The Compliance of Governance on Family Data Protection Regulation

Ni Komang Sutrisni [a*], Putu Angga Pratama Sukma [a], Rahimah Embong [b], Khanlar Haydarov [c]

[a] Faculty of Law, Universitas Mahasaraswati Denpasar, Denpasar, Indonesia
[b] Faculty of Islamic Contemporary Studies, Universiti Sultan Zainal Abidin, Gong Badak, Malaysia.
[c] Department of Public Administration, Baku Engineering University, Baku, Azerbaijan.

* Corresponding Author: komangsutrisnifh@unmas.ac.id

ARTICLE INFO

Article history
Received: June 27, 2024
Revised: October 23, 2024
Accepted: December 4, 2024

Keywords
Data;
Digital;
Family;
Protection;
Regulation.

ABSTRACT

Digital transformation has changed the way family data is managed and stored. The vulnerability of family data has become a serious concern due to the increase in data breach incidents. This research aims to analyze public compliance with family data protection regulations and the ideality of government governance regulations regarding family data protection regulations. This research uses normative legal research methods to analyze the comparison of family data privacy protection regulations between Indonesia and England. This research examines various legal guidelines and policies by applying legislative techniques and a conceptual approach. The legal system theory is used as an analytical framework to evaluate the effectiveness of regulations, law enforcement, and legal culture's influence on public compliance. Data was collected through a literature review of primary and secondary sources, including documents, archives, books, and scientific research findings. The research results show *First*, that family data protection regulations in England are first more standardized with a higher level of public compliance than in Indonesia. *Secondly*, Indonesia still faces challenges such as the weak bargaining position of data subjects, the absence of clear guidelines for data controllers, and the need for an independent oversight authority. This research recommends regulatory improvements, the establishment of competent authorities, and enhanced public education to strengthen Indonesia's personal data protection system, particularly family data.

1. Introduction

Entering the era of sustainable digital technology development, fundamental changes have occurred in how we interact with the world around us.[1] The growth of digital technology, such as the internet, smart devices, and social media platforms, has significantly changed how we access information, communicate, and play an increasingly important role in every individual's life. Digital

[1] Guan Zheng and Jinchun Shu, 'In the Name of Protection—A Critical Analysis of China's Legal Framework of Children's Personal Information Protection in the Digital Era', *Computer Law and Security Review*, 53.October 2022 (2024), 105979 https://doi.org/10.1016/j.clsr.2024.105979

technology has created an ocean of data encompassing our personal information and behavior. Online activities such as internet searches, social media interactions, and online transactions generate digital footprints that can be used to identify, understand, and predict individual behavior patterns.[2] This certainly has a positive impact, as our access to doing something is easier and much faster. Here is the data on individual internet usage from year to year.

Table 1 Data on the increase in Internet Users (Last 10 years)

Year	Number of Individuals Using The Internet Over Time (in Millions)
2015	2,939
2016	3,205
2017	3,568
2018	3,808
2019	4,148
2020	4,534
2021	4,880
2022	5,098
2023	5,250
2024	5,347

Source: Digital 2024: Global Overview Report

From the data above, it is evident that there is an annual increase in internet usage within society. However, besides the positive impacts, one of the critical challenges is related to the sensitivity, privacy, and personal data information that spreads quickly and widely.[3] Privacy is the most fundamental human right. This can be proven in several international regulations, such as the International Covenant on Civil and Political Rights (ICCPR), the Universal Declaration of Human Rights (UDHR), and the European Convention on Human Rights (ECHR). The ECHR explicitly states that everyone has the right to respect their private and family life, home, and correspondence.[4] The correlation between privacy and personal data protection is a legal issue that significantly affects social progress and

[2] Riduan Siagian, Leonard Siahaan, and Muhammad Ichwan Hamzah, 'Human Rights in the Digital Era: Online Privacy, Freedom of Speech, and Personal Data Protection', *Journal of Digital Learning and Distance Education*, 2.1 (2023), 548–58 https://doi.org/https://doi.org/10.56778/jdlde.v2i4.149

[3] Muharman Lubis and Dini Oktarina D. Handayani, 'The Relationship of Personal Data Protection towards Internet Addiction: Cyber Crimes, Pornography and Reduced Physical Activity', *Procedia Computer Science*, 197.2021 (2021), 151–61 https://doi.org/10.1016/j.procs.2021.12.129

[4] Dawen Zhang and others, 'Right to Be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions', *AI and Ethics*, 2024 https://doi.org/10.1007/s43681-024-00573-9

civil rights and generates substantial disputes.[5] Therefore, protecting personal data is one of the current issues faced by information protection agencies worldwide.[6]

Rapidly disseminated data information concerning the privacy rights of every individual and their families, parents, and children is often found in various fields, including the internet.[7] The digital access of society to increasingly sophisticated electronic surveillance technology has changed the dynamics of family relationships, where previously one person was a pair of eyes; now, smartphones with social media access have become the eyes of the world. This mediated monitoring through internet technology has changed the nature of family privacy. This shows that the impact of digital transformation on family life influences the emergence of significant ethical issues related to privacy and personal data protection.[8] In addition, digital transformation has fundamentally changed how family data is managed and stored. The vulnerability of family data has become a serious concern as incidents of data breaches increase. Personal data breaches are a serious issue that can lead to financial losses, identity theft, and even further data misuse.[9] Governments, companies, and individuals must raise awareness about data security and take appropriate preventive measures to protect personal data. Here is the data on countries with the highest data breaches from 2020 to 2024.

Table 2 10 Countries with the Highest Data Leak Rates in 2020-2024

Ranking	Country	Number of Leaked Accounts (in Millions)
1	United States	994,72
2	Russia	338,57
3	India	165,08
4	China	161,37
5	Iran	155,42
6	Brazil	134,67
7	France	100,92
8	Indonesia	94,22
9	England	76,59
10	Philippines	65,13

Source: databoks 2024

[5] Zhilong Guo, Jie Hao, and Lewis Kennedy, 'Protection Path of Personal Data and Privacy in China: Moving from Monism to Dualism in Civil Law and Then in Criminal Law', *Computer Law and Security Review*, 52.December 2023 (2024), 105928 https://doi.org/10.1016/j.clsr.2023.105928

[6] Vera Zinovievaa, Mikhail Shchelokovb, and Evgeny Litvinovsky, 'Legal Issues of Protection of Personal Data: Cases of Transport Data Leaks', *Transportation Research Procedia*, 68 (2023), 461–67 https://doi.org/10.1016/j.trpro.2023.02.062

[7] Debra Laxton, Linda Cooper, and Sarah Younie, 'Translational Research in Action: The Use of Technology to Disseminate Information to Parents during the COVID-19 Pandemic', *British Journal of Educational Technology*, 52.4 (2021), 1538–53 https://doi.org/https://doi.org/10.1111/bjet.13100

[8] Yogesh K. Dwivedi and others, 'Impact of COVID-19 Pandemic on Information Management Research and Practice: Transforming Education, Work and Life', *International Journal of Information Management*, 55.July (2020), 102211 https://doi.org/10.1016/j.ijinfomgt.2020.102211

[9] Jaeung Lee and others, 'Investigating Perceptions about Risk of Data Breaches in Financial Institutions: A Routine Activity-Approach', *Computers and Security*, 121 (2022) https://doi.org/10.1016/j.cose.2022.102832

Based on that data, Indonesia has become one of the countries with the highest data breach rates in the world. Indonesia ranks eighth with a total of 94.22 million accounts. According to data from the Ministry of Communication and Information, from 2019 to May 2024, there were 124 alleged personal data protection violations. Data breaches in Indonesia have previously affected the data of participants in the Social Security Organizing Agency (BPJS) Health, the permanent voter data for the 2024 elections, the data of customers of PT Perusahaan Listrik Negara (Persero), the data of customers of mobile telecommunications service providers, and even the recently leaked taxpayer data. The impact of such data breaches, if the National Identity Number and Family Card Number are revealed, is that information about the data owner's family can be identified for criminal purposes. Furthermore, research conducted by Patterson and Associates shows that in most United Nations member countries, nearly 90% of family units residing at the same address can be uniquely identified using just two easily obtainable data points: postal code and birth date, including the year, of one family member. This shows that family data leaks can threaten the privacy and safety of family members.[10] These risks have created ethical and legal issues, leading to constant innovations in personal information protection regulations.[11]

Family data information, especially regarding children and incapacitated individuals, must be effectively protected.[12] Regarding privacy, children are often considered vulnerable individuals who need protection because they are born in a state of biological dependence on their parents, who cannot survive unless they are cared for. Second, they need more capacity to make appropriate decisions in the early stages of their lives. Nevertheless, their cognitive performance generally develops, and their capacity matures. Indeed, the opportunity to practice decision-making is integral to their successful transition to adulthood. Therefore, protecting data privacy, particularly family data, has become a significant issue that requires serious attention from government institutions and society, with strong regulations and careful oversight to ensure the security and fair use of personal data. The security of personal information becomes crucial in maintaining privacy rights and preventing potential harm from data misuse.[13]

However, the main obstacle is the public's compliance and awareness regarding the importance of protecting their personal data and that of their family members.

