Facial Recognition Technology: A Multinational Analysis of Regulatory Framework, Ethics, and Legal Implications in Security and Privacy

Abd. Azis DP[1], Andi Annisa Nurlia Mamonto[2], Bachrul Amiq[3], Khairul Mufti Rambe[4], Alfin Reza Syahputra[5]
[1]Universitas Pejuang Republik Indonesia, Makassar, Indonesia
[2]universitas YAPIS Papua, Indonesia
[3]Universitas Negeri Surabaya, Surabaya, Indonesia
[4]STAI Syekh H. Abdul Halim Hasan Al-Ishlahiyah Binjai, Indonesia
[5]Universitas Indonesia, Depok, Indonesia
Email: abd.azisdp@gmail.com

Abstract

The latest technological developments allow for the presence of facial recognition technology. This technology itself is widely used in everyday life, such as for using personal devices or registering. But at the same time, the presence of this technology can cause problems with personal data. This research then aims to see the relationship between facial recognition technology and regulations, ethics, and legal implications in data security and privacy. This research will be carried out using a descriptive qualitative approach. The data used in this research was obtained through the results of relevant previous research and studies. The results of this research then found that the presence of facial recognition technology has significant benefits, but at the same time poses significant challenges. These challenges generally center around data security and privacy issues. Therefore, it is necessary to have guidelines that can regulate the use of facial technology, so that in the future this technology is not misused, and can maintain the security and privacy of society in general.

Keywords: *Facial Recognition Technology, Security, Personal Data.*

A. INTRODUCTION

With the rapid development of facial recognition technology in recent years, the use of this technology has penetrated various aspects of our lives, from securing mobile devices to applications in banking and public services. Facial recognition technology promises convenience and efficiency, allowing users to unlock their devices or access services quickly and easily using just their faces as identification. However, behind this convenience, serious questions arise regarding the security, privacy, and ethics associated with the use of this technology (Brem et al., 2021).

In an increasingly connected global context, facial recognition technology has become the focus of attention in various countries, from both positive and negative perspectives. Some countries have adopted this technology quickly for security and administrative purposes, while others have been more cautious about the possible ethical and privacy implications. Therefore, a deep understanding of the regulatory, ethical, and legal implications associated with the use of facial recognition technology at national and international levels is required (Tao et al., 2022).

The continued development of facial recognition technology also creates new challenges in managing sensitive biometric data. The security of biometric data, such as facial data, is very important to protect individuals from the potential risk of misuse of personal data. Previous research has shown its vulnerability to cyberattacks and hacking that could threaten the security of this biometric data. Therefore, it is important to understand the applicable regulations and explore efforts to improve the security of biometric data in the context of facial recognition (Van Natta et al., 2020).

Apart from that, the ethics of using facial recognition technology is also a major concern. Ethical questions arise regarding unwanted monitoring, unauthorized data collection, and the potential misuse of this technology in mass surveillance. All of this creates ethical dilemmas that policymakers and stakeholders must overcome in developing fair and ethical guidelines for the use of facial recognition technology (Ahmad et al., 2022).

Meanwhile, the legal aspects of using facial recognition technology are also the subject of debate. The legal implications include questions surrounding individuals' rights to the privacy and security of their biometric data, as well as the responsibilities of those who use this technology. In this context, differences between countries in their legal regulations are confusing and require comprehensive analysis to understand their legal impact (Bragias et al., 2021).

By considering the complexities involved in the regulation, ethics, and legal implications of facial recognition technology in different countries, this research aims to provide in-depth insight into the challenges and opportunities associated with this technology. In this way, a strong foundation can be built for the development of better guidelines and policies for the use of facial recognition technology that respects privacy rights, ethics, and legal regulations at national and international levels.

B. LITERATURE REVIEW

1. Facial Recognition Technology

Facial recognition is a face-oriented recognition method. This recognition can be divided into two parts, namely recognized or not recognized, after comparing it with patterns previously stored in the database. In general, facial image recognition systems are divided into 2 types, namely feature-based and image-based systems. In the first system, features are used that are extracted from facial image components (eyes, nose, mouth, etc.) and then the relationship between these features is modeled geometrically. Meanwhile, the second system uses raw information from image pixels which is then represented in a certain method, which is then used for image identity classification (Peterson et al., 2023).

