, in future works, we intend to compare the identified systems with the governance framework for the adoption of facial recognition technologies proposed by [21]. We will keep an updated record of new available systems and identify further characteristics, such as the existence of privacy policies, information on data controllers, disclosure of purposes on the use of personal data, and the existence of specific legislation authorizing the use of such systems.

[3] https://covid19.who.int/

[4] https://www.datakalab.com/detection-de-masque

ACKNOWLEDGMENTS

This paper is a result of the project "SmartEGOV: Harnessing EGOV for Smart Governance (Foundations, methods, Tools) / NORTE-01-0145-FEDER-000037", supported by Norte Portugal Regional Operational Programme (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (EFDR).

REFERENCES

[1] ABI Research. "Taking Stock of Covid-19: The Short- and Long-Term Ramifications on Technology and End Markets." White Paper, March 17, 2020. https://go.abiresearch.com/lp-taking-stock-of-covid-19.

[2] Baichoo, Sunilduth; Maleika Heenaye-Mamode Khan; Pramod Bissessur; Narainsamy Pavaday; Nazmeen Boodoo-Jahangeer; and Neel R. Purmah. "Legal and Ethical Considerations of Biometric Identity Card: Case for Mauritius." Computer Law & Security Review 34, no. 6 (December 2018): 1333–41. https://doi.org/10.1016/j.clsr.2018.08.010.

[3] BBC. "Coronavirus France: Cameras to Monitor Masks and Social Distancing," May 4, 2020. https://www.bbc.com/news/world-europe-52529981.

[4] Courtney, Chris. "COVID-19 and China's Health Code System." Somatosphere, April 5, 2020. http://somatosphere.net/forumpost/covid-19-china-health-code-system/.

[5] Dargan, Shaveta, and Munish Kumar. "A Comprehensive Survey on the Biometric Recognition Systems Based on Physiological and Behavioral Modalities." Expert Systems with Applications 143 (April 2020): 113114. https://doi.org/10.1016/j.eswa.2019.113114.

[6] Ding, Jeffrey. "Deciphering China's AI Dream." University of Oxford, March 2018. https://www.dx2025.com/wp-content/uploads/2019/11/deciphering-chinas-ai-dream.pdf.

[7] eHealth Network. "Mobile Applications to Support Contact Tracing in the Eu's Fight against COVID-19." eHealth Network, April 15, 2020. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[8] European Commission. "Communication from the Commission Guidance on Apps Supporting the Fight against COVID 19 Pandemic in Relation to Data Protection 2020/C 124 I/01. Official Journal of the European Union. 2020;63:1-9.," April 17, 2020.

[9] European Data Protection Board (EDPB). "Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak." European Data Protection Board (EDPB), April 21, 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

[10] European Data Protection Board (EDPB). "Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak." European Data Protection Board (EDPB), March 19, 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

[11] Gréco, Bertrand, and David Revault d'Allonnes. "EXCLUSIF. Coronavirus : le plan d'Anne Hidalgo pour déconfiner Paris." Le Journal du Dimanche, April 18, 2020. https://www.lejdd.fr/JDD-Paris/exclusif-coronavirus-le-plan-danne-hidalgo-pour-deconfiner-paris-3962789.

[12] Habersetzer, Nicola. "Moscow Silently Expands Surveillance of Citizens." Human Rights Watch, March 25, 2020. https://www.hrw.org/news/2020/03/25/moscow-silently-expands-surveillance-citizens.

[13] Human Rights Watch. "Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights," April 2, 2020. https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight.

[14] Human Rights Watch. "Russia: Intrusive Tracking App Wrongly Fines Muscovites," May 21, 2020. https://www.hrw.org/news/2020/05/21/russia-intrusive-tracking-app-wrongly-fines-muscovites.

[15] Ikeda, Scott. "Moscow's 105,000 Facial Recognition Cameras Here to Stay as Country's Court System Entrenches Video Surveillance." CPO Magazine, March 19, 2020. https://www.cpomagazine.com/data-privacy/moscows-105000-facial-recognition-cameras-here-to-stay-as-countrys-court-system-entrenches-video-surveillance/.

[16] Katiyar, Shivendra; Kullai Reddy Meka; Ferdous A. Barbhuiya; and Sukumar Nandi. "Online Voting System Powered by Biometric Security Using Steganography." In 2011 Second International Conference on Emerging Applications of Information Technology, 288–91. Kolkata, India: IEEE, 2011. https://doi.org/10.1109/EAIT.2011.70.

