Regulating Facial Recognition Technology under the Indonesian Privacy and Data Protection Frameworks: *The Pacing Problem?*

Adelia Rachmaniar[1], Aris Mustriadi[2], Hasyimi Pradana[3], Aditya Prastian Supriyadi[4]

[1] *Postgraduate , Tilburg University rachmaniaradelia@gmail.com*
[2] *LBH Peradi Malang Raya, arismustriadhi@gmail.com*
[3] *postgraduate, Brawijaya University , hasyimipradana23@gmail.com*
[4] *postgraduate, Brawijaya University , aditpart4@gmail.com*

ABSTRACT

The incentive behind artificial intelligence is to develop computers that can perform complex tasks that could only be performed by humans. One of the embodiments is facial recognition that is utilised in a commercial context to law enforcement. This technology could endanger the fundamental rights of an individual; the right to privacy and the right for personal data protection. The terms privacy and data protection should not be used interchangeably since privacy refers to what extent interferences against an individual can be justified, whereas data protection covers protection against unlawful processing of one's personal data. In Indonesia, the regulatory frameworks on privacy and data protection are still widely fragmented. European Convention on Human Rights (ECHR) and General Data Protection Regulation (GDPR) in the European Union have become prime examples for privacy and data protection frameworks. Therefore, this paper uses a doctrinal methodology to analyse the regulatory gaps in the current Indonesian privacy and data protection frameworks, by taking into account the ECHR and GDPR. It can be concluded that facial recognition highlights the pacing problem in Indonesia data governance. There should be exhaustive lists for limitations against interferences on privacy and newly unified regulation on data protection.

Keywords: *Artificial Intelligence, Facial Recognition Technology, Data Protection.*

1. Introduction

Facial recognition is one of the technology innovations in today's society. The embodiment can be seen from an application such as FaceApp or in public places such as an airport for security purposes. The technology has been deployed all around the world with China leading the advancement with its facial recognition database that can identify a person amongst more than two billion people in a few seconds.[6]

In Indonesia, the newest implementation can be seen from the installation of facial recognition technology in a commercial context. In Indonesia, one of the giant retail stores from China, JD.ID with the affiliation of JD.com recently opened the first unmanned store at a mall in North Jakarta.[7] The store utilizes facial recognition technology for the

[6] Sara M. Smyth, Biometrics, Surveillance and the Law: Societies of Restricted Access, Discipline and Control, Routledge, 2019.
[7] Christina Dewi, 'Taking a sneak peek of JD's first unmanned store in Indonesia', (*Techinasia*, 2018) <https://www.techinasia.com/talk/sneak-peek-jd-unmanned-store-indonesia> accessed 08 October 2020.

purpose of verification, tracking the consumers, and the payment.[8] The Indonesian government has also implemented the technology for various purposes such as to assist the citizens in social aid disbursement, in which facial recognition will serve as a verification system to claim the disbursement in subsidized household gas, staple food assistance and subsidized electricity.[9]

Undeniably, facial recognition may bring many benefits, for instance, law enforcement authorities may use it to identify criminals, hence it may result in deterring crimes. Moreover, based on the abovementioned implementation cases, the technology offers a quick, automatic, and seamless verification experience.[10] However, despite the advantages, there are some concerns due to the massive use of facial recognition technology.

The identification of an individual in facial recognition technology can be done by capturing key features from the central position of a facial image. Then, those features will be extracted while the system avoids superficial features such as expressions or hair.[11] Facial recognition works based on machine-learning algorithms, in which it requires a wide range of data sets to be able to identify a facial image. The technology is said to have two major problems: 1) the possibility of inaccuracy in which the trained algorithms are biased and result in few false positives, and 2) the individual may not have consented to the use of this technology. The latter highlights a deep underlying issue on the right to privacy and data protection.[12]

Undeniably, the current dynamics of information technology development have a high potential to violate the right to privacy and right to personal data protection. This threat is mainly due to the global development of information technology and the cross boundaries nature behind it. Each operating system is also increasingly able to exchange and process various forms of data and information. Current developments also allow the

---

[8] *ibid.*,
[9] Eisya A. Eloksari, 'Government trials facial recognition system to improve social aid disbursement', (*The Jakarta Post, 2020*), <https://www.thejakartapost.com/news/2020/05/22/government-trials-facial-recognition-system-to-improve-social-aid-disbursement.html> accessed 08 October 2020.
[10] Bernard Marr, 'Facial Recognition Technology: Here Are The Important Pros And Cons', (*Forbes*, 2019) <https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/#e52097514d16>accessed 08 October 2020.
[11] John Vacca, *Biometric Technologies and Verification Systems*, Elsevier, 2007, p.13.
[12] Nicholas Fearn, How facial recognition technology threatens basic privacy rights, (*ComputerWeekly.com*, 2019),<https://www.bcl.com/wp-content/uploads/2019/07/Computer-Weekly-How-facial-recognition-technology-threatens-basic-privacy-rights-28.06.2019.pdf> accessed 08 October 2020.

transfer from one form of data to another.[13] This can result in a higher threat of privacy and data protection.