---

[10] Wayne Patterson, 'Analysis of Risks to Data Privacy for Family Units in Many Countries', in *Advances in Human Factors in Robots, Unmanned Systems and Cybersecurity* (Springer, Cham, 2021), CCLXVIII, 215–222 https://doi.org/https://doi.org/10.1007/978-3-030-79997-7_27

[11] Shujie Cui and Peng Qi, 'The Legal Construction of Personal Information Protection and Privacy under the Chinese Civil Code', *Computer Law and Security Review*, 41.105560 (2021), 1–17 https://doi.org/https://doi.org/10.1016/j.clsr.2021.105560

[12] Ingrida Milkaite and others, 'Children's Reflections on Privacy and the Protection of Their Personal Data: A Child-Centric Approach to Data Protection Information Formats', *Children and Youth Services Review*, 129.December 2020 (2021), 106170 https://doi.org/10.1016/j.childyouth.2021.106170

[13] Zlatan Morić and others, 'Protection of Personal Data in the Context of E-Commerce', *Journal of Cybersecurity and Privacy*, 4.3 (2024), 731–61 https://doi.org/https://doi.org/10.3390/jcp4030034

The 2020 Indonesian Digital Literacy Status Research by Katadata Insight Center (KIC) revealed that public understanding of the importance of personal data confidentiality still needs to be improved. As many as 67.4% of internet users in Indonesia share their birth dates, 53.7% write down their phone numbers, 29.6% write down their home addresses, and 22.5% include the names of family members and their family relationships or occupations. In addition to that, the existing Indonesian legal framework for personal data protection identifies challenges in providing a comprehensive legal framework. It explores strategies for the government and society to comply with regulations.[14] As a result, awareness of the role of data privacy protection as data subjects, data controllers, and data processors is of utmost importance.[15]

Indonesia's current personal data protection regulation (UU PDP) still has significant areas for improvement in regulating family data protection. The existing rules are general and have yet to accommodate the complexity of data protection in the family context, thereby creating legal gaps that could potentially harm family privacy rights in the digital era. The need for a clear operational definition of family data has become one of the fundamental issues. UU PDP has yet to comprehensively explain the boundaries of data that fall into the category of family data, nor has the mechanisms for its protection. This results in legal uncertainty in protecting sensitive family structure and dynamics information. The absence of comprehensive regulations regarding family data in the PDP Law ultimately creates a legal vacuum that endangers the privacy and security of family information amidst the rapid development of digital technology.

One of the countries with a higher awareness of the importance of data protection laws compared to other countries is England. Unlike Indonesian society, in recent years, users in England have significantly increased their awareness of data privacy and the collection of personal data. The increase in online fraud, data breaches, and online tracking by advertisers causes this development. In addition, about one-third of adults in England say they feel more cautious and aware of the privacy and data protection regulations in England. According to research, around 54% of England public knows the Data Protection Act. This is relatively high compared to other countries, such as Australia at only 23%, Spain at 28%, Japan at 31%, and Italy at 33%.[16] England public responds quicker to regulations, including personal data protection. England has more stringent and comprehensive privacy and data protection rules, particularly concerning family privacy and data

[14] Marune Abraham Ethan Martupa Sahat and Brandon Hartanto, 'Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective', *International Journal of Business, Economics and Social Development*, 2.4 (2021), 143–52 https://doi.org/https://doi.org/10.46336/ijbesd.v2i4.170

[15] Panchapawn Chatsuwan and others, 'Personal Data Protection Compliance Assessment: A Privacy Policy Scoring Approach and Empirical Evidence from Thailand's SMEs', *Heliyon*, 9 (2023), 1–30 https://doi.org/https://doi.org/10.1016/j.heliyon.2023.e20648

[16] Rina Arum Prastyanti and Ridhima Sharma, 'Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India', *Journal of Human Rights, Culture and Legal System*, 4.2 (2024), 354–90 https://doi.org/10.53955/jhcls.v4i2.200

protection. The main legal instruments are the UK Data Protection Act 2018 (DPA) and the EU General Data Protection Regulation 2016/679 (GDPR) concerning the protection of individuals in processing personal data and the free movement of such data.[17]

Protecting personal and family data is also outlined in Article 4 of the GDPR, which also states that efforts to protect personal data must consider its function in society and be balanced with human rights according to the principle of proportionality. Since protecting family data is emphasized, it can be linked to interpersonal relationships that can be used to identify the person, thereby determining their entity. The protection mechanisms in the digital era must protect these entities. The reasons why family privacy should be protected are: first, to respect interpersonal relationships within the family; second, each family has its own rules and culture in educating, nurturing, and raising, so privacy is essential for someone in their daily life and future; third, it is a right that should not be disturbed; fourth, only they have the right to publish personal matters to the public; fifth when there is abuse in processing family personal data, the resulting harm affects all family members.

Previous research by Ingrida Milkaite (2021) indicates that it is necessary to guide and inform the policymaking and practical design of privacy and data policies by families processing family data, particularly children's data.[18] Furthermore, Meng Wang (2017) shows that the current privacy preservation mechanisms in GWAS only focus on case-control studies. Because the data is recorded and organized in family units in this study, an attacker could breach the entire family's privacy, not just one individual. This article focuses on protecting family privacy data for GWAS's transmission disequilibrium test (TDT).[19] Benjamin Phillips' research (2021) shows that in the higher education sector in England, training in collecting large amounts of data must be well-managed to ensure it is processed fairly and transparently, maintaining compliance with good information governance and data protection laws.[20] The research by Clement Labadie and Christine Legner (2022) introduces a resource-based view as a theoretical lens to explain the long journey towards compliance with increasing data protection regulations for companies.[21] Furthermore, research by Julia Helena

---

[17] David Erdos, 'The UK and the EU Personal Data Framework after Brexit: A New Trade and Cooperation Partnership Grounded in Council of Europe Convention 108+?', *Computer Law & Security Review*, 44.105639 (2022), 1–17 https://doi.org/https://doi.org/10.1016/j.clsr.2021.105639

[18] Milkaite and others.

[19] Meng Wang and others, 'Mechanisms to Protect the Privacy of Families When Using the Transmission Disequilibrium Test in Genome-Wide Association Studies', *Bioinformatics*, 33.23 (2017), 3716–3725 https://doi.org/https://doi.org/10.1093/bioinformatics/btx470

[20] Benjamin Phillips, 'UK Further Education Sector Journey to Compliance with the General Data Protection Regulation and the Data Protection Act 2018', *Computer Law and Security Review*, 42 (2021) https://doi.org/10.1016/j.clsr.2021.105586

[21] Clément Labadie and Christine Legner, 'Building Data Management Capabilities to Address Data Protection Regulations: Learnings from EU-GDPR', *Journal of Information Technology*, 38.1 (2022), 6–44 https://doi.org/https://doi.org/10.1177/02683962221141456

Zhang and Others (2024) underscores the need for policymakers to streamline and standardize data protection measures so as not to undermine the GDPR's intent. It highlights the necessity of moving beyond reliance on self-privacy management by better regulating data management architecture and enforcing privacy principles.[22]

Several studies have investigated public compliance with personal data protection regulations and laws. However, there are still gaps. The gap in the current literature is more than merely the absence of research; it is a significant void that needs to be filled. This gap arises from the need for more research on public compliance with family data protection regulations and awareness of personal and family data privacy. After several years of personal data protection regulations being in effect, more research is needed on the urgency of family data privacy and protection in developing these regulations. Therefore, the main focus of this research is not only to fill this gap but also to potentially influence public awareness of their compliance with family data protection regulations and the importance of protecting family data, as well as the ideality of government governance regulations and compliance forms regarding family data protection regulations.

2. Research Method

This research uses normative legal research to compare privacy protection regulations for families in two countries, namely Indonesia and England, to find and recommend directions for regulations regarding family data protection. This research method uses legislative techniques related to the review of all relevant legal guidelines and policies.[23] In addition, this research uses a conceptual approach. This research also uses legal system theory as a tool to discuss and examine issues related to the effectiveness of family data protection regulations, law enforcement regarding personal data protection, and the legal culture of society that influences the level of compliance and public awareness of issues and regulations concerning family data privacy protection. Primary and secondary data are the types of data used. The technique for collecting legal materials involves library studies of documents, archives, books, and proven scientific research results.

3. Results and Discussion

The Compliance Governance in England Family Data Protection Regulations

The legal system adopted by England is common law, which bases the resolution of many cases on previous court considerations.[24] Family data protection in England is a combination of national laws, such as the United

[22] Julia Helena Zhang, Timo Koivumäki, and Dominic Chalmers, 'Privacy vs Convenience: Understanding Intention-Behavior Divergence Post-GDPR', *Computers in Human Behavior*, 160.108382 (2024), 1–9 https://doi.org/https://doi.org/10.1016/j.chb.2024.108382

[23] Prastyanti and Sharma.

[24] Katrina Navickas, 'Legal and Historical Geographies of the Greenham Common Protest Camps in the 1980s', *Journal of Historical Geography*, 82 (2023), 11–22 https://doi.org/10.1016/j.jhg.2023.07.002

Kingdom General Protection Regulation and the Data Protection Act 2018, and is strengthened by court decisions regarding family data protection cases.[25] To see the level of compliance in a legal system in England, it can be analysed based on the effectiveness of the law.[26] Lawrence Friedman explained that the parameters of legal effectiveness are seen based on three factors, namely substance, structure, and legal culture.[27] Compliance is closely related to the internalization of legal culture in society, which is determined by people's knowledge and attitudes toward the legal system, including assessments of legal certainty, justice, and usefulness.[28]

The effectiveness of family data protection regulations in England can be analysed based, *first*, on their legal substance. England government regulates family data protection more comprehensively in the General Protection Regulation and the Data Protection Act 2018. Although not explicitly stated, England provides a more detailed protection framework for data covering individuals within a family. Some of the specific protections implemented by England include an age-appropriate design code (child code), which is a guideline for digital services to process and select children's data; consent to data processing; the right to access and correct personal data within the family; protection of sensitive family data, namely data containing health, mental, or financial diagnoses; restrictions on third-party access; and the application of sanctions for breaches of family data.[29]

England has strict rules regarding explicit consent, particularly regarding children's personal data and sensitive data. The entity processing the data must explicitly grant the government or institution permission. If the data processing involves children under the age of 18, the consent of the child's parents is required.[30] England regulations value consensus highly. Explicit consent is also required if the government or agency is going to access sensitive data, such as

---

[25] Milfrid Tonheim and others, 'Relational and Cultural Continuity for Children in Foster Care; A Critical Explo- Ration of National Policies in Norway, Sweden, Denmark, England, Ireland and Scotland', *Children and Youth Services Review*, 2024, 108040 https://doi.org/10.1016/j.childyouth.2024.108040

[26] Navneet Aujla and others, 'A Comparative Overview of Health and Social Care Policy for Older People in England and Scotland, United Kingdom (UK)', *Health Policy*, 132.April (2023), 104814 https://doi.org/10.1016/j.healthpol.2023.104814

[27] Alberto Febbrajo, *Law, Legal Culture and Society*, *Law, Legal Culture and Society*, 2018 https://doi.org/10.4324/9781351040341

[28] Susan S. Silbey, *Legal Culture and Legal Consciousness*, *International Encyclopedia of the Social & Behavioral Sciences: Second Edition*, Second Edi (Elsevier, 2015), XIII https://doi.org/10.1016/B978-0-08-097086-8.86067-5