This face detection process works by checking the input image, whether it has a face image or not. If it does, it will be separated by cutting the face image from the background of the input image. If the input is in the form of a video, the process carried out is a face-tracking process. In general, the face-tracking process and the face-detection process have the same function. The difference lies in the detection process alone, if the input is in the form of an image, the system runs offline so it can use a

face detection process, whereas, for video input, the system runs online or in real-time which requires direct detection so the process used is the face tracking process (Guo et al., 2021).

In the face detection process, the facial image obtained is still a rough estimate or still has quite poor quality, such as a size that is different from the normal size, less or more lighting factors, poor image clarity, and so on. So it is necessary to carry out a harmonization process. The face alignment process is a process that aims to normalize the face from the facial image obtained from the face detection process (Jayaraman et al., 2020). This process consists of the following stages:

a. Grayscaling
   Image grayscaling is the first stage of the alignment process, at this stage, the RGB color image is converted into a gray image. The RGB color image consists of 3 color parameters, namely red, green, and blue. If this RGB color image is entered into the extraction process, the process will be difficult to carry out because the RGB image consists of 3 parameters. Therefore, it is necessary to equalize parameters, namely by carrying out this grayscaling stage (Ahmed & Nandi, 2021).
b. Cutting
   At this stage, image cutting occurs which separates the face image from the input image, the aim is to take images that are only needed for the extraction process, in this case, the face image, and discard other images that are not needed. The dimensions of the cropped image are adjusted to the dimensions of the facial object segmentation or compartmentalization process carried out in the face detection process (Yamane & Chun, 2020).
c. Resizing (image dimension normalization stage)
   At the image resizing stage, a process of normalizing the dimensions of the facial image occurs, namely the process of enlarging or reducing the dimensions of the facial image to predetermined dimensions. The goal is to equalize the facial dimensions of each image entered, so that in the image extraction process, there will be no differences in the dimensions of the facial image data matrix (Liang et al., 2021).
d. Equalizing (image brightness level correction stage)
   This stage is the final stage of the alignment process, the aim of which is to clarify the histogram values of the facial image resulting from the previous stages (Sadeghi & Raie, 2022).

2. Data Security

In the digital era, communication via computer networks plays an important role. Through electronic communication, someone can carry out transactions or communications very quickly and practically. This is the influence of very significant developments in information technology, where internet bandwidth is getting bigger and access costs are getting cheaper. The consequence is that risks in information security are increasing (Dhar Dwivedi et al., 2021).

Data security is the protection of data in a system against unauthorized authorization, modification, or destruction and the protection of a computer system against unauthorized use or modification. There are four main aspects of data and information security, namely:

a. Privacy/Confidentiality, namely efforts to protect personal information data from people who do not have the right to access it.
b. Integrity, namely efforts to protect data or information from being changed by unauthorized persons.
c. Authentication, namely an effort or method to determine the authenticity of the information, for example, whether the information sent was opened by the correct person or the service from the server provided came from the server in question.
d. Availability relates to the availability of systems and data (information) when needed (Gunduz & Das, 2020).

Data security can be divided into two categories, namely physical security and system security. Physical security is a form of physical security from servers, terminals/client routers to cabling. Meanwhile, system security is security in the operating system or more specifically in the software area, for example by using cryptography and steganography. In this research, we will discuss the use of a combination of steganography and cryptography to provide security for data (Zhang et al., 2023).

The very importance of the value of information means that often desired information can only be accessed by certain people. Information falling into the hands of other parties (for example business counterparties) can cause losses for the owner of the information. For example, a lot of information in a company can only be accessed by certain people within the company, such as information about products that are being developed, and algorithms and techniques used to produce these products. For this reason, the security of the information system must be guaranteed within acceptable limits (Hummel et al., 2021).