The right to privacy and the right to the protection of personal data are two rights that should be distinguished although both strive to protect similar values; the autonomy and human dignity of individuals, in which they are granted a personal sphere to develop their own personalities and opinions. [14] The right to privacy involves a general prohibition on interferences, by providing certain lists of exceptions that can justify interferences in special circumstances.[15] Samuel Warren and Louis Brandeis were the first to conceptualize the right to privacy as a legal right through their writing in Harvard Law Review in 1890 which titled "The Right to Privacy".[16] This writing itself arose when newspapers began printing pictures of people for the first time In this article, Warren and Brandeis simply define the right to privacy as the right to be let alone. Their definition is based on two aspects: (i) personal honor; and (ii) values such as individual dignity, autonomy, and personal independence.[17]

On one hand, the rationales behind the need to protect personal data is to ensure that personal integrity and privacy will not be infringed due to the processing of personal data. [18] Digitalisation and the amount of information being processed is growing exponentially by the day due to technological development. The constant growth in the amount of information that is being processed and stored by organisations leads to strong data protection regulations being enforced and become top priorities for the government around the world to ensure that those organisations

have real incentives to make sure our data remains protected.[19] To conclude, right to privacy concerns circumstances in which the private life of an individual has been interfered (e.g. surveillance by law enforcement agency), and right to personal data concerns every situation in which personal data of an individual has been processed.[20]

---

[13] Privacy and Human Rights: *An International Survey of Privacy Laws and Practices, Privacy International*, P. 4
[14] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law*, (2018), page 19.
[15] *ibid*., page 19.
[16] Samuel Warren dan Louis Brandeis, The Right to Privacy, dalam Harvard Law Review Vol. IV No. 5, 15 Desember 1890, di http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm, accesed on 07 Nov. 2020.
[17] E. Bloustein, Privacy as An Aspect of Human Dignity: an Answer to Dean Prosser, on New York University Law Review Vol. 39 (1964).
[18] Peter Blume, 'The Citizens' Data Protection' (1998) 1 Journal of Information Law & Technology <https://warwick.ac.uk/fac/soc/law/elj/jilt/1998_1/blume/> accessed 08 October 2020, p.1.
[19] PWC, 'The global footprint of data protection regulations', <https://www.pwc.ch/en/publications/2019/The%20global%20footprint%20of%20data%20protection%20regulations_EN_V3-web.pdf>, page 3, accessed 11 November 2020.
[20] *ibid.,* n(9) page 20.

In Indonesia, there is a mandate for the protection of privacy and personal data under Article 28G (1) 1945 Constitution of the Republic of Indonesia that stipulates the individual's right for the "*protection of self, his family, honor, dignity, the property he owns and has the right to feel secure and to be protected against threats from fear to do or not to do something that is part of basic rights*".[21] However, that provision does not explicitly mention privacy, and in terms of data protection regulations, the regulations are still widely fragmented with data protection matters regulated under the different fields.

On the other hand, there are already 126 countries around the world that have implemented data protection regulations in their jurisdiction.[22] In the European Union (EU), European Convention on Human Rights (ECHR) and General Data Protection Regulation (GDPR) have become prime examples for privacy and data protection frameworks with many other countries having incorporated the concepts into their own regulations. This issue eventually highlights 'the pacing problem' in Indonesian data governance, in which the rapid technological innovations often outpace and challenge the adequacy of laws and regulations.[23]

Therefore, this paper aims to analyse the regulatory gaps in the current Indonesian privacy and data protection frameworks through the use of facial recognition technology. The analysis will take into account the implementation of ECHR and GDPR in the EU area to point out important concepts that should be incorporated in the Indonesian data governance.

2. Research Methods

Therefore, this paper uses a doctrinal methodology which consists of simple research aimed at finding a specific statement of the law, or legal analysis with more complex logic and depth.[24] There will be a brief description on the ECHR and GDPR to highlight the key concepts in the EU privacy and data protection frameworks. Then, the current regulations in the Indonesian privacy and data protection will be analysed and described to highlight the gaps in the Indonesian data governance related to the use of

[21] Article 28G (1) 1945 Constitution of the Republic of Indonesia
[22] Heru Andriyanto, 'Indonesia Expects to Adopt Data Protection Law Sooner' *Jakarta Globe* (2020) <https://jakartaglobe.id/tech/indonesia-expects-to-adopt-data-protection-law-sooner> accessed 08 October 2020.
[23] Adam Thierer, 'The Pacing Problem and The Future of Technology Regulation' (*Mercatus Center*, 2020) <https://www.mercatus.org/bridge/commentary/pacing-problem-and-future-technology-regulation> accessed08 October 2020.
[24] Salim Ibrahim Ali, et.al., 'Legal Research of Doctrinal and Non-Doctrinal' (2017) Volume 4 (1) International Journal of Trend in Research and Development, page 493, accessed 14 October 2020.

facial recognition technology.

3. Results and Discussion

1) Facial Recognition Technology under The European Union Frameworks on Privacy and Data Protection

a. Limitations on the right to privacy according to Article 8 (2) ECHR

The use of facial recognition technology by the government or law enforcement authorities should fall under the scope of the right to privacy due to the nature of infringement behind it. The right to privacy is one of the fundamental rights protected under the ECHR. The incentive behind the establishment of ECHR can be drawn back to the 1940's during the Second World War, to ensure that the governments will not be allowed to dehumanise and abuse people's rights with impunity.[25] The convention was then signed by 47 Member States of the Council of Europe (27 states which are the members of the European Union), and it strives as a legal commitment from the parties to abide by the certain principles to protect the fundamental rights of its citizens.[26]

Article 8 (1) of the ECHR acknowledges the right to privacy by stipulating that "*everyone has the right to respect for his private and family life, his home and his correspondence*".[27] However, in the second paragraph of the Article, there are several exceptions and justifications in which the right to privacy is allowed to be infringed by a public authority due to certain circumstances. Article 8 (2) ECHR stated as follows:

> "*there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*".