[29] Frøydis Lønborg Haarberg, 'What Do We Know about Children's Representation in Child Protection Decisions? A Scoping Review', *Children and Youth Services Review*, 160.March (2024) https://doi.org/10.1016/j.childyouth.2024.107588

[30] Neil Boothby and Lindsay Stark, 'Data Surveillance in Child Protection Systems Development: An Indonesian Case Study', *Child Abuse and Neglect*, 35.12 (2011), 993–1001 https://doi.org/10.1016/j.chiabu.2011.09.004

medical, mental, religious, ethnic, biometric, or financial records. Explicit consent standardisation of family data must be informed and documented so that each family member fully understands the data being processed.[31]

Transparency arrangements and rights of access to family data in England have provided strict legal protection for personal data, including family data, while ensuring transparency and access for individuals to their information.[32] in England, every institution is required to have at least a straightforward standard operating procedure before collecting, storing, and processing personal data. Data transparency standardisation is accommodated with privacy notices and notification standards that require institutions to convey information briefly, clearly, and easily understood and comply with data protection principles, such as minimising data, data accuracy, limited storage, and data security.[33] The principle of data transparency for every institution that collects or manages family data is required to comply with several principles, including: 1) Each institution must clearly explain how it uses, stores, and shares individuals' data through a privacy policy or specific notice. 2) The government of England restricts the use of data, limiting its use to the stated purposes at the time of collection. Any use of data beyond these specified purposes requires additional approval. 3) Individuals have the right to know the type, purpose, duration of data storage, and the subject who accesses the data. 4) The institution must notify the party whose data is affected if a data breach occurs.[34]

The England government has also established special sanctions for violations of family data, such as data leaks. The sanctions applied are administrative and criminal. There are several types of administrative sanctions: a) minor violations, which include not providing adequate privacy notices to individuals, collecting data without a clear legal basis, and not responding to individual data access requests; b) serious violations, which include misuse of data that significantly impacts individuals, failing to report a data breach within 72 hours, and processing data without consent or violating the terms to which the individual agreed. Meanwhile, administrative fines have been regulated in detail, with a

[31] Shuling Yang and Yan Hou, 'Cultivation Strategies of English Thinking Ability in the Environment of Internet of Things Shuling', *HELIYON*, 2024, e39515 https://doi.org/10.1016/j.heliyon.2024.e39515

[32] O.L. van Daalen, 'The Right to Encryption: Privacy as Preventing Unlawful Access', *Computer Law & Security Review*, 49 (2023), 105804 https://doi.org/10.1016/j.clsr.2023.105804

[33] Lyn E. Pleger, Katharina Guirguis, and Alexander Mertes, 'Making Public Concerns Tangible: An Empirical Study of German and UK Citizens' Perception of Data Protection and Data Security', *Computers in Human Behavior*, 122.February 2020 (2021), 106830 https://doi.org/10.1016/j.chb.2021.106830

[34] Bart Custers, 'A Fair Trial in Complex Technology Cases: Why Courts and Judges Need a Basic Understanding of Complex Technologies', *Computer Law & Security Review*, 52 (2024), 105935 https://doi.org/10.1016/j.clsr.2024.105935

maximum fine of 4% of the company's annual global turnover or up to €20 million.[35]

Second, the legal structure is a state apparatus that implements legal protection for the implementation of personal and family data provisions. in England, there is the Information Commissioner's Office (ICO), an independent body with the authority to monitor, examine, and take action against personal data violations.[36] The ICO has a good track record in carrying out its duties including:[37] independence that is directly accountable to England parliament; strong authority in law enforcement; proactive oversight and audit of institutions at risk of data breaches; taking an educational and preventive approach; being very responsive to technology and digitalisation and being an institution with a high level of transparency and accountability.[38] As an institution free from political or commercial influence, the ICO has strong independence and accountability, enabling it to act impartially. The England parliament's direct accountability to the ICO guarantees the monitoring and accounting of all its actions and authorities.

However, despite the ICO's significant advantages as a data protection regulatory body in England, several weaknesses and challenges were found, such as a high workload, limited resources, dependence on reporting, legal complexity, limitations in enforcement, and adaptation to the use of technology. The England government is trying to increase human resources through funding and special training, developing collaborations with technology experts to address new challenges in data protection, and strengthening international cooperation to collaborate more closely with other regulators on cross-border cases more effectively.[39]

Third, legal culture is part of the legal system and includes values, beliefs, attitudes, and patterns of people toward the law. Legal awareness and compliance will create a legal culture of reciprocity between law and society. The plurality of legal cultures in one society and another creates differences in the internalization of values in a legal system. Social legitimacy is important for seeing regulations as

[35] Jonas Montenarh and Simon Marsden, 'Unmasking the Oligarchs – Using Open Source Data to Detect Sanctions Violations', *Journal of Economic Criminology*, 3.February (2024), 100055 https://doi.org/10.1016/j.jeconc.2024.100055

[36] 'UK Strategy Slated by Own Biometrics Commissioner', *Biometric Technology Today*, 2018.7 (2018), 11–11 https://doi.org/10.1016/s0969-4765(18)30096-1

[37] Valentin Rupp and Max von Grafenstein, 'Clarifying "Personal Data" and the Role of Anonymisation in Data Protection Law Including and Excluding Data from the Scope of the GDPR (More Clearly) through Refining the Concept of Data Protection', *Computer Law and Security Review*, 52.1 (2024), 105932 https://doi.org/10.1016/j.clsr.2023.105932

[38] Sonia Livingstone and others, 'The Googlization of the Classroom: Is the UK Effective in Protecting Children's Data and Rights?', *Computers and Education Open*, 7.June (2024), 100195 https://doi.org/10.1016/j.caeo.2024.100195

[39] Livingstone and others.

generally acceptable and guaranteeing social order.[40] Alberto Febbrajo explains that there are models of legal culture, including traditional legal culture, that contribute to the stability of the legal order based on customs; a reactive legal culture that contributes to selecting possible government interventions or public opinion against deviant behaviour; an innovative legal culture that contributes to the compatibility between new legal systems; and a global legal culture that contributes to transnational dialogue on universal values.[41]

England public has a higher level of compliance, a number of institutions have attempted to adapt to existing data protection standards.[42] England has a strong privacy culture and a long history of data protection. As a result, people's understanding of privacy makes them more vigilant and demands transparency from the agencies that process their data. [43] England society possesses an excellent legal culture that responds to regulations, exemplifying a culture of compliance and responsiveness. For example, with rules on personal data, institutions and companies try to respond quickly to adjust to the regulation because the risk of punishment is high. Institutions tend to invest in data compliance infrastructure by appointing data protection officers and adopting more secure technologies.

The Compliance Governance in Indonesia's Family Data Protection Regulations

England and Indonesia regulatory frameworks show fundamental differences due to the systems of governance adopted. England uses a common law system, while Indonesia uses a civil law system.[44] England places the courts in charge of interpreting personal data protection cases, whereas in Indonesia, personal data protection is more dependent on specific laws. The power of law enforcement must be supported by the legal awareness of the community.[45] Legal compliance

[40] G.K. Kaya and others, 'Exploring the Impact of Safety Culture on Incident Reporting: Lessons Learned from Machine Learning Analysis of NHS England Staff Survey and Incident Data', *Safety Science*, 166 (2023), 106260 https://doi.org/10.1016/j.ssci.2023.106260

[41] Vasiliy Boychuk and others, 'An Exploratory Sentiment and Facial Expressions Analysis of Data from Photo-Sharing on Social Media: The Case of Football Violence', *Procedia Computer Science*, 80 (2016), 398–406 https://doi.org/10.1016/j.procs.2016.05.340

[42] Carsten Maple, *Security and Privacy in the Internet of Things*, *Journal of Cyber Policy*, 2017, II https://doi.org/10.1080/23738871.2017.1366536

[43] Ismaeel Alhadidi, Aman Nweiran, and Ghofran Hilal, 'The Influence of Cybercrime and Legal Awareness on the Behavior of University of Jordan Students', *Heliyon*, 10.12 (2024), e32371 https://doi.org/10.1016/j.heliyon.2024.e32371

[44] Priyo Hutomo and Markus Marselinus Soge, 'Perspektif Teori Sistem Hukum Dalam Pembaharuan Pengaturan Sistem Pemasyarakatan Militer', *Legacy: Jurnal Hukum Dan Perundang-Undangan*, 1.1 (2021), 46–68 https://doi.org/10.21274/legacy.2021.1.1.46-68

[45] Aluisius Hery Pratono and Ari Sutanti, 'The Ecosystem of Social Enterprise: Social Culture, Legal Framework, and Policy Review in Indonesia', *Pacific Science Review B: Humanities and Social Sciences*, 2.3 (2016), 106–12 https://doi.org/10.1016/j.psrb.2016.09.020

differs from legal awareness in that it involves a fear of sanctions.[46] Assessing the level of compliance in a legal system can be analysed based on its effectiveness.[47] Lawrence Friedman explains the legal system theory, which states that the parameters of legal effectiveness are based on three factors: substance, structure, and legal culture.[48] Compliance is closely related to the internalization of legal culture in society, which is determined by society's knowledge and attitudes toward the legal system. This includes assessments of certainty, justice, and the benefits of law. [49]

The effectiveness of family data protection regulations in Indonesia can be analysed based on *first*, their legal substance. Data protection regulations in Indonesia are regulated in the Personal Data Protection Act. However, the law does not explicitly mention the nomenclature of family data. One type of specific personal data is child data, where the child is part of the family, but it still needs to be regulated if the data includes aspects of information provided by family members.[50] The misuse of family data for personal gain or commercial gain necessitates the implementation of special regulations.

Indonesia has not yet regulated in detail the consent arrangements for processing family data for more than one family member. Indonesia specifically processes children's data and requires parental consent. General provisions for processing children's data, including: a) It is necessary to obtain parental consent; b) Data should only be used for legitimate purposes and in the child's best interests; c) Service provider institutions must guarantee the security of children's data to prevent any leakage or misuse. In addition, if the data being processed concerns all family members, it is essential that all members know and agree to all forms of data processing. It would be a problem if only one family member agreed to use data while the data involved other family members.