Computer networks, such as LANs and the internet, make it possible to provide information quickly. This is one of the reasons companies or organizations are starting to create LANs for their information systems and connect these LANs to the internet. Connecting a LAN or computer to the internet opens up the potential for security holes that could previously be covered with physical security mechanisms. This is following the saying that the ease (comfort) of accessing an information system is inversely proportional to the level of security of the information system itself. The higher the security level, the more difficult (inconvenient) it is to access information (Koripi, 2020).

3. Personal Data

The definition of Personal Data in Article 1 number 27 of the ITE Law Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems (Permen

Kominfo Number 20 of 2016) is certain individual data that is stored, maintained and maintained as true and protected as confidential (Suryono et al., 2021). Meanwhile, Certain Individual Data is "any true and real information that is attached to and can be identified, either directly or indirectly, on each individual whose use is following the provisions of statutory regulations". The owner of personal data is the individual to whom certain individual data is attached. Regarding the definition of sensitive personal data, the Indonesian Government has not provided a specific and specific definition regarding sensitive personal data in the law or technical regulations under the law (Peloquin et al., 2020).

According to the GDPR (General Data Protection Regulation), personal data is any information related to an individual or "data subject" that can be used to identify a person directly or indirectly. The data in question can be names, photos, information, Internet protocol addresses (IP Address), and online identifiers such as a person's physical, physiological, genetic, mental, economic, cultural, or social identity (Lopes et al., 2020).

The regulation of personal data is indirectly regulated in the provisions of Law No. 39 of 1999 concerning Human Rights, as follows:

a. Article 29 paragraph (1) regulates personal protection, family, honor, dignity and property rights;
b. Article 30 regulates protection against threats of fear of doing or not doing something.
c. Article 31 stipulates that no one's residence may be disturbed, stepping on or entering the yard of a residence or entering a house against the will of the person who lives there, is only permitted in cases that have been determined by law.
d. Article 32 regulates that independence and confidentiality in correspondence relations, including correspondence communication relations, including communication relations by electronic means, must not be disturbed, except by order of a judge or other legitimate authority following the provisions of statutory regulations (Zuiderveen Borgesius, 2020).

Thus, the scope of personal rights in Indonesia includes, among others:

a. something that concerns a person's personality, family, personal belongings, and reputation;
b. doing and not doing something;
c. private residence;
d. personal communication (Hope et al., 2022).

Meanwhile, it is hoped that several laws in several sectors will regulate the need to protect a person's rights, such as regulations prohibiting legal interception of communications, as well as obligations for data collectors to protect the confidentiality of the personal data they collect. Article 26 of the Information and Electronic Transactions Law specifically stipulates that a person's data may not be transferred arbitrarily without the consent of the data owner (Sarabdeen, 2022). There are at least 32 laws whose material has content related to regulating citizens' data. The majority

of the 32 laws are related to granting authority to both public (government) and private (private) authorities to collect and manage citizens' data, including the authority to carry out intrusions with several exceptions. The regulated sectors vary, from telecommunications, finance and banking, taxation, population, archives, law enforcement, and security, to the health sector (Kiss et al., 2022).

C. METHOD

This research will be carried out using a descriptive qualitative approach. The data used in this research comes from various research results and previous studies which still have relevance to the content of this research. In analyzing the comparative implementation of facial recognition technology in the public and private sectors, as well as the need for better guidelines and policies, descriptive qualitative methods will be used to understand and describe various related aspects. All discussions in this research focus on developing insight and a better understanding of the impact of facial recognition technology in various contexts, regulations, and ethics, as well as possible solutions to overcome emerging challenges. By combining data from previous research and a comprehensive analysis of current issues in the use of facial recognition technology, this research aims to provide a valuable contribution to supporting the development of better ethics, regulations, and guidelines for the use of this technology in the future (Jaya, 2020).

D. RESULT AND DISCUSSION

1. Comparison of Regulations in Various Countries

Regulatory approaches to facial recognition technology vary across countries. Some countries may have strict regulations with strict requirements for the use of this technology, while others are more permissive. For example, several European countries have adopted strict regulations that protect individual privacy with stricter licensing requirements for the use of facial recognition technology compared to other countries such as Indonesia. Various factors influence the regulatory approach in each country. These include culture, social values, national security needs, and the influence of the technology industry. For example, countries with highly privacy-protective cultures tend to have stricter regulations to protect individual rights.