Therefore, there are three exhaustive lists to decide whether an interference of right to privacy can be justified: 1) the interference is in accordance with the law, 2) there is a legitimate aim for the interference, 3) the interference is necessary in a democratic society.

---

[25] Amnesty International UK, 'What is the European Convention on Human Rights?', (*Amnesty International UK*, 2018), <https://www.amnesty.org.uk/what-is-the-european-convention-on-human-rights> accessed 03 November 2020.
[26] *ibid.,*
[27] Article 8 (1) ECHR

The first exception, interference is justified to the extent that it is in accordance with the law. In this context, it requires that the interferences should have some legal grounds in the domestic law and should be compatible with the rule of law.[28] The rule of law poses these questions to decide whether any interference can be deemed as legitimate: "1) is the legal provision accessible to the citizens?, 2) is the legal provision sufficiently foreseeable for the citizens to foresee the consequences which a given action may entail?, and lastly 3) does the law provide adequate safeguards against arbitrary interference with the respective substantive rights?".[29]

Accessibility refers to whether "the citizen is able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case"[30]. Domestic law must be sufficiently clear to indicate the scope and manner of exercise given to the public authorities, to provide the citizens with the minimum degree of protection to which they are entitled.[31] The second test requires a degree of foreseeability, in which the law should give the citizen an adequate indication to foresee the circumstances in which and the conditions on which the authorities are entitled to resort to measures affecting their rights under the Convention.[32] Lastly, "in accordance with the law" requires adequate safeguards to guarantee the protection of the right to privacy under Article 8 (1) ECHR. The safeguard may include a responsibility for the State to enact clear statutory provision to ensure adequate regard for Article 8 rights at the national level.[33]

The second exception is that the interference must pursue a legitimate aim. The lists of acceptable grounds of legitimate aim under Article 8 (2) ECHR namely: the interests of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, and the protection of the rights and freedoms of others.[34] Lastly, a State could justify its action of interference under the notion of 'necessary in a democratic society'. The last exception requires the

[28] Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, (*Springer Netherland*, 2013), page 456
[29] Steven Greer, The exceptions to Articles 8 to 11 of the European Convention on Human Rights, (*Council of Europe Publishing*, 1997), <https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf>, page 9, accessed 03 November 2020.
[30] Judgment of 26 April 1979, *Case of The Sunday Times v. The United Kingdom*, *Application no. 6538/74*, paragraph 49.
[31] European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence, <https://www.echr.coe.int/documents/guide_art_8_eng.pdf>, page 10, accessed 03 November 2020.
[32] Judgment of 12 June 2014, *Case of Fernandez Martinez v. Spain*, *Application no. 56030/07*, paragraph 117.
[33] *ibid*., n(22), page 11.
[34] Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', International Data Privacy Law, 2013, Vol. 3, No. 4, <https://academic.oup.com/idpl/article/3/4/222/727206>, page 224, accessed 03 November 2020.

proportionality test, in which it involves balancing the rights of the individual and the interests of the State.[35] It requires that any interference must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim or aims pursued.[36]

The use of facial recognition by the law enforcement agencies has been challenged to the Court in the *Case of R (Bridges) v-Chief Constable of South Wales Police & Ors*, in which the plaintiff filed an appeal against the use of Automated Facial Recognition (AFR) by the police of South Wales, United Kingdom. The Court of Appeal stated that the use of AFR by the law enforcement was not in accordance with the law and incompatible with Article 8 (2) ECHR.[37] Initially, the AFR was used to monitor "wanted persons" in the database. However, the Court of Appeal found that the use of AFR involves two wide discretion: 1) the selection of those on watchlists, especially the "persons where intelligence is required" category, and 2) the locations where AFR may be deployed in which a large number of public will be monitored.[38]

b. Key concepts and takeaways on personal data protection from the GDPR

Adopted in 2016, GDPR is set to replace the Data Protection Directive and requires all the Member States in the European Union to comply with the standard of data protection. It has become a legal framework that requires business to protect the personal data of the EU citizens for transactions that occur within EU member states, and it covers all companies that conduct such personal data processing.[39] GDPR creates a consistency and legal certainty since it provides a uniform set of data protection rules across the EU.[40] There are several core concepts in the GDPR that will be described further.

1) Nature of data (including special categories of data)

In the abovementioned paragraph, it is said that the scope of GDPR is when the processing of data involves personal data of the EU citizens. Facial recognition technology

[35] Ursula Kilkelly, The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights, (*Council of Europe*, Human Rights Handbook) <https://rm.coe.int/168007ff47>, page 31, accessed 03 November 2020.
[36] *ibid*., n(25), page 225.
[37] Judgment of 11 August 2020, *Case of R (Bridges) v-Chief Constable of South Wales Police & Ors,* Case No: C1/2019/2670, paragraph 210.
[38] Judgment of 11 August 2020, *Case of R (Bridges) v-Chief Constable of South Wales Police & Ors,* Case No: C1/2019/2670, paragraph 152.
[39] Andrew Rossow, 'The Birth Of GDPR: What Is It And What You Need To Know', (*Forbes*, 25 May 2018), <https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/?sh=ce23c7755e5b>, accessed 04 November 2020.
[40] *ibid.,* n(8), page 31.

itself may lead to processing of personal data and even special categories of data. GDPR provides an added layer of protection of special categories of data, which is "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".[41] The collected data from facial recognition technology can be used to deduce special categories of data and infer other information to achieve a different purpose listed on Article 9 (1) GDPR.[42] Such processing of personal data is strictly prohibited and only allowed under certain conditions.