In Indonesia, there are no regulations governing transparency or access rights to family data pertaining to more than one family member. If access rights are only given to the personal data owner, other family members will have difficulty validating whether the managed data has been appropriately used.[51] Indonesian

[46] Miranda Risang Ayu Palar, Laina Rafianti, and Helitha Novianty Muchtar, 'Inclusive Rights to Protect Communal Intellectual Property: Indonesian Perspective on Its New Government Regulation', *Cogent Social Sciences*, 9.2 (2023), 1–19 https://doi.org/10.1080/23311886.2023.2274431

[47] Silbey, XIII.

[48] Febbrajo.

[49] Donna Okthalia Setiabudhi and others, 'The Role of Land Management Paradigm Towards Certainty and Justice', *BESTUUR*, 11.1 (August) (2023), 43 https://doi.org/10.20961/bestuur.v11i1.71710

[50] Hamzah Ismail and others, 'Methods to Prevent Privacy Violations on the Internet on the Personal Level in Indonesia', *Procedia Computer Science*, 216.2022 (2022), 650–54 https://doi.org/10.1016/j.procs.2022.12.180

[51] Sybil Sharpe, *National Security, Personal Privacy and the Law: Surveying Electronic Surveillance and Data Acquisition*, *National Security* (Routledge, 2019) https://doi.org/10.4324/9780429020025

regulations have indeed provided individuals with access to find out, change, update, and delete data, but the implementation is still not harmonious because it depends on the management of each institution Indonesia applies the principle of protecting personal data and family data; transparency can be provided if it meets the requirements, including: a) Fulfilling the data subject's consent, namely, that personal or family data may only be used with the data owner's explicit consent. b) Right of access and information: Data owners have the right to know how their data is used, stored, and shared with third parties. c) Any data collection or processing must have a legitimate purpose and transparently communicate it to the data subject. d) Confidentiality and security, namely transparency, do not mean freely opening data; protection against data leaks remains a priority.[52]

The regulation of sanctions against misuse of family data in Indonesia only applies to personal data in general and does not provide specific sanctions for violations involving family data. The sanctions applied are administrative, criminal, and civil. The administrative fine for personal data violations in Indonesia is a maximum of 2% of annual income against the violation variable.[53] Meanwhile, in England the sanctions applied are administrative and criminal.[54] The regulations regulate administrative fines in detail, with a maximum fine of 4% of the company's annual global turnover or up to €20 million.[55] So, England has more severe violation sanctions in terms of administrative fines compared to Indonesia. The sanctions, which tend to be lower, also affect the level of community compliance. Meanwhile, civil sanctions are applied if personal data is misused, and you can challenge it through a lawsuit for compensation.

Second, the legal structure. Indonesia has established the Personal Data Protection Authority as a supervisory body that specifically controls and handles personal data protection, including family and child data. Indonesia's relatively new personal data regulations provide a gradual enforcement approach that aims to facilitate institutions' adaptation to them. However, several obstacles still exist in the implementation of the regulation, including a suboptimal supervision infrastructure and limited sanctions and enforcement capacity. Additionally, the Directorate General of Population and Civil Registration is responsible for managing family and population data, which includes maintaining data confidentiality in the Indonesian Population Administration Information System.

---

[52] Gunawan A. Tauda, Andy Omara, and Gioia Arnone, 'Cryptocurrency: Highlighting the Approach, Regulations, and Protection in Indonesia and European Union', *BESTUUR*, 11.1 (August) (2023), 1 https://doi.org/10.20961/bestuur.v11i1.67125

[53] Ismail and others.

[54] Hendry Julian Noor, Kardiansyah Afkar, and Henning Glaser, 'Application of Sanctions Against State Administrative Officials in Failure to Implement Administrative Court Decisions', *BESTUUR*, 9.1 (2021), 72 https://doi.org/10.20961/bestuur.v9i1.49686

[55] Montenarh and Marsden.

Third, legal culture. Soerjano Soekoanto explained that four indicators form legal awareness, closely linking compliance to it, there are: [56] legal knowledge is public knowledge regarding behaviour regulated by regulations. Legal understanding refers to the various pieces of information that the public possesses about the substance, purpose, and benefits of the law. Legal attitude is a tendency to accept or reject the law because one recognizes that it is beneficial for community life. Legal behaviour patterns serve as a form of legal compliance, demonstrating the extent to which the law applies and its impact on society.[57] So, the primary function of legal awareness is to achieve legal compliance.

The Personal Data Protection Law is a relatively new regulation in Indonesia, so many institutions are still adjusting to the regulated standards. Because this regulation is still quite new, the level of compliance is still quite low. Public awareness of data privacy in Indonesia is still developing. Frequent cases of data breaches, such as data leaks and the use of data without consent.[58] While England public has a higher level of compliance, a number of institutions have attempted to adapt to existing data protection standards.[59]

The comparison of the level of compliance of England and Indonesian society with family data protection regulations reveals that, generally, England exhibits higher levels of public compliance with these regulations compared to Indonesia. Based on the analysis of regulatory effectiveness, namely based on the factors of substance, structure, and legal culture, England has more rigid and standardised regulatory arrangements than Indonesia. Likewise, in law enforcement efforts and internalising regulations for society, England is superior in various aspects, including the use of more advanced technology. Therefore, it is necessary to increase the optimality related to the implementation of family data protection regulations in Indonesia by making recommendations for policy directions that can be adopted from other countries, including: increasing public awareness of the importance of maintaining family data security through training, socialisation, or public discussions; working with local authorities to educate application access restrictions to avoid data theft; and providing the public with an understanding of data protection policies.

The Governance Compliance on Arrangements Family Data Protection

The Constitution of the Republic of Indonesia contains a clause stating that everyone has the right to protection of themselves, their families, their honor, their

---

[56] Agung Wicaksono, Irni Yunita, and Gede Ginaya, 'Living Side by Side with Nature: Evidence of Self-Governance in Three Local Communities in Indonesia', *Heliyon*, 8.12 (2022), e12248 https://doi.org/10.1016/j.heliyon.2022.e12248

[57] Hanif Qaid and others, 'Speed Choice and Speeding Behavior on Indonesian Highways: Extending the Theory of Planned Behavior', *IATSS Research*, 46.2 (2022), 193–99 https://doi.org/10.1016/j.iatssr.2021.11.013

[58] Alan Tang, *Privacy in Practice*, *Privacy in Practice*, 2022 https://doi.org/10.1201/9781003225089

[59] Maple, II.

dignity, and their property under their control.[60] It has the right to a sense of security and protection from the threat of fear to do or not do something that is a human right.[61] John Locke stated that every individual has fundamental rights that cannot be revoked, including the right to privacy.[62] Personal data protection can be seen as part of this right to privacy. Immanuel Kant also emphasized the importance of human dignity and individual autonomy.[63] Concerning data protection, every individual must have control over their personal information.

In its development history, privacy is a universal concept known in various countries, written in the form of laws and unwritten in the form of morals.[64] Personal Data, which is specific individual data stored, maintained, and kept accurate, and its confidentiality is protected, includes information that can identify a person.[65] Family data is based on information on the personal data of each family member, such as name, date of birth, address, and other personal information.[66] Therefore, family data must be protected by personal data protection regulations.[67] Protection of personal data that includes family data means ensuring that the personal information of each family member is protected from misuse and unauthorized access, including maintaining data confidentiality and ensuring that data is only used for legitimate purposes and by laws and regulations.

The ideality of government governance arrangements and compliance with family data protection regulations can be seen from several indicators, namely in terms of regulations and policies, implementation and law enforcement, security and technology infrastructure, education and public awareness, and transparency

---

[60] Panjun Sun and others, 'A Survey on Privacy and Security Issues in IoT-Based Environments: Technologies, Protection Measures and Future Directions', *Computers & Security*, 148 (2025), 104097 https://doi.org/https://doi.org/10.1016/j.cose.2024.104097

[61] Majid Mollaeefar and Silvio Ranise, 'Identifying and Quantifying Trade-Offs in Multi-Stakeholder Risk Evaluation with Applications to the Data Protection Impact Assessment of the GDPR', *Computers & Security*, 129 (2023), 103206 https://doi.org/https://doi.org/10.1016/j.cose.2023.103206

[62] John Locke, *Two Treatises of Government* (Cambridge university press, 1967).

[63] Immanuel Kant, *Kant: The Metaphysics of Morals* (Cambridge University Press, 2017).

[64] Richard Steppe, 'Online Price Discrimination and Personal Data: A General Data Protection Regulation Perspective', *Computer Law and Security Review*, 33.6 (2017), 768–85 https://doi.org/10.1016/j.clsr.2017.05.008

[65] Hanifan Niffari, 'Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain', *Jurnal Hukum Dan Bisnis (Selisik)*, 6.1 (2020), 1–14 https://doi.org/10.35814/selisik.v6i1.1699

[66] Shuai Guo and Xiang Li, 'Cross-Border Data Flow in China: Shifting from Restriction to Relaxation?', *Computer Law & Security Review*, 56 (2025), 106079 https://doi.org/https://doi.org/10.1016/j.clsr.2024.106079

[67] Piotr Rataj, 'Botnet Defense under EU Data Protection Law', *Computer Law & Security Review*, 56 (2025), 106080 https://doi.org/https://doi.org/10.1016/j.clsr.2024.106080

and accountability.[68] *The first indicator* concerns regulations and policies, where comprehensive regulations are needed. In Indonesia, there is already a law on personal data protection.[69] However, there is still a need for regulatory harmonization to create harmony between the various regulations governing the protection of personal data and family data to avoid legal conflicts and ensure effective implementation.[70] The United Kingdom, which implements GDPR, sets high standards for personal data protection, including the right to access, the right to be forgotten, and the obligation to report data breaches.

Legal instruments for protecting personal data, including family data, are becoming increasingly relevant in the rapidly developing digital economy era. Family data, which includes sensitive information such as names, addresses, and relationships between family members, requires protection that meets three main criteria. *First*, cross-border arrangements are critical for family data because this data can often be processed or stored abroad by global companies.[71] Therefore, rules that ensure that family data is only transferred to countries with equivalent privacy protection, accompanied by special permission, are essential to prevent privacy protection. *Second*, family data protection must include personal rights.[72] States must avoid violations of personal data (negative rights) and are responsible for taking active steps, such as providing secure technological infrastructure, creating solid regulations, and supporting reporting and resolution mechanisms related to family data violations (positive rights). It is essential to consider that family data is often used in various digital services, such as education, banking, or health services, which require the state to be active in ensuring its security.[73] *Third*, adequate protection of personal data can increase public trust in participating in the era of the digital economy.[74] When individuals feel their data is secure, they will be more comfortable using the ever-growing digital services, such as online education applications or family health platforms. It supports digital

[68] Lia Sautunnida, 'Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia', *Kanun Jurnal Ilmu Hukum*, 20.2 (2018), 369–84 https://doi.org/10.24815/kanun.v20i2.11159

[69] Boothby and Stark.