Different regulations in different countries may influence the development of facial recognition technology. Strict regulations may limit the use of this technology in some cases, while looser regulations may facilitate innovation in the development of facial recognition technology. This can influence the level of technology adoption in the market. A major challenge in regulating facial recognition technology is the harmonization of international regulations. Because this technology is used across borders, differences in regulations between countries can hinder data exchange and collaboration across borders. Efforts to reach an agreement on global guidelines and regulations are a significant challenge.

Additionally, it is important to understand that regulations must continue to adapt to the evolving dynamics of facial recognition technology. As these technologies

continue to develop, regulations must remain relevant and effective in the face of new challenges, such as the development of more sophisticated algorithms or the use of facial recognition technology in different contexts such as autonomous vehicles and digital banking. One approach to overcome regulatory differences is collaboration between countries to develop global standards that can regulate the consistent use of facial recognition technology. This requires strong agreement and cooperation at the international level.

Regulatory implementation can also face technical obstacles such as difficulties in verifying compliance, differences in technological infrastructure in various countries, and limited resources for regulatory enforcement. All of this must be considered in the regulatory comparison process. When looking at regulatory comparisons, it is important to understand that an approach that is effective in one country may not be suitable for another. Therefore, continuous evaluation is needed to ensure regulations remain relevant and effective according to each country's context. Despite differences in regulations, opportunities for collaboration between countries can be used to address shared challenges related to facial recognition technology. This includes sharing experiences and learning from successful approaches in different countries.

A comparison of regulations across countries illustrates the diversity in regulatory approaches to facial recognition technology. Understanding these differences is an important step in developing balanced and effective regulations that can maintain a balance between security, privacy, and innovation in the use of these technologies globally.

2. Ethical Evaluation of the Use of Facial Recognition Technology

Evaluation of the ethics of using facial recognition technology is important in the context of the development and application of this technology in various sectors. First of all, we need to evaluate the ethics of using facial recognition technology in community monitoring. Although this technology can be used to improve security, there is a risk of unwanted surveillance and invasion of individual privacy. It is important to identify clear boundaries in the use of this technology to avoid abuse of power and invasion of privacy.

The collection of facial data is a critical element in the ethical use of facial recognition technology. In this context, it is important to consider permissions for the use of facial data. Do individuals provide explicit consent for the use of their facial data, or is the data collected without their knowledge? Transparency in facial data collection and granting consent is an ethical principle that must be upheld. In the business sector, facial recognition technology is used for various purposes, such as verifying customer identity or transaction security. However, there are ethical questions that need to be answered. How do companies ensure that customer facial data is properly safeguarded? Does the use of this technology violate consumer privacy? This ethical evaluation is important in ensuring that businesses employ fair and ethical practices in the use of facial recognition technology.

The use of facial recognition technology in law enforcement raises several ethical dilemmas. While this technology can help identify criminals, there is a risk of misuse and violation of individual rights. Ethical questions involve the extent to which law enforcement powers are permitted to use this technology, how facial data is stored, and how individuals can be protected from unauthorized use or racial profiling. It is important to recognize that in dealing with various ethical dilemmas, clear ethical guidelines and standards are needed. These guidelines should cover the principles of transparency, privacy protection, fair use of data, and ethical considerations in each context of the use of facial recognition technology. These guidelines and standards can help regulate the ethical use of this technology and maintain a balance between security and privacy.

Lastly, it is important to increase public awareness of the ethical issues associated with facial recognition technology. Ethical education of the public can help individuals understand their rights and the risks associated with this technology. In this way, the public can participate more in policy formation and urge more ethical use of facial recognition technology. Evaluating the ethical use of facial recognition technology is an important step in addressing the complex issues that arise as this technology develops. By considering the various ethical aspects involved, we can create an adequate framework for the fair and safe use of facial recognition technology.