2) Data controller and processor

There are clear distinctions in GDPR related to the stakeholders who conduct personal data processing. There are two terms related to this in GDPR: data controller and data processor. Data controller means "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"[43]. Whereas, a data processor means "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".[44]

3) Lawful grounds of personal data processing

Article 6 (1) GDPR stipulates 6 (six) lawful grounds for the processing of personal data which include consent, performance of a contract, compliance with legal obligation, vital interest of the data subject, public interest, and legitimate interest. This list of lawful grounds is exhaustive, and the collecting and processing of personal data shall fulfill at least one of those legal bases.[45] However, in case of facial recognition used to sensitive information under the notion of special categories of data, the collecting and processing of those data will have to apply one of the conditions listed in Article 9 (2) GDPR.

4) Accountability principle

---

[41] Article 9 (1) GDPR.
[42] European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, Adopted on 29 January 2020, paragraph 62-64.
[43] Article 4 (7) GDPR
[44] Article 4 (8) GDPR
[45] Bart Custers and Helena Ursic, 'Worker Privacy in a Digitalized World Under European Law', Comparative Labour Law & Policy Journal, January 2018, <https://ssrn.com/abstract=3179425>, page 333, accessed 05 November 2020.

The principle of accountability is crucial to ensure the enforcement of data protection across the EU. It requires data controllers to implement appropriate and effective measures to put into effect the principles and obligations for effective data protection.[46] Accountability principle is a proactive obligation and should not only come into play after a violation has occurred.[47] The measures include the appointment of Data Protection Officers (DPO), the keeping of records and documentations related to the processing, and the conduct of privacy impact assessment.[48]

The appointment of DPO in the utilisation of facial recognition technology is mandatory due to the activities of the processing which require regular and systematic monitoring of data subjects on a large scale, and/or the activities of the processing on a large scale which include special categories of data.[49] Therefore, there is an obligation of DPO to monitor compliance with GDPR and provide advice in regards to data protection impact assessment pursuant to Article 39 GDPR.

5) Data protection by design and by default

Pursuant to Article 25 (1) GDPR, there is an obligation for data controllers to impose appropriate technical and organisational measures which are designed to integrate the necessary safeguards into the processing to meet the requirements set in GDPR and to protect the rights of data subjects.[50] However, the measures referred to that provision embrace more than the design and operation of software or hardware, but encompass business strategies and other organisational and managerial practices to comply with the data protection standard.[51] It requires data controllers to develop a set of practical, actionable guidelines, which involve assessment of the risks posed by the data processing, and any measures to overcome it.[52] In regards to facial recognition, a thorough assessment of risks and safeguards will be needed before the technology can be implemented.

---

[46] Article 29 Working Party, *Opinion 3/2010 on the Principle of Accountability*, Adopted on 13 July 2010, page 3.
[47] *ibid.,* n(8), page 174
[48] *ibid.,* n(8), page 174
[49] Article 37 (1) GDPR
[50] Article 25 (1) GDPR
[51] Lee A. Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements', Oslo Law Review, Volume 4, No. 2-2017, <https://www.idunn.no/oslo_law_review/2017/02/data_protection_by_design_and_by_default_deciphering_the >, page 115, accessed 05 November 2020.
[52] Lydia F de La Torre, 'What does 'data protection by design and by default' mean under EU Data Protection Law?', (*Medium*, 2019), <https://medium.com/golden-data/what-does-data-protection-by-design-and-by-default-mean-under-eu-data-protection-law-fc40f585c0c5>, accessed 05 November 2020.

2) Facial Recognition Technology under The Indonesian Frameworks on Privacy and Data Protection

a. Derogation to the Right to Privacy under the current regulatory frameworks

It has been stated before that the Constitution has acknowledged the right to privacy as one of the fundamental rights that should be protected. Article 31 and Article 32 Law Number 39 Year 1999 on Human Rights also further emphasise this right by stating that "no one shall be subject to arbitrary interference with his home"[53], and that "no one shall be subject to arbitrary interference with his correspondence, including electronic communications, except upon the order of a court or other legitimate authority according to prevailing legislation".[54]

In regards to what extent any interferences to privacy could be justified is not yet clearly stipulated under the current regulations and laws. For example, the State Intelligence Agency is given the authority to "conduct wiretapping, examine flow of funds, and extract information on targets which are activities that threaten national interests and security; and any acts related to terrorism, separatism, espionage, and sabotage that threaten national safety, security, and sovereignty".[55] However, it is unclear whether the regulation actually provides categories of people who fall under the scope of the "watchlist". Further, it is stipulated that the wiretapping can be conducted for up to 6 (six) months and can be extended when it is necessary for targets who have the indication of conducting those acts listed in Article 31.[56]

Law Number 17 Year 2011 on State Intelligence has been challenged before to the Constitutional Court due to the vague and broadly-defined articles contained in it.[57] The plaintiff claimed that the law provides authorities a chance to classify public information as state intelligence and it evoked fears of surveillance.[58] The Court denied the judicial review and maintained that the law has "appropriately regulated intelligence practices in