[70] Upik Mutiara and Romi Maulana, 'Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi', *Indonesian Journal of Law and Policy Studies*, 1.1 (2020), 42 https://doi.org/10.31000/ijlp.v1i1.2648

[71] Livingstone and others.

[72] Konrad Kollnig and others, 'Privacy in Chinese IOS Apps and Impact of the Personal Information Protection Law', *Computer Law and Security Review*, 55.February 2020 (2024), 106041 https://doi.org/10.1016/j.clsr.2024.106041

[73] Zhiqiang Xiao and others, 'Privacy Preservation Network with Global-Aware Focal Loss for Interactive Personal Visual Privacy Preservation', *Neurocomputing*, 602 (2024), 128193 https://doi.org/https://doi.org/10.1016/j.neucom.2024.128193

[74] Pierre Dewitte, 'Better Alone than in Bad Company: Addressing the Risks of Companion Chatbots through Data Protection by Design', *Computer Law and Security Review*, 54.July (2024), 106019 https://doi.org/10.1016/j.clsr.2024.106019

transformation and strengthens public trust in the government and service providers. Regulations on the Transfer of Personal Data to other countries or international organizations can be seen in the EU GDPR regulatory model, especially Chapter V, which states that countries receiving personal data transfers must have the same regulatory standards for protecting personal data.[75]

Individuals in the England can control the right to access and correct their data, and organizations must respond to these requests within one month.[76] Then, there is also the right to be forgotten, where the GDPR gives individuals the right to request the deletion of their data in certain circumstances, such as when the data is no longer necessary for the original purpose for which it was collected.[77] Organizations in the England should report data breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.[78] In addition to individual rights and organizational obligations, what can be adopted in Indonesia is to apply data protection principles, including[79]: (1) The principle of transparency states that governments and institutions must inform individuals about the collection and use of their data; (2) The purpose limitation principle is that family data based on personal data may only be collected for legitimate and specific purposes; (3) The principle of data minimization means that only relevant and necessary data should be collected; (4) The principle of accuracy is that data must be updated periodically to ensure accuracy and correctness; (5) The principle of limited storage is that data is stored for a certain period and should not be stored longer than necessary for the initial purpose of collection.

To create comprehensive policies and regulations, various adoptions of regulations need to be carried out based on comparisons of regulations from other countries.[80] The absorption of policies and regulations needs to be initiated and analyzed more deeply to suit Indonesia's socio-cultural climate of personal data protection. The essential things in the England's policies and regulations on personal data protection are fairness and openness, strengthening data subject rights, independent supervisory authority, and the preparation of Data Impact

[75] Rupp and von Grafenstein.
[76] Mollaeefar and Ranise.
[77] Zenghui Yang and others, 'An Attribute-Based Access Control Scheme Using Blockchain Technology for IoT Data Protection', *High-Confidence Computing*, 4.3 (2024), 100199 https://doi.org/https://doi.org/10.1016/j.hcc.2024.100199
[78] Benjamin Phillips, 'UK Further Education Sector Journey to Compliance with the General Data Protection Regulation and the Data Protection Act 2018', *Computer Law & Security Review*, 42.105586 (2021), 1–13 https://doi.org/https://doi.org/10.1016/j.clsr.2021.105586
[79] Cécile de Terwangne, 'Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data', *Computer Law and Security Review*, 40.September 1980 (2021), 3–4 https://doi.org/10.1016/j.clsr.2020.105497
[80] Yu Wang, 'Data Structure and Privacy Protection Analysis in Big Data Environment Based on Blockchain Technology', *International Journal of Intelligent Networks*, 5 (2024), 120–32 https://doi.org/https://doi.org/10.1016/j.ijin.2024.02.005

Assessment (DPIA).[81] In Indonesia, efforts that have been made include the adoption of three principles in Data Free Flow with Trust (DFFT) and Cross Border Data Flows (CBDF), namely lawfulness, fairness, and transparency in the G20 Digital Economy Working Group (DEWG).

The second indicator is the implementation and enforcement of the law.[82] The England has an independent regulatory body to oversee the implementation and enforcement of the law, namely the ICO, responsible for enforcing the GDPR, with the authority to conduct investigations, including audits and inspections of organizations that manage personal data, take enforcement action against organizations that violate data protection regulations including imposing fines, warnings and orders to correct violations, and provide guidance to organizations for GDPR compliance.[83] The England government funds the ICO but operates independently of the government to ensure objectivity and integrity in carrying out its duties.[84]

The ICO is also tasked with public education and awareness. To raise public awareness of their rights regarding personal data and the organization's obligations to protect data, the ICO runs educational campaigns, one of which is "Your Data Matters".[85] The ICO provides various resources, guidance, and training to help organizations understand and comply with data protection regulations.[86] Another task is regarding complaints handling. This supervisory body receives and handles complaints from individuals who feel their rights regarding personal data have been violated, investigates complaints, and takes necessary action to resolve the problem. Consultation and policy recommendations by the ICO to the government and organizations to improve England personal data protection regulations and practices.

---

[81] Nóra Ni Loideain and Rachel Adams, 'From Alexa to Siri and the GDPR: The Gendering of Virtual Personal Assistants and the Role of Data Protection Impact Assessments', *Computer Law and Security Review*, 36 (2020), 1–14 https://doi.org/10.1016/j.clsr.2019.105366

[82] Wayne Wei Wang, 'Contextualizing Personal Information: Privacy's Post-Neoliberal Constitutionalism and Its Heterogeneous Imperfections in China', *Computer Law & Security Review*, 55 (2024), 106030 https://doi.org/https://doi.org/10.1016/j.clsr.2024.106030

[83] Linghong Kuang, Wenlong Shi, and Jing Zhang, 'Hierarchical Privacy Protection Model in Advanced Metering Infrastructure Based on Cloud and Fog Assistance', *Computers, Materials and Continua*, 80.2 (2024), 3193–3219 https://doi.org/https://doi.org/10.32604/cmc.2024.054377

[84] Miranda Mourby and others, 'Are "Pseudonymised" Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK', *Computer Law and Security Review*, 34.2 (2018), 222–33 https://doi.org/10.1016/j.clsr.2018.01.002

[85] Akira Imakura and others, 'Non-Readily Identifiable Data Collaboration Analysis for Multiple Datasets Including Personal Information', *Information Fusion*, 98 (2023), 101826 https://doi.org/https://doi.org/10.1016/j.inffus.2023.101826

[86] Meng Chen, 'Developing China's Approaches to Regulate Cross-Border Data Transfer:Relaxation and Integration', *Computer Law & Security Review*, 54 (2024), 105997 https://doi.org/https://doi.org/10.1016/j.clsr.2024.105997

The implementation of the Independent Watchdog in the England is the ICO taking enforcement action against organizations that violate the GDPR, such as British Airways and Marriott International, where the ICO issued hefty fines.[87] The ICO announced it would fine British Airways £183.39 million (around $230 million) for GDPR breaches due to a cybersecurity incident in September 2018.[88] The incident resulted in the personal data of around 500,000 customers being compromised. Marriott International was fined £99.2 million (around $123 million) for GDPR breaches related to a data breach that affected around 339 million guests. The breach occurred on Marriott's systems acquired by Starwood in 2016, but the breach was not discovered until 2018.[89]

The adoption of implementing and enforcing the law on PDP in Indonesia through an independent body has been encouraged.[90] In October 2024, the PDP Law will come into effect. Before that, two derivative policies must be prepared. There are two derivative policies. First, a presidential regulation (prepress) by Article 58 of the Personal Data Protection Law, and second, a government regulation (PP). In Articles 12-61 of the PDP Law, this derivative PP regulates 1) a system for filing objections to automatic data processing; 2) violations of personal data processing and compensation; 3) the right of recipients of personal data to use it; 4) implementation of personal data processing; 5) evaluation of the impact of personal data protection; 6) notification procedures; and 7) officials or officers responsible for personal data protection tasks. The government is currently working to create two derivative policies.[91] This PDP institution will be an essential instrument and infrastructure for how PDP is carried out.[92] They will create a safe environment for data protection in Indonesia and avoid uncertainty

[87] Jun Ye and others, 'An Electronic Voting Scheme with Privacy Protection', *Procedia Computer Science*, 243 (2024), 1248–56 https://doi.org/https://doi.org/10.1016/j.procs.2024.09.147

[88] 'Marriott Breached Again', *Computer Fraud & Security*, 2020.4 (2020), 3 https://doi.org/https://doi.org/10.1016/S1361-3723(20)30035-X

[89] Katerina Demetzou, Gabriela Zanfir-Fortuna, and Sebastião Barros Vale, 'The Thin Red Line: Refocusing Data Protection Law on ADM, a Global Perspective with Lessons from Case-Law', *Computer Law & Security Review*, 49 (2023), 105806 https://doi.org/https://doi.org/10.1016/j.clsr.2023.105806

[90] Esra Demir, 'The Protection of Human Biodata: Is There Any Role for Data Ownership?', *Computer Law and Security Review*, 51.August 2022 (2023), 105905 https://doi.org/10.1016/j.clsr.2023.105905

[91] Silvia De Conca, 'The Present Looks Nothing like the Jetsons: Deceptive Design in Virtual Assistants and the Protection of the Rights of Users', *Computer Law & Security Review*, 51 (2023), 105866 https://doi.org/https://doi.org/10.1016/j.clsr.2023.105866

[92] Feng Wang, Yongjie Gai, and Haitao Zhang, 'Blockchain User Digital Identity Big Data and Information Security Process Protection Based on Network Trust', *Journal of King Saud University - Computer and Information Sciences*, 36.4 (2024), 102031 https://doi.org/https://doi.org/10.1016/j.jksuci.2024.102031

for electronic service providers.[93] As a result, the establishment of this institution must be reviewed thoroughly. The existence of a PDP institution that is reliable and trusted by the public will have a very positive impact on digital transformation and the development of the digital economy in Indonesia. The PDP institution is crucial when the PDP Bill is discussed in the DPR. Eight of the nine factions in Commission I of the DPR have been reminded that the PDP institution should be designed as an independent institution in carrying out its duties and authorities. Although the PDP institution was formed and is responsible to the President, this institution should be independent of the executive, considering that the PDP Law does not only bind private institutions but also public institutions. The existence of the PDP institution as a data protection authority will be a supervisor in the implementation of the PDP Law.