3. Legal Impact on Security and Privacy

In the context of facial recognition technology, privacy rights, and biometric data security are of primary concern. Individual privacy rights must be carefully safeguarded when facial data is used. This includes the right to know how their data is used, to consent or deny the use of facial data, and to request deletion of such data if necessary. Biometric data security is also a key element, as stolen or misused facial data can have serious consequences, such as identity theft or the use of the data for illegal purposes.

The use of facial recognition technology has resulted in various legal cases relating to data privacy and security. These cases include misuse of facial data by companies or third parties, as well as law enforcement-related issues involving identification based on this technology. These cases often raise questions about the extent to which individuals have rights to the privacy and security of their biometric data. When a biometric data security breach occurs, legal responsibility becomes important. Companies or entities that collect and store facial data must be responsible for protecting that data from unauthorized access. Cases of data security breaches can result in significant legal claims, including damages to affected individuals. Therefore, facial data owners must understand and comply with applicable laws in protecting biometric data.

Legal efforts have been made to protect individual rights in the context of the use of facial recognition technology. This includes data privacy laws governing the collection and use of facial data, as well as laws protecting individuals' rights against

unlawful monitoring. These efforts also include the creation of an independent oversight body that monitors breaches of biometric data privacy and security. Then the existence of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) requires that individuals, including those who carry out business or e-commerce activities at home, can be categorized as personal data controllers. So that he is legally responsible for the processing of personal data that he holds and fulfills the provisions in the PDP Law. The legal basis for this Law is Article 5 paragraph (1), Article 20, Article 28G paragraph (1), Article 28H paragraph (4), and Article 28J of the 1945 Constitution of the Republic of Indonesia.

Meanwhile, global laws and efforts to harmonize regulations in various countries are also focused on protecting the privacy and security of biometric data. Because the use of facial recognition technology involves cross-border transactions and international data exchange, consistent and coherent regulation between countries is essential. International efforts to develop guidelines and legal agreements can help create a safer and more private environment in the use of this technology. In cases of privacy and security breaches of biometric data, law enforcement also has a significant role. Companies or individuals who violate the law may face legal consequences, including fines and civil lawsuits. Strict law enforcement is one way to put pressure on entities that ignore data privacy and security.

Courts are often the place to decide controversial cases related to facial recognition technology. The court's decision may influence further legal developments regarding the privacy and security of biometric data. Therefore, the role of the courts in resolving legal disputes in cases of this kind is very important. Public awareness about privacy rights and biometric data security is also important. Legal education that increases understanding of individual rights in the context of facial recognition technology can help individuals protect themselves and support legal protection efforts.

4. Comparison of the Implementation of Facial Recognition Technology in the Public and Private Sectors

The use of facial recognition technology in the public sector has become an increasingly common trend. For example, the use of this technology can be found in government systems that use it for administrative purposes such as identity verification in public services. This can simplify the service process but also raises questions about individual privacy and potential misuse of data. The use of facial recognition technology in national identification systems is a significant debate in many countries. Such systems can enable fast and efficient identification, but they also raise issues related to the security of biometric data and potential privacy violations. Therefore, it is important to develop strict regulations and effective monitoring mechanisms in the implementation of the national identification system.

In the private sector, facial recognition technology is used in a variety of applications, including in business and consumer services. The benefits of using this technology include improved security, efficiency, and customer experience. However,

risks related to data privacy and security also need to be considered. Businesses must ensure that customer biometric data is properly protected and follows applicable regulations. The security of biometric data is of particular concern in the context of the use of facial recognition technology in the private sector. Biometric data breaches can have serious consequences, including identity theft and data misuse. Therefore, companies must take strong security measures to protect their customers' biometric data and comply with applicable regulations.

Over-reliance on facial recognition technology, in both the public and private sectors, creates its challenges. If this technology fails or is misused, there could be significant disruption in public services or business operations. Therefore, it is important to have a backup plan and think critically about reliance on this technology. Transparency and public participation are key in implementing facial recognition technology. Community involvement in the policymaking process and open discussion about the implications of using these technologies can help create more equitable and safer solutions. Transparency also plays a role in building public trust in this technology.