[53] Article 31 Law Number 39 Year 1999 on Human Rights
[54] Article 32 Law Number 39 Year 1999 on Human Rights
[55] Article 31 Law Number 17 Year 2011 on State Intelligence
[56] Article 32 (2) Law Number 17 Year 2011 on State Intelligence
[57] Aliansi Jurnalis Independen/Alliance of Independent Journalists (AJI), 'State Intelligence Law Challenged in Court', 26 January 2012, <https://ifex.org/state-intelligence-law-challenged-in-court/>, accessed 05 November 2020.
[58] CitizenLab and Canada Centre for Global Security Studies, Island of Control Island of Resistance: Monitoring the 2013 Indonesian IGF, Number 29, January 20, (2014), <https://citizenlab.ca/briefs/29-igf-indonesia/29-igf-indonesia.pdf>, page 52, accessed 05 November 2020.

Indonesia".[59]

Further, Article 42 (2) Law Number 36 Year 1999 on Telecommunications provides a justification for the telecommunications services operator "to record the information transmitted or received by them for the purposes of criminal prosecution, on the basis of: a) a written request from the Attorney General and/or the Chief of Police of the Republic of Indonesia for certain criminal offenses; and b) the request of an investigator for certain criminal offenses- in accordance with prevailing laws".[60] The Directorate General of Post and Telecommunication which falls under the Ministry of Communication and Information Technology has the authority for licensing, legal compliance, and supervision of operators in regards to surveillance.[61] It should be noted that in regards to oversight, the function of this institution remains unclear.

The unclear limitation on derogation to the right to privacy also resulted in dualism views regarding information disclosure and the protection of privacy. It can be seen in the case of a public information request on the alleged embezzlement in the Indonesian Centre Police. Indonesia Corruption Watch (ICW) is a NGO who requested that the name of all the account holders who allegedly conduct the embezzlement be revealed to the public. However, the request was denied since the information was categorised as protected information under Article 10 (a) Law Number 25 Year 2003 on The Amendment to Law Number 15 Year 2002 on Money Laundering Crime *jo.* Article 17 Law Number 14 Year 2008 on Transparency in Public Information. This refusal resulted in a Central Information commission hearing and an order for the National Police to disclose the data submitted by ICW.[62] However, the National Police remained to refuse the disclosure and eventually being sued to the State Administrative Courts.[63]

Due to the development of technology, it is possible for the authorities in Indonesia to deploy facial recognition technology for purposes such as law enforcement. However, the oversight or checks and balances to prevent excessive monitoring and

[59] *ibid.*,
[60] Article 42 (2) Law Number 36 Year 1999 on Telecommunications
[61] Privacy International, 'State of Privacy Indonesia', 26 January 2019, <https://privacyinternational.org/state-privacy/1003/state-privacy-indonesia>, accessed 10 November 2020.
[62] ICW Ajukan Sengketa Rekening Gendut ke KIP, lihat http://nasional.tempo.co/read/news/2010/10/21/063286320/icw-ajukan-sengketa-informasi-rekening-gendutpolisi-ke-kip, accesed on 07 Nov. 2020
[63] Polri Tolak Buka INformasi 17 Rekening Gendut Perwira, Lihat http://www.republika.co.id/berita/breakingnews/hukum/11/02/08/163015-polri-tolak-buka-informasi-17-rekening-gendut-perwira, accesed on 07 Nov. 2020

abuse by the authorities are left unclear and inadequate.[64]

b. Key concepts on the right to personal data protection under the main regulations on data protection

Data protection regulations actually have an important role in responding to technological advances. It will balance the fundamental rights of the data subject, as well as become an incentive for investors to build a safe and trusted business environment, and to accommodate the interests of consumers, who will feel safe in conducting economic transactions.[65] In Indonesia, there are at least currently 30 (thirty) regulations that oversee the processing of personal data in various fields, such as telecommunications, defense and security, law enforcement, health, population, trade, and economy.[66] Therefore, the paper will focus on the main regulations in Indonesian data protection frameworks:

1. Law Number 19 Year 2016 on the Amendment to Law Number 11 Year 2008 on Electronic Information and Transactions ("Law 19/2016").
2. Government Regulation Number 71 Year 2019 regarding Provisions of Electronic Systems and Transactions ("GR 71/2019").
3. Minister of Communications and Informatics Regulation Number 20 Year 2016 concerning the Protection of Personal Data in an Electronic System ("MoCI 20/2016").

1) Consent and other lawful grounds for personal data processing

Article 26 (1) Law 19/2016 requires that "the use of any information through electronic media involving personal data must be done with the consent of that people unless stipulated otherwise by laws and regulations".[67] Further in the second paragraph, it is stipulated that the use of personal data without prior consent of the people concerned can become a legal ground to file a lawsuit.

In addition, Article 14 (4) GR 71/2019 requires that the processing of personal data should be based on the consent of the data subject, as well as fulfill the necessary purposes as follows:

---

[64] *ibid.,* n(49), page 52.
[65] *ibid.,*
[66] Lintang Setianti, Urgensi Regulasi Perlindungan Data Pribadi, (ELSAM, Lembaga Studi dan Advokasi Masyarakat), <https://elsam.or.id/urgensi-regulasi-perlindungan-data-pribadi/> accessed 11 November 2020.
[67] Article 26 (1) Law Number 19 Year 2016 on the Amendment to Law Number 11 Year 2008 on Electronic Information and Transactions

a. fulfillment of contractual obligations in which the data subject is one of the parties, or to fulfill the request of the data subject.
b. fulfillment of legal obligations in accordance with the law.
c. protection of vital interest of the data subject.
d. execution of authority of data controller based on statutory provisions.
e. fulfillment of the performance of a task carried out for the public interest; and
f. fulfillment of legitimate interests of the data controller or data subject.