In PDP law, the institution has considerable and complex authority. Therefore, it must be strong, independent, credible, and have public trust.[94] Unlike other independent institutions whose leaders are usually selected through a fit and proper test in the DPR, the PDP institution is entirely in the executive domain.[95] With these authorities, the PDP institution must be vital from its formation and filled with highly credible people. This institution is vital when dealing with private institutions and the government's own public bodies.

The third indicator is security and technological infrastructure.[96] The Indonesian government has encouraged implementing adequate security measures to protect personal data from unauthorized access.[97] The steps taken based on technological infrastructure are implementing encryption, access control, monitoring and auditing, and security training.[98] Encryption converts data into a

[93] Cayetano Valero and others, 'Analysis of Security and Data Control in Smart Personal Assistants from the User's Perspective', *Future Generation Computer Systems*, 144 (2023), 12–23 https://doi.org/https://doi.org/10.1016/j.future.2023.02.009

[94] Aditya Kaushal Ranjan and Prabhat Kumar, 'APPS: Authentication-Enabled Privacy Protection Scheme for Secure Data Transfer in Internet of Things', *Ad Hoc Networks*, 164 (2024), 103631 https://doi.org/https://doi.org/10.1016/j.adhoc.2024.103631

[95] Eleftherios Chelioudakis, 'Unpacking AI-Enabled Border Management Technologies in Greece: To What Extent Their Development and Deployment Are Transparent and Respect Data Protection Rules?', *Computer Law & Security Review*, 53 (2024), 105967 https://doi.org/https://doi.org/10.1016/j.clsr.2024.105967

[96] Prof. Dr. Paolo Balboni and Kate Elizabeth Francis, 'Data Ethics and Digital Sustainability: Bridging Legal Data Protection Compliance and ESG for a Responsible Data-Driven Future', *Journal of Responsible Technology*, 2024, 100099 https://doi.org/https://doi.org/10.1016/j.jrt.2024.100099

[97] Daeeun Daniel Choi and Paul Benjamin Lowry, 'Balancing the Commitment to the Common Good and the Protection of Personal Privacy: Consumer Adoption of Sustainable, Smart Connected Cars', *Information & Management*, 61.1 (2024), 103876 https://doi.org/https://doi.org/10.1016/j.im.2023.103876

[98] Cristòfol Daudén-Esmel, Jordi Castellà-Roca, and Alexandre Viejo, 'Blockchain-Based Access Control System for Efficient and GDPR-Compliant Personal Data Management', *Computer Communications*, 214 (2024), 67–87 https://doi.org/https://doi.org/10.1016/j.comcom.2023.11.017

format that cannot be read without a decryption key.[99] Encryption protects data during storage and transmission so that even if it is stolen, it cannot be used without the correct key. Encryption that is often used in Indonesia is Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Secure Socket Layer (SSL), and Transport Layer Security (TSL).[100] As in Indonesia, the England also uses an encryption system recommended by the ICO.

Then, access control is carried out by restricting data access only to authorized individuals or systems, including using strong passwords, two-factor authentication, and strict access rights management.[101] Monitoring and auditing to ensure compliance with PDP regulations and to detect and respond to security breaches.[102] They use security monitoring tools to detect real-time suspicious activity on systems, networks, and applications or security breaches.[103] They periodically conduct internal and external compliance audits to assess compliance with PDP policies and regulations. This audit includes an assessment of data management policies, procedures, and practices. Incident reports are needed to conduct cause identification analysis and necessary corrective steps. Personal data security training in Indonesia involves several essential steps: Routine Training Programs, Data Protection Officer (DPO) Certification, and Simulations and Trials.[104]

The approach to personal data security through technology infrastructure has many advantages.[105] The Indonesian government has implemented comprehensive efforts. However, this approach has its drawbacks. Reliance on technology and resources requires significant investments, a challenge for small organizations.[106]

---

[99] Danny S Guamán and others, 'Automated GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Applications', *Computers & Security*, 130 (2023), 103262 https://doi.org/https://doi.org/10.1016/j.cose.2023.103262

[100] Zhangxiang Hu, 'Layered Network Protocols for Secure Communications in the Internet of Things', *University of Oregon: Eugene, OR, USA*, 2021.

[101] Mohsin Ali Farhad, 'Consumer Data Protection Laws and Their Impact on Business Models in the Tech Industry', *Telecommunications Policy*, 48.9 (2024), 102836 https://doi.org/https://doi.org/10.1016/j.telpol.2024.102836

[102] Jose Tomas Llanos, Madeline Carr, and Omer Rana, 'Using the Blockchain to Enable Transparent and Auditable Processing of Personal Data in Cloud- Based Services: Lessons from the Privacy-Aware Cloud Ecosystems (PACE) Project', *Computer Law & Security Review*, 51 (2023), 105873 https://doi.org/https://doi.org/10.1016/j.clsr.2023.105873

[103] Alessandra Calvi, 'Data Protection Impact Assessment under the EU General Data Protection Regulation: A Feminist Reflection', *Computer Law & Security Review*, 53 (2024), 105950 https://doi.org/https://doi.org/10.1016/j.clsr.2024.105950

[104] Núbia Augusto de Sousa Rocha and others, 'Critical Points for the Processing of Personal Data by the Government: An Empirical Study in Brazil', *Computer Law & Security Review*, 54 (2024), 106023 https://doi.org/https://doi.org/10.1016/j.clsr.2024.106023

[105] Andrean Antonius and others, 'Sosialisasi Perbandingan Hukuman Tindak Pidana Pembukaan Rahasia Data Pribadi Negara Indonesia Dan Inggris', *Jurnal Pengabdian West Science*, 3.04 (2024), 383–94 https://doi.org/10.58812/jpws.v3i04.1080

[106] Dewitte.

Data management competencies are uneven across sectors or regions, and human error remains a significant risk even when technology is implemented. In addition, more vigorous law enforcement and time or resource constraints in audits reduce the effectiveness of security measures.

The government needs to incentivize small organizations to adopt security technologies, such as subsidies for encryption software or monitoring tools, to address these gaps.[107] Access to DPO training and certification should also reach underserved areas through government programs or partnerships with educational institutions. Public awareness campaigns are needed to educate the public and workers about the importance of data security practices.[108] Consistent and strict enforcement of violations of the PDP Law should be a priority to encourage compliance.[109] In addition, developing AI-based monitoring tools that are easily accessible to various organizations can strengthen threat detection.[110] International collaboration is also essential to adopt best practices from other countries, such as the England, while independent external audits can objectively assess infrastructure security. With these steps, Indonesia can improve personal data protection effectively and sustainably.

The fourth indicator is education and public awareness.[111] As in the previous discussion in the England through the ICO promoting an education campaign, Indonesia is doing the same thing. Through the Ministry of Communication and Information (*Kominfo*), the government has launched various education campaigns to increase public awareness of the importance of personal data protection. The scope of this campaign is to use social media, seminars, and workshops. In Indonesia, the average social media user spends around 3 hours 11 minutes every day using social media, which is higher than the global average of only 2 hours 31 minutes. This duration of use shows that social media is an integral part of the daily lives of Indonesian people. The most frequently used platform is TikTok, with users spending around 1 hour 32 minutes per day, followed by YouTube,

---

[107] Guan Zheng and Jinchun Shu, 'In the Name of Protection—A Critical Analysis of China's Legal Framework of Children's Personal Information Protection in the Digital Era', *Computer Law and Security Review*, 53.April (2024), 105979 https://doi.org/10.1016/j.clsr.2024.105979

[108] Wenlong Li and Jiahong Chen, 'From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China', *Computer Law & Security Review*, 54 (2024), 105994 https://doi.org/https://doi.org/10.1016/j.clsr.2024.105994

[109] Hugo Pascual and others, 'Hunter: Tracing Anycast Communications to Uncover Cross-Border Personal Data Transfers', *Computers & Security*, 141 (2024), 103823 https://doi.org/https://doi.org/10.1016/j.cose.2024.103823

[110] Tanja Kammersgaard Christensen, 'Pre-Installed Cameras in Vehicles—New Technology from a Data Protection Law Perspective', *Computer Law & Security Review*, 53 (2024), 105980 https://doi.org/https://doi.org/10.1016/j.clsr.2024.105980

[111] Xiongbiao Ye and others, 'Privacy and Personal Data Risk Governance for Generative Artificial Intelligence: A Chinese Perspective', *Telecommunications Policy*, 48.10 (2024), 102851 https://doi.org/https://doi.org/10.1016/j.telpol.2024.102851

which is used for around 1 hour 14 minutes daily.[112] Considering how much time people spend in the digital world, this is an essential foundation for public education and awareness efforts regarding personal data protection.[113] Through this social media platform, the Ministry of Communication and Informatics (*Kominfo*) is holding an educational campaign related to digital literacy, security risk identification, and prevention of phishing attacks to raise awareness of the importance of protecting personal data more optimally.

In addition, through digital literacy, *Kominfo* can provide education on identifying security risks, using strong passwords, managing application permissions, and preventing phishing attacks. *Kominfo* also collaborates with the private sector, namely technology companies and non-governmental organizations, to organize training and seminars on personal data protection. DPO certification is also needed to provide training and certification for related officials to ensure they have the appropriate competencies.