Collaboration between the public and private sectors can be a solution to overcoming several challenges related to the implementation of facial recognition technology. Good cooperation between the two sectors can help develop an adequate framework to protect data security and privacy while leveraging the benefits of this technology. Public education and awareness about privacy rights and the risks associated with facial recognition technology also play an important role. People need to be educated on how their data is used, their rights, and the steps they can take to protect their privacy.

5. The Need for Better Guidelines and Policies

Developing global ethical guidelines for the use of facial recognition technology is an important step in ensuring ethical and responsible use. These guidelines should cover basic principles such as transparency, privacy, and security of biometric data. It can also guide on how this technology should be used in various contexts, including the public and private sectors. In the face of differences in regulatory approaches across countries, it is important to propose recommendations for better regulatory improvements. This includes harmonization of international regulations to address more consistent use of facial recognition technology. These recommendations may also include improvements in protecting individuals' privacy rights and regulating the use of biometric data.

Challenges related to facial recognition technology are a global issue that requires international collaboration. Countries can work together to address privacy, data security, and ethical issues in the use of this technology. This may include exchanging information regarding regulations, security standards, and best practices in the use of facial recognition technology. It is important to increase public awareness about privacy and security rights related to biometric technology. Public education programs can help the public understand the risks and benefits of facial recognition

technology. It can also guide how individuals can protect their privacy and take action if their privacy rights are violated.

Developing a strong oversight and compliance framework is an important part of better policy. This framework must include audit procedures, monitoring the use of facial recognition technology, as well as strict sanctions in the event of violations. This helps ensure that organizations, both in the public and private sectors, comply with applicable regulations and guidelines. Involving various stakeholders, including experts, privacy activists, and civil society representatives in policy development is important. This participation helps ensure that diverse views and interests are considered in designing better guidelines and policies. Encouraging the development of facial recognition technology that is more respectful of privacy is an important step. Technology companies should be incentivized to develop solutions that prioritize the privacy and security of biometric data.

Implementing a code of ethics in the workplace is also a key element. Organizations must ensure that their employees understand and comply with ethical principles in the use of facial recognition technology in their business activities. Finally, openness and transparency in the use of facial recognition technology is an important principle. Organizations and entities must provide clear information about how this technology is used, what data is collected, and how the data is safeguarded. In responding to the challenges that arise with developments in facial recognition technology, better guidelines and policies are a critical foundation. This helps create an adequate framework for the use of this technology that is ethical, safe, and respects individual privacy rights.

E. CONCLUSION

The implementation of facial recognition technology is a significant development in the modern world, bringing great benefits in various sectors, such as public services, business, and security. However, the use of this technology also raises several challenges related to privacy, security, and ethics. To face this challenge, the need for better guidelines and policies cannot be ignored. Global ethical guidelines for the use of facial recognition technology can provide consistent and universal guidance for the entire world in regulating the use of this technology. Recommendations for improving regulations in various countries are an important step to ensure that regulations adapt quickly to technological developments. International collaboration also needs to be increased to overcome this challenge together. Additionally, public education about privacy and security rights related to biometric technology is integral to efforts to protect individual rights and develop a better understanding of the risks and benefits of this technology. To create a fairer, safer, and more privacy-respecting environment, better guidelines and policies are an important foundation for the responsible and ethical use of facial recognition technology.