Therefore, the collecting and processing of personal data for the use of facial recognition technology should be based on a prior consent of the data subjects, as well as the necessary purposes listed in aforementioned provision.

2) Rights of the data subject

Article 26 MoCI 20/2016 recognises five different rights of the data subject as follows:

a. the right to the confidentiality of their personal data.
b. the right to file a complaint to the Minister for the purpose of dispute settlements due to the failure in the protection of the confidentiality of their personal data by the Electronic System Operators.
c. the right to access or rectify their personal data without disrupting the personal data management system.
d. the right to access the history if their personal data have been submitted to the Electronic System Operators as long as it is still in accordance with the applicable regulations; and
e. the right to erasure of their personal data unless specified otherwise in the Indonesian laws and regulations.

Therefore, Electronic System Operators who conduct the processing of personal data for facial recognition technology should ensure that they can provide facilities or access to accommodate these rights of the data subject.

3) Data retention

In regards to data retention, Article 15 MoCI 20/2016 requires that the data should only be stored when the accuracy has been verified and should be kept in the form of encryption. Moreover, in the third paragraph, it is required that the personal data: a)

is stored in accordance with the provision of laws and regulations regulating the obligation of personal data storage period with the respective Supervisory Agency and Sector Supervisory, and b) in case of the absence of such regulations, the shortest period of data retention is 5 (five) years.[68]

The newest established Government Regulation Number 80 Year 2019 on Trading through Electronic Systems ("GR 80/2019") provides a higher level of personal data protection. Article 59 (1) GR 80/2019 stipulates that personal data should be stored in accordance with data protection standards or customary business practices. In the explanation it is stated that data protection standards should refer to the European standard and/or APEC Privacy Frameworks. It can be concluded that the facial images data can be retained for at least 5 (five) years, while taking into account data protection standards or customary business practices.

4) Cross-border transfer of data

Transfer of personal data outside of the jurisdictions of Indonesia is allowed under certain circumstances below:

a. Article 21 (1) GR 71/2019 stipulates that sending and storing of personal data outside the jurisdiction of Indonesia is permitted by ensuring the effectiveness of supervision by the Ministry or Institution and law enforcement.
b. Article 59 (2) GR 80/2019 requires that sending and storing of personal data outside the jurisdiction of Indonesia is permitted if the country or region in which personal data will be transferred or stored is declared by the Minister to have the same standards of protection with Indonesia.
c. Article 22 MoCI 20/2016 stipulates that sending and storing of personal data outside the jurisdiction of Indonesia is permitted in coordination with the Minister or assigned officials/ institutions/authority related to this matter; and by implementing regulatory provisions laws regarding the exchange of personal data across national borders.

In regards to facial recognition technology, there is a possibility that foreign companies will invest or cooperate with the Indonesian government or companies to deploy this

[68] Article 15 (3) Minister of Communications and Informatics Regulation Number 20 Year 2016 concerning the Protection of Personal Data in an Electronic System

technology. Therefore, the three provisions above should be taken into account in case personal data of Indonesian citizens may be sent or stored outside of the jurisdiction of Indonesia.

3. Regulatory gaps in Indonesian data governance based on the comparison with the ECHR and the GDPR

Based on the prior explanation, we can conclude several problems that highlight the regulatory gaps in the current Indonesian privacy and data protection. These gaps become even more prominent when being compared to the ECHR and the GDPR. The explanation will be completed using a table below.

No.	Context	Issues/gaps in the current framework
1.	Privacy	**The absence of limitation to surveillance and oversight** ● Article 8 (2) ECHR provides 3 (three) exhaustive lists to decide whether an interference of right to privacy can be justified: 1) the interference is in accordance with the law, 2) there is a legitimate aim for the interference, 3) the interference is necessary in a democratic society. ● These exhaustive lists cannot be found in the current privacy frameworks in Indonesia. The State Intelligence is given wide authority to interfere privacy with conducting wiretapping, examine flow of funds, and extract information on targets under the purpose of law enforcement and crime prevention. It is unclear whether the framework actually provides categories of people who fall under the scope of the "watchlist". ● The oversight or checks and balances to prevent excessive monitoring and abuse by the authorities are left unclear and inadequate. ● In regards to facial recognition technology, the government will eventually have wide authority to conduct surveillance under the purpose of law enforcement. It has proven before that the deployment of this technology may result in bias or inaccuracy. Therefore, with the absence of limitation and oversight, the right to privacy may be jeopardised due to the excessive use of facial recognition technology by the government.