[17] Khasawneh, Mohammed; Mohammad Malkawi; Omar Al-Jarrah; Laith Barakat; Thaier S. Hayajneh; and Munzer S. Ebaid. "A Biometric-Secure e-Voting System for Election Processes." In 2008 5th International Symposium on Mechatronics and Its Applications, 1–8. Amman: IEEE, 2008. https://doi.org/10.1109/ISMA.2008.4648818.

[18] Kindt, Els J. "The Processing of Biometric Data: A Comparative Legal Analysis with a Focus on the Proportionality Principle and Recommendations for a Legal Framework." Tese de Doutoramento, Katholieke Universiteit Leuven, 2012.

[19] Labati, Ruggero Donida; Angelo Genovese; Enrique Muñoz; Vincenzo Piuri; Fabio Scotti; and Gianluca Sforza. "Biometric Recognition in Automated Border Control: A Survey." ACM Computing Surveys 49, no. 2 (June 30, 2016): 1–39. https://doi.org/10.1145/2933241.

[20] Madianou, Mirca. "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies." Television & New Media 20, no. 6 (September 2019): 581–99. https://doi.org/10.1177/1527476419857682.

[21] Madzou, Lofred, and Sebastien Louradour. "Building a Governance Framework for Facial Recognition." Biometric Technology Today 2020, no. 6 (June 2020): 5–8. https://doi.org/10.1016/S0969-4765(20)30083-7.

[22] Marrow, Alexander. "Russian Court Rules in Favor of Facial Recognition over Privacy Claims." Reuters, March 3, 2020. https://www.reuters.com/article/us-russia-technology-facialrecognition/russian-court-rules-in-favor-of-facial-recognition-over-privacy-claims-idUSKBN20Q29U.

[23] Pan, Xiao-Ben. "Application of Personal-Oriented Digital Technology in Preventing Transmission of COVID-19, China." Irish Journal of Medical Science (1971 -), March 27, 2020. https://doi.org/10.1007/s11845-020-02215-5.

[24] Ring, Tim. "Face ID Firms Battle Covid-19 as Users Shun Fingerprinting." Biometric Technology Today 2020, no. 4 (April 2020): 1–2. https://doi.org/10.1016/S0969-4765(20)30042-4.

[25] RosKomSvoboda. "Эксперты назвали приложение от правительства Москвы шпионской программой." RosKomSvoboda, April 1, 2020. https://roskomsvoboda.org/56900/.

[26] Ross, Arun; and Anil K. Jain. "Biometrics, Overview." In Encyclopedia of Biometrics, edited by Stan Z. Li and Anil K. Jain, 289–94. Boston, MA: Springer US, 2015. https://doi.org/10.1007/978-1-4899-7488-4_182.

[27] Schumacher, Elizabeth. "Coronavirus Antibody Tests and Immunity Certificates Pose Ethical and Scientific Problems." Deutsche Welle, April 14, 2020. https://p.dw.com/p/3atNs.

[28] Sontowski, Simon. "Speed, Timing and Duration: Contested Temporalities, Techno-Political Controversies and the Emergence of the EU's Smart Border." Journal of Ethnic and Migration Studies 44, no. 16 (December 10, 2018): 2730–46. https://doi.org/10.1080/1369183X.2017.1401512.

[29] Van der Ploeg, Irma. "Written on the Body: Biometrics and Identity." ACM SIGCAS Computers and Society 29, no. 1 (1999): 37–44. https://doi.org/10.1145/382042.382051.

[30] Vincent, James. "France Is Using AI to Check Whether People Are Wearing Masks on Public Transport." The Verge, May 7, 2020. https://www.theverge.com/2020/5/7/21250357/france-masks-public-transport-mandatory-ai-surveillance-camera-software.

[31] Wighton, Daniel, and David Chazan. "Germany Will Issue Coronavirus Antibody Certificates to Allow Quarantined to Re-Enter Society." The Telegraph, March 29, 2020. https://www.telegraph.co.uk/news/2020/03/29/germany-will-issue-coronavirus-antibody-certificates-allow-quarantined/.

[32] Willoughby, Angus. "Biometric Surveillance and the Right to Privacy [Commentary]." IEEE Technology and Society Magazine 36, no. 3 (September 2017): 41–45. https://doi.org/10.1109/MTS.2017.2728736.

[33] World Bank. "Identification for Development (ID4D) 2019 Annual Report." Washington, DC, USA: World Bank Group, 2019. http://documents.worldbank.org/curated/en/566431581578116247/Identification-for-Development-ID4D-2019-Annual-Report.