REFERENCES

1. Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J., & Al-Fuqaha, A. (2022). Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. *Computer Science Review*, *43*, 100452.
2. Ahmed, H. O., & Nandi, A. K. (2021). Connected components-based colour image representations of vibrations for a two-stage fault diagnosis of roller bearings using convolutional neural networks. *Chinese Journal of Mechanical Engineering*, *34*, 1-21.
3. Bragias, A., Hine, K., & Fleet, R. (2021). 'Only in our best interest, right?'Public perceptions of police use of facial recognition technology. *Police Practice and Research*, *22*(6), 1637-1654.
4. Brem, A., Viardot, E., & Nylund, P. A. (2021). Implications of the coronavirus (COVID-19) outbreak for innovation: Which technologies will improve our lives?. *Technological forecasting and social change*, *163*, 120451.
5. Dhar Dwivedi, A., Singh, R., Kaushik, K., Rao Mukkamala, R., & Alnumay, W. S. (2021). Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions. *Transactions on Emerging Telecommunications Technologies*, e4329.
6. Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, *169*, 107094.
7. Guo, Z., Yang, G., Chen, J., & Sun, X. (2021). Fake face detection via adaptive manipulation traces extraction network. *Computer Vision and Image Understanding*, *204*, 103170.
8. Hope, L., Anakwah, N., Antfolk, J., Brubacher, S. P., Flowe, H., Gabbert, F., ... & Anonymous. (2022). Urgent issues and prospects at the intersection of culture, memory, and witness interviews: Exploring the challenges for research and practice. *Legal and criminological psychology*, *27*(1), 1-31.
9. Hummel, P., Braun, M., & Dabrock, P. (2021). Own data? Ethical reflections on data ownership. *Philosophy & Technology*, *34*(3), 545-572.
10. Jaya, I. M. L. M. (2020). *Metode Penelitian Kuantitatif dan Kualitatif: Teori, Penerapan, dan Riset Nyata*. Anak Hebat Indonesia.
11. Jayaraman, U., Gupta, P., Gupta, S., Arora, G., & Tiwari, K. (2020). Recent development in face recognition. *Neurocomputing*, *408*, 231-245.
12. Kiss, B., Sekulova, F., Hörschelmann, K., Salk, C. F., Takahashi, W., & Wamsler, C. (2022). Citizen participation in the governance of nature-based solutions. *Environmental Policy and Governance*, *32*(3), 247-272.
13. Koripi, M. (2020). A review on architectures and needs in advanced wireless-communication technologies. *A Journal Of Composition Theory*, *13*, 208-214.
14. Liang, H., Gao, J., & Qiang, N. (2021). A novel framework based on wavelet transform and principal component for face recognition under varying illumination. *Applied Intelligence*, *51*, 1762-1783.

15. Lopes, I. M., Guarda, T., & Oliveira, P. (2020). General data protection regulation in health clinics. *Journal of Medical Systems*, *44*(2), 53.
16. Peloquin, D., DiMaio, M., Bierer, B., & Barnes, M. (2020). Disruptive and avoidable: GDPR challenges to secondary research uses of data. *European Journal of Human Genetics*, *28*(6), 697-705.
17. Peterson, L. M., Susilo, T., Clifford, C. W., & Palmer, C. J. (2023). Discrimination of facial identity based on simple contrast patterns generated by shading and shadows. *Vision Research*, *212*, 108307.
18. Sadeghi, H., & Raie, A. A. (2022). HistNet: Histogram-based convolutional neural network with Chi-squared deep metric learning for facial expression recognition. *Information Sciences*, *608*, 472-488.
19. Sarabdeen, J. (2022). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, *8*(3).
20. Suryono, R. R., Budi, I., & Purwandari, B. (2021). Detection of fintech P2P lending issues in Indonesia. *Heliyon*, *7*(4).
21. Tao, R., Su, C. W., Naqvi, B., & Rizvi, S. K. A. (2022). Can Fintech development pave the way for a transition towards low-carbon economy: A global perspective. *Technological Forecasting and Social Change*, *174*, 121278.
22. Van Natta, M., Chen, P., Herbek, S., Jain, R., Kastelic, N., Katz, E., ... & Vattikonda, N. (2020). The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic. *Journal of Law and the Biosciences*, *7*(1), lsaa038.
23. Yamane, T., & Chun, P. J. (2020). Crack detection from a concrete surface image based on semantic segmentation using deep learning. *Journal of Advanced Concrete Technology*, *18*(9), 493-504.
24. Zhang, L., Wang, G., You, X., Liu, Z., Ma, L., Tian, J., & Su, M. (2023). Research on the Cyberspace Map and Its Conceptual Model. *ISPRS International Journal of Geo-Information*, *12*(9), 353.
25. Zuiderveen Borgesius, F. J. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The International Journal of Human Rights*, *24*(10), 1572-1593.