2.	Data protection	**Liability issues for which stakeholders reliable for any breaches in the processing of personal data** ● Unlike GDPR, the current Indonesian data protection framework does not acknowledge the difference between data controller and data processor. The term used in the regulations is Electronic System Operators. ● In case of data breaches, this will lead to liability issues when the data is being processed by two or more Electronic System Operators.
3.	Data protection	**The lack of oversight and supervisory authority** ● There is no requirement to appoint Data Protection Officers for organisations who conduct the processing of personal data. Data Protection Officers will ensure that there is adequate measurement implemented in protecting the rights of the data subject, as well as monitor compliance with the related laws and regulations. ● The current framework does not explicitly establish which institution or authority is responsible for data protection oversight. In case of breaches to the rights of data subject, the redress mechanism is also only provided in Article 26 (2) Law 19/2016.
4.	Data protection	**Lawful grounds for processing of personal data (misinterpretation of GDPR?)** ● Article 6 (1) GDPR provides legal bases for processing of personal data. Therefore, the collecting and processing of personal data shall fulfill at least one of those legal bases. ● The list of necessary purposes in Article 14 (4) GR 71/2019 is the exact like the list of legal bases in Article 6 (1) GDPR. ● However, GDPR only requires that the processing of personal data should fulfill at least one of those legal bases, whereas the list of legal bases in GR 71/2019 are exhaustive. It means that the collecting and processing of personal data should be based on consent as well as to fulfill the necessary purposes as listed. ● It will be difficult for the Electronic System Provider to have all the necessary purposes fulfilled so that the processing of personal data can become lawful. Therefore, it raises the question *whether there is an attempt to copy the provision in the GDPR and it resulted in misinterpretation?.*

6.	Data protection	**Overlapping requirement for cross-border transfer of data and the absence of related institutions for this matter** ● In the abovementioned explanation, we can see that there are three provisions regulating cross-border transfer of data: 1) Article 21 (1) GR 71/2019, 2) Article 59 (2) GR 80/2019, and 3) Article 22 MoCI 20/2016. ● The overlapping between those provisions raises a question whether all the conditions listed in each provision should be fulfilled before transfer of data outside of the jurisdiction of Indonesia can be done. ● Article 59 (2) GR 80/2019 stated that the "sending and storing of personal data outside the jurisdiction of Indonesia is permitted if the country or region in which personal data will be transferred or stored is declared by the Minister to have the same standards of protection with Indonesia". The mechanism of declaration and what standards are used to determine the level of protection are left unclear.

4. Conclusion

It can be concluded based on the prior research that the Indonesian privacy and data protection framework is still widely fragmented and the regulations are scattered in different fields. There are overlaps between the current regulations and it highlights the need for harmonisation and a unified regulation in Indonesian privacy and data protection framework. Moreover, the deployment of facial recognition technology for various purposes also highlights the gaps in the current regulatory framework.

On the perspective of privacy, there is an inadequate limitation to what extent interferences against the right to privacy can be justified. In case facial recognition technology is deployed by the government for law enforcement purposes, the government will have a wide authority since the categorisation of people that can have their facial images compared to the database remains unclear. The oversight or checks and balances to prevent excessive monitoring and abuse by the authorities are inadequate.

In regards to data protection, there are several regulatory gaps identified in the current framework: 1) liability issues for which stakeholders reliable for any breaches in the processing of personal data, 2) the lack of oversight and supervisory authority, 3)

lawful grounds for processing of personal data (misinterpretation of GDPR?), and lastly 4) overlapping requirements for cross-border transfer of data and the absence of related institutions for this matter. The main data protection frameworks are still in the form of Government Regulations and Ministerial Regulation. It is certainly inadequate with the current dynamics of technology advances. The threat of sanctions which is only in the form of administrative sanctions in the Ministerial Regulation is considered to have less binding power and force for Electronic System Operators.

Therefore, there is an urgency for an independent privacy and data protection regulation that can ensure the fundamental rights of the people regarding the use of facial recognition technology. A new unified privacy and data protection law is hoped to overcome the pacing problem in the current Indonesian privacy and data protection frameworks.

References

European Regulations

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
2. Convention for the Protection of Human Rights and Fundamental Freedoms

Indonesian Regulations

1. 1945 Constitution of the Republic of Indonesia
2. Law Number 36 Year 1999 on Telecommunications
3. Law Number 39 Year 1999 on Human Rights
4. Law Number 25 Year 2003 on The Amendment to Law Number 15 Year 2002 on Money Laundering Crime
5. Law Number 14 Year 2008 on Transparency in Public Information
6. Law Number 17 Year 2011 on State Intelligence
7. Law Number 19 Year 2016 on the Amendment to Law Number 11 Year 2008 on Electronic Information and Transactions

8. Government Regulation Number 71 Year 2019 regarding Provisions of Electronic Systems and Transactions
9. Minister of Communications and Informatics Regulation Number 20 Year 2016 concerning the Protection of Personal Data in an Electronic System

Official Documents

Adam Thierer, 'The Pacing Problem and The Future of Technology Regulation' (MercatusCenter,2020)<https://www.mercatus.org/bridge/commentary/pacing-problem-and-future-technology-regulation> accessed08 October 2020.

Aliansi Jurnalis Independen/Alliance of Independent Journalists (AJI), 'State Intelligence Law Challenged in Court', 26 January 2012, <https://ifex.org/state-intelligence-law-challenged-in-court/>, accessed 05 November 2020.

Amnesty International UK, 'What is the European Convention on Human Rights?', (Amnesty International UK, 2018), <https://www.amnesty.org.uk/what-is-the-european-convention-on-human-rights> accessed 03 November 2020.

Andrew Rossow, 'The Birth Of GDPR: What Is It And What You Need To Know', (Forbes, 25,May,2018),https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to know/?sh=ce23c7755e5b , accessed 04 November 2020.