The fifth indicator is transparency and accountability.[114] Regulations in Indonesia require organizations to be transparent in managing personal data, including notifying individuals about how their data is collected, used, and protected. This is one form of adoption of the GDPR, which requires organizations to provide clear and easy-to-understand information to individuals about the processing of their data. This includes detailed privacy policies and individual rights to access and control their data. The legal relationship between the Controller and the Subject is generally based on valid consent, by the provisions of Article 20 Paragraphs (1) and (2) of the PDP Law, which requires the Controller to have a valid basis before processing personal data. Some of the bases for processing personal data regulated in the article include consent from the Subject for a specific purpose that has been previously informed, providing an agreement obligation if the Subject becomes a party or fulfills a request in the agreement, and fulfilling legal obligations by the Controller by applicable laws and regulations. Given the importance of the agreement between the Controller and the Subject in this legal relationship, it is necessary to study the notification obligation related to personal data breaches through three concepts. First, the concept of binding law

[112] Abdillah Abdillah and others, 'Big Data Security & Individual (Psychological) Resilience: A Review of Social Media Risks and Lessons Learned from Indonesia', *Array*, 21 (2024), 100336 https://doi.org/https://doi.org/10.1016/j.array.2024.100336

[113] Paolo Balboni and Kate Francis, 'Chapter 55 - Personal Privacy Policies', in *Computer and Information Security Handbook (Fourth Edition)*, ed. by John R Vacca, Fourth Edition (Morgan Kaufmann, 2025), pp. 907–16 https://doi.org/https://doi.org/10.1016/B978-0-443-13223-0.00055-2

[114] Nadezhda Purtova and Robin L Pierce, 'Citizen Scientists as Data Controllers: Data Protection and Ethics Challenges of Distributed Science', *Computer Law & Security Review*, 52 (2024), 105911 https://doi.org/https://doi.org/10.1016/j.clsr.2023.105911

emphasizes the legal relationship between the Subject and the Controller.[115] Second, contract law focuses on consent as the basis for the legal relationship between the two.[116] Third, the concept of consumer protection views the Controller as a business actor, the Subject as a consumer, and the existence of a standard contract between them.[117] This discussion is essential to provide a deeper understanding of the notification obligation for personal data breaches in the legal relationship between the Subject and the Controller in processing personal data.

In Indonesia, several things need special attention regarding personal data protection. First, it is related to the bargaining position of data subjects.[118] Although the Personal Data Protection (PDP) Law is in place, there are still legal limitations that can strengthen the bargaining position of data subjects, primarily related to the obligation of supervisors to provide clear and transparent notification and the obligation to document personal data breaches.[119] The absence of notification if an interest includes individual rights and freedoms—as implemented in the UK GDPR—indicates that the protection of subject rights still needs to be strengthened to balance subjects and data controllers.[120]

Second, the convenience and facilities for controllers in carrying out their obligations are also still important issues.[121] Currently, needs to be adequate technical guidance can be used as a reference by data controllers in carrying out their obligations, especially regarding notification of personal data breaches.[122] It differs from countries such as the England, which have provided guidelines and best practices for operators, making it easier for them to fulfill these obligations.

---

[115] Federico Costantini and Giada Soncini, 'Chapter 14 - Healthcare Data Governance in the EU: Main Challenges in Personal Data Protection', in *Endorobotics*, ed. by Luigi Manfredi (Academic Press, 2022), pp. 319–36 https://doi.org/https://doi.org/10.1016/B978-0-12-821750-4.00014-1

[116] Yuanxin Li and Darina Saxunová, 'A Perspective on Categorizing Personal and Sensitive Data and the Analysis of Practical Protection Regulations', *Procedia Computer Science*, 170 (2020), 1110–15 https://doi.org/https://doi.org/10.1016/j.procs.2020.03.060

[117] Jiacheng Lin and others, 'BRPPNet: Balanced Privacy Protection Network for Referring Personal Image Privacy Protection', *Expert Systems with Applications*, 233 (2023), 120960 https://doi.org/https://doi.org/10.1016/j.eswa.2023.120960

[118] Christian Pauletto, 'Options towards a Global Standard for the Protection of Individuals with Regard to the Processing of Personal Data', *Computer Law & Security Review*, 40 (2021), 105433 https://doi.org/https://doi.org/10.1016/j.clsr.2020.105433

[119] Nóra Ni Loideain and Rachel Adams, 'From Alexa to Siri and the GDPR: The Gendering of Virtual Personal Assistants and the Role of Data Protection Impact Assessments', *Computer Law & Security Review*, 36 (2020), 105366 https://doi.org/https://doi.org/10.1016/j.clsr.2019.105366

[120] Tuulia Karjalainen, 'The Battle of Power: Enforcing Data Protection Law against Companies Holding Data Power', *Computer Law and Security Review*, 47.August 2018 (2022), 105742 https://doi.org/10.1016/j.clsr.2022.105742

[121] Joanna Studzinska, 'Request for Information as an Auxiliary Measure in Intellectual Property Litigation Concerning Electronic Works and the Protection of Personal Data', *Procedia Computer Science*, 207 (2022), 4276–87 https://doi.org/https://doi.org/10.1016/j.procs.2022.09.491

[122] de Terwangne.

The provision of these guidelines will also be an incentive for controllers to carry out their obligations more effectively.

Third, regarding the authorized institution in personal data protection, Indonesia still needs an independent authority to supervise and enforce the law effectively.[123] Establishing such an authority is necessary to fill the existing legal gap and facilitate administrators' carrying out their obligations in accordance with applicable provisions.[124] This authority is also essential to providing technical guidelines regarding sending personal data breach notifications to the public and authorized parties. However, the political-legal configuration in Indonesia, which still needs to support personal data protection fully, is a significant challenge.[125] One of the problems faced is the need for more public awareness of the importance of personal data security and privacy.[126] Survey results show that many individuals still share personal information carelessly and do not properly maintain their data's security. With the public realizing it, personal data protection can run effectively. Therefore, in addition to policy updates and establishing more robust authorities, education and public awareness of the importance of privacy are also very much needed to strengthen personal data protection in Indonesia. However, even though the PDP Law has been implemented, many improvements still need to be made in various aspects, both in terms of regulation, supervision, convenience for controllers, and increasing public awareness to ensure better personal data protection in Indonesia.

Personal data leaks severely negatively impact a person whose personal data is widely distributed.[127] Privacy disruption and the threat of becoming a victim of cybercrime such as fraud, intrusion, blackmail, or doxing practices, namely spreading and exposing target targets by unauthorized parties.[128] When viewed

---

[123] Dr David Erdos, 'Identification in Personal Data: Authenticating the Meaning and Reach of Another Broad Concept in EU Data Protection Law', *Computer Law & Security Review*, 46 (2022), 105721 https://doi.org/https://doi.org/10.1016/j.clsr.2022.105721

[124] Muharman Lubis and Dini Oktarina D. Handayani, 'The Relationship of Personal Data Protection towards Internet Addiction: Cyber Crimes, Pornography and Reduced Physical Activity', *Procedia Computer Science*, 197.2021 (2021), 151–61 https://doi.org/10.1016/j.procs.2021.12.129

[125] Bart Custers and Gianclaudio Malgieri, 'Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data', *Computer Law & Security Review*, 45 (2022), 105683 https://doi.org/https://doi.org/10.1016/j.clsr.2022.105683

[126] Vera Zinovieva, Mikhail Shchelokov, and Evgeny Litvinovsky, 'Legal Issues of Protection of Personal Data: Cases of Transport Data Leaks', *Transportation Research Procedia*, 68 (2023), 461–67 https://doi.org/https://doi.org/10.1016/j.trpro.2023.02.062

[127] Ingrida Milkaite and others, 'Children's Reflections on Privacy and the Protection of Their Personal Data: A Child-Centric Approach to Data Protection Information Formats', *Children and Youth Services Review*, 129.December 2020 (2021), 106170 https://doi.org/10.1016/j.childyouth.2021.106170

[128] Miliane dos Santos Fantonelli and others, 'Organization and Management of Sensitive Personal Health Data in Electronic Systems in Countries with Implemented Data Protection Laws, Lessons

from a state perspective, data leaks can disrupt state stability because the leak of population data will make it easier for any party globally to carry out computational propaganda operations. Organizations and governments can make one effort through the Provision of Complaint Facilities. Facilities for filing complaints regarding personal data breaches must be available. Organizations are required to respond to these complaints with transparent and responsible resolution mechanisms.

Table 1. Provision of Complaint Facilities in Indonesia

NO.	COMPLAINTS FACILITY	DESCRIPTION	CHALLENGE	ASPIRATION
1.	Ministry of Communication and Information	Kominfo provides an official website, call center, complaint email, and digital application to receive complaints related to personal data breaches.	Complaint responses are still slow in some cases.	Complaints System becomes more responsive with better technology.
2.	Personal Data Protection Agency	An independent authority mandated by the PDP Law to handle complaints, investigate and impose administrative sanctions related to personal data breaches.	The Personal Data Protection Agency is still in the formation stage and is not yet functioning actively.	The Personal Data Protection Agency can function optimally and become a trusted body for personal data protection.
3.	Data Compliance Unit in Organization	Every organization is required to provide an internal complaints mechanism through a data protection officer or unit, such as a DPO.	Not all organizations have the competence and resources to appoint or train a DPO.	All organizations have a clear complaints mechanism with a competent DPO.
4.	General Consumer Complaints Service	The Indonesian Ombudsman and other public complaint institutions as alternative channels for the public to report personal data violations that are not resolved at the organizational level.	Not all people understand the existence or procedures of these institutions for complaints.	Public education about this complaint service can be improved to expand public access.

Protecting personal data, including family data, is an integral part of the right to privacy that must be maintained through ideal regulatory arrangements, strict community law enforcement, strengthening technological infrastructure, and increasing education and awareness.[129] Harmonized regulations, independent solid supervisory bodies, and applying the principles of transparency, synchronization of objectives, and data minimization are the main pillars of

to Brazil: A Brief Systematic Review', *Computer Law and Security Review*, 51 (2023), 105872 https://doi.org/10.1016/j.clsr.2023.105872

[129] Raichuk Isus and others, 'Development of a Model of Personal Data Protection in the Context of Digitalization of the Educational Sphere Using Information Technology Tools', *Procedia Computer Science*, 231 (2024), 347–52 https://doi.org/https://doi.org/10.1016/j.procs.2023.12.215

effective personal data protection governance.[130] In addition, encryption, access control, and regular audits play an essential role in maintaining data security from the threat of breaches.

Recommendations to strengthen governance include harmonizing national regulations with international standards such as GDPR, establishing a credible independent oversight body free from executive subordination, and providing incentives for small organizations to adopt security technologies.[131] Training and certification programs that reach remote areas, massive public awareness campaigns, and international collaboration to adopt best practices should also be included.[132] Finally, increasing transparency and accountability through clear privacy policies and active community engagement will ensure better personal data protection in Indonesia, supporting a safe and sustainable digital transformation.

4. Conclusion

Based on the analysis and discussion, a conclusion is drawn: *First*, the comparison of England regulatory settings for the protection of personal or family data is more rigid and standardised than that of Indonesia. In comparison, the England public's level of compliance with data protection is higher than that of Indonesia. Likewise, the England is superior in various aspects, including the use of more advanced technology, in efforts to enforce the law and internalise regulations for society. *Second*, Personal data protection in Indonesia still faces various challenges, such as the lack of regulations that strengthen the bargaining position of data subjects, the unavailability of clear guidelines for controllers in carrying out their obligations, and the absence of an independent authority to oversee the implementation of personal data protection. In addition, low public awareness of the importance of personal data security is also a significant challenge. Therefore, there needs to be improved regulations, the establishment of competent authorities, and increased public education to ensure more effective personal data protection in Indonesia.

Refrences

Abdillah, Abdillah, Ida Widianingsih, Rd Ahmad Buchari, and Heru Nurasa, 'Big Data Security & Individual (Psychological) Resilience: A Review of Social Media Risks and Lessons Learned from Indonesia', *Array*, 21 (2024), 100336

[130] Massimo Marelli, 'The Law and Practice of International Organizations' Interactions with Personal Data Protection Domestic Regulation: At the Crossroads between the International and Domestic Legal Orders', *Computer Law & Security Review*, 50 (2023), 105849 https://doi.org/https://doi.org/10.1016/j.clsr.2023.105849

[131] Rupp and von Grafenstein.

[132] Panchapawn Chatsuwan and others, 'Personal Data Protection Compliance Assessment: A Privacy Policy Scoring Approach and Empirical Evidence from Thailand's SMEs', *Heliyon*, 9 (2023), 1–30 https://doi.org/https://doi.org/10.1016/j.heliyon.2023.e20648

https://doi.org/https://doi.org/10.1016/j.array.2024.100336

Alhadidi, Ismaeel, Aman Nweiran, and Ghofran Hilal, 'The Influence of Cybercrime and Legal Awareness on the Behavior of University of Jordan Students', *Heliyon*, 10.12 (2024), e32371 https://doi.org/10.1016/j.heliyon.2024.e32371

Antonius, Andrean, Yuni Ginting, Clarissa Mulia, Sharron Syallomeita, Dennis Taweranusa, Gabriel Daffa, and others, 'Sosialisasi Perbandingan Hukuman Tindak Pidana Pembukaan Rahasia Data Pribadi Negara Indonesia Dan Inggris', *Jurnal Pengabdian West Science*, 3.04 (2024), 383–94 https://doi.org/10.58812/jpws.v3i04.1080

Aujla, Navneet, Helen Frost, Bruce Guthrie, Barbara Hanratty, Eileen Kaner, Amy O'Donnell, and others, 'A Comparative Overview of Health and Social Care Policy for Older People in England and Scotland, United Kingdom (UK)', *Health Policy*, 132.April (2023), 104814 https://doi.org/10.1016/j.healthpol.2023.104814

Ayu Palar, Miranda Risang, Laina Rafianti, and Helitha Novianty Muchtar, 'Inclusive Rights to Protect Communal Intellectual Property: Indonesian Perspective on Its New Government Regulation', *Cogent Social Sciences*, 9.2 (2023), 1–19 https://doi.org/10.1080/23311886.2023.2274431

Balboni, Paolo, and Kate Francis, 'Chapter 55 - Personal Privacy Policies', in *Computer and Information Security Handbook (Fourth Edition)*, ed. by John R Vacca, Fourth Edition (Morgan Kaufmann, 2025), pp. 907–16 https://doi.org/https://doi.org/10.1016/B978-0-443-13223-0.00055-2

Balboni, Prof. Dr. Paolo, and Kate Elizabeth Francis, 'Data Ethics and Digital Sustainability: Bridging Legal Data Protection Compliance and ESG for a Responsible Data-Driven Future', *Journal of Responsible Technology*, 2024, 100099 https://doi.org/https://doi.org/10.1016/j.jrt.2024.100099

Boothby, Neil, and Lindsay Stark, 'Data Surveillance in Child Protection Systems Development: An Indonesian Case Study', *Child Abuse and Neglect*, 35.12 (2011), 993–1001 https://doi.org/10.1016/j.chiabu.2011.09.004

Boychuk, Vasiliy, Kirill Sukharev, Daniil Voloshin, and Vladislav Karbovskii, 'An Exploratory Sentiment and Facial Expressions Analysis of Data from Photo-Sharing on Social Media: The Case of Football Violence', *Procedia Computer Science*, 80 (2016), 398–406 https://doi.org/10.1016/j.procs.2016.05.340

Calvi, Alessandra, 'Data Protection Impact Assessment under the EU General Data Protection Regulation: A Feminist Reflection', *Computer Law & Security Review*, 53 (2024), 105950 https://doi.org/https://doi.org/10.1016/j.clsr.2024.105950

Chatsuwan, Panchapawn, Tanawat Phromma, Navaporn Surasvadi, and Suttipong Thajchayapong, 'Personal Data Protection Compliance Assessment: A Privacy Policy Scoring Approach and Empirical Evidence from Thailand's SMEs', *Heliyon*, 9 (2023), 1–30 https://doi.org/https://doi.org/10.1016/j.heliyon.2023.e20648

Chelioudakis, Eleftherios, 'Unpacking AI-Enabled Border Management Technologies in Greece: To What Extent Their Development and Deployment Are Transparent and Respect Data Protection Rules?', *Computer Law & Security Review*, 53 (2024), 105967

https://doi.org/https://doi.org/10.1016/j.clsr.2024.105967

Chen, Meng, 'Developing China's Approaches to Regulate Cross-Border Data Transfer:Relaxation and Integration', *Computer Law & Security Review*, 54 (2024), 105997 https://doi.org/https://doi.org/10.1016/j.clsr.2024.105997

Choi, Daeeun Daniel, and Paul Benjamin Lowry, 'Balancing the Commitment to the Common Good and the Protection of Personal Privacy: Consumer Adoption of Sustainable, Smart Connected Cars', *Information & Management*, 61.1 (2024), 103876 https://doi.org/https://doi.org/10.1016/j.im.2023.103876

Christensen, Tanja Kammersgaard, 'Pre-Installed Cameras in Vehicles—New Technology from a Data Protection Law Perspective', *Computer Law & Security Review*, 53 (2024), 105980 https://doi.org/https://doi.org/10.1016/j.clsr.2024.105980

Conca, Silvia De, 'The Present Looks Nothing like the Jetsons: Deceptive Design in Virtual Assistants and the Protection of the Rights of Users', *Computer Law & Security Review*, 51 (2023), 105866 https://doi.org/https://doi.org/10.1016/j.clsr.2023.105866

Costantini, Federico, and Giada Soncini, 'Chapter 14 - Healthcare Data Governance in the EU: Main Challenges in Personal Data Protection', in *Endorobotics*, ed. by Luigi Manfredi (Academic Press, 2022), pp. 319–36 https://doi.org/https://doi.org/10.1016/B978-0-12-821750-4.00014-1

Custers, Bart, 'A Fair Trial in Complex Technology Cases: Why Courts and Judges Need a Basic Understanding of Complex Technologies', *Computer Law & Security Review*, 52 (2024), 105935 https://doi.org/10.1016/j.clsr.2024.105935

Custers, Bart, and Gianclaudio Malgieri, 'Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data', *Computer Law & Security Review*, 45 (2022), 105683 https://doi.org/https://doi.org/10.1016/j.clsr.2022.105683

van Daalen, O.L., 'The Right to Encryption: Privacy as Preventing Unlawful Access', *Computer Law & Security Review*, 49 (2023), 105804 https://doi.org/10.1016/j.clsr.2023.105804

Daudén-Esmel, Cristòfol, Jordi Castellà-Roca, and Alexandre Viejo, 'Blockchain-Based Access Control System for Efficient and GDPR-Compliant Personal Data Management', *Computer Communications*, 214 (2024), 67–87 https://doi.org/https://doi.org/10.1016/j.comcom.2023.11.017

Demetzou, Katerina, Gabriela Zanfir-Fortuna, and Sebastião Barros Vale, 'The Thin Red Line: Refocusing Data Protection Law on ADM, a Global Perspective with Lessons from Case-Law', *Computer Law & Security Review*, 49 (2023), 105806 https://doi.org/https://doi.org/10.1016/j.clsr.2023.105806

Demir, Esra, 'The Protection of Human Biodata: Is There Any Role for Data Ownership?', *Computer Law and Security Review*, 51.August 2022 (2023), 105905 https://doi.org/10.1016/j.clsr.2023.105905

Dewitte, Pierre, 'Better Alone than in Bad Company: Addressing the Risks of Companion Chatbots through Data Protection by Design', *Computer Law and Security Review*, 54.July

(2024), 106019 https://doi.org/10.1016/j.clsr.2024.106019

Dwivedi, Yogesh K., D. Laurie Hughes, Crispin Coombs, Ioanna Constantiou, Yanqing Duan, John S. Edwards, and others, 'Impact of COVID-19 Pandemic on Information Management Research and Practice: Transforming Education, Work and Life', *International Journal of Information Management*, 55.July (2020), 102211 https://doi.org/10.1016/j.ijinfomgt.2020.102211

Erdos, Dr David, 'Identification in Personal Data: Authenticating the Meaning and Reach of Another Broad Concept in EU Data Protection Law', *Computer Law & Security Review*, 46 (2022), 105721 https://doi.org/https://doi.org/10.1016/j.clsr.2022.105721

Fantonelli, Miliane dos Santos, Wagner Luiz Zanotto, Fabiana Magarrote Fernandes de Melo, Ianka Cristina Celuppi, Thaisa Cardoso Lacerda, Fernanda Maia de Oliveira, and others, 'Organization and Management of Sensitive Personal Health Data in Electronic Systems in Countries with Implemented Data Protection Laws, Lessons to Brazil: A Brief Systematic Review', *