CitizenLab and Canada Centre for Global Security Studies, Island of Control Island of Resistance: Monitoring the 2013 Indonesian IGF, Number 29, January 20, (2014),<https://citizenlab.ca/briefs/29-igf-indonesia/29-igf-indonesia.pdf>, page 52, accessed 05 November 2020.

European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence,<https://www.echr.coe.int/documents/guide_art_8_eng.pdf>, accessed 03 November 2020.

European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, Adopted on 29 January 2020

Nicholas Fearn, How facial recognition technology threatens basic privacy rights,

(ComputerWeekly.com,2019),<https://www.bcl.com/wpcontent/uploads/2019/07/Computer-Weekly-How-facial-recognition-technology-threatens-basic-privacy-rights-28.06.2019.pdf> accessed 08 October 2020.

Privacy International, 'State of Privacy Indonesia', 26 January 2019, <https://privacyinternational.org/state-privacy/1003/state-privacy-indonesia>, accessed 10 November 2020.

PWC, 'The global footprint of data protection regulations', <https://www.pwc.ch/en/publications/2019/The%20global%20footprint%20of%20data%20protection%20regulations_EN_V3-web.pdf>, page 3, accessed 11 November 2020.

Steven Greer, The exceptions to Articles 8 to 11 of the European Convention on Human Rights, (Council of Europe Publishing, 1997), <https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf>, page 9, accessed 03 November 2020.

Ursula Kilkelly, The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights, (Council of Europe, Human Rights Handbook) <https://rm.coe.int/168007ff47>, page 31, accessed 03 November 2020.

Books

Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, (Springer Netherland, 2013),

European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, (2018),

Privacy and Human Rights: An International Survey of Privacy Laws and Practices, Privacy International

John Vacca, Biometric Technologies and Verification Systems, Elsevier, 2007,

Sara M. Smyth, Biometrics, Surveillance and the Law: Societies of Restricted Access, Discipline and Control, Routledge, 2019.

Journal Articles

Bart Custers and Helena Ursic, 'Worker Privacy in a Digitalized World Under European Law', Comparative Labour Law & Policy Journal, January 2018, <https://ssrn.com/abstract=3179425>, page 333, accessed 05 November 2020.

Bernard Marr, 'Facial Recognition Technology: Here Are The Important Pros And Cons', (Forbes,2019)https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and cons/#e52097514d16 accessed 08 October 2020.

E. Bloustein, Privacy as An Aspect of Human Dignity: an Answer to Dean Prosser, on New York University Law Review Vol. 39 (1964).

Samuel Warren dan Louis Brandeis, The Right to Privacy, dalam Harvard Law Review Vol. IV No. 5, 15 Desember 1890, di http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm, accesed on 07 Nov. 2020.

Lee A. Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements', Oslo Law Review, Volume 4, No. 2-2017, <https://www.idunn.no/oslo_law_review/2017/02/data_protection_by_design_and_by_default_deciphering_the_>, page 115, accessed 05 November 2020.

Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', International Data Privacy Law, 2013, Vol. 3, No. 4, <https://academic.oup.com/idpl/article/3/4/222/727206>, page 224, accessed 03 November 2020.

Peter Blume, 'The Citizens' Data Protection' (1998) 1 Journal of Information Law & Technology <https://warwick.ac.uk/fac/soc/law/elj/jilt/1998_1/blume/> accessed 08 October 2020

Salim Ibrahim Ali, et.al., 'Legal Research of Doctrinal and Non-Doctrinal' (2017) Volume 4 (1) International Journal of Trend in Research and Development, page 493, accessed 14 October 2020.

Websites

Christina Dewi, 'Taking a sneak peek of JD's first unmanned store in Indonesia', (Techinasia, 2018)<https://www.techinasia.com/talk/sneak-peek-jd-unmanned-store indonesia> accessed 08 October 2020.

Eisya A. Eloksari, 'Government trials facial recognition system to improve social aid disbursement', (The Jakarta Post, 2020),

Heru Andriyanto, 'Indonesia Expects to Adopt Data Protection Law Sooner' Jakarta Globe (2020) <https://jakartaglobe.id/tech/indonesia-expects-to-adopt-data-protection-law-sooner> accessed 08 October 2020.

ICW Ajukan Sengketa Rekening Gendut ke KIP, lihat http://nasional.tempo.co/read/news/2010/10/21/063286320/icw-ajukan-sengketa-informasi-rekening-gendutpolisi-ke-kip, accesed on 07 Nov. 202

Lintang Setianti, Urgensi Regulasi Perlindungan Data Pribadi, (ELSAM, Lembaga Studi dan Advokasi Masyarakat), <https://elsam.or.id/urgensi-regulasi-perlindungan-data-pribadi/> accessed 11 November 2020.

Lydia F de La Torre, 'What does 'data protection by design and by default' mean under EU Data Protection Law?', (Medium, 2019), <https://medium.com/golden-data/what-does-data-protection-by-design-and-by-default-mean-under-eu-data-protection-law-fc40f585c0c5>, accessed 05 November 2020.

Polri Tolak Buka INformasi 17 Rekening Gendut Perwira, Lihat http://www.republika.co.id/berita/breakingnews/hukum/11/02/08/163015-polri-tolak-buka-informasi-17-rekening-gendut-perwira, accesed on 07 Nov. 2020

https://www.thejakartapost.com/news/2020/05/22/government-trials-facial-recognition-system-to-improve-social-aid-disbursement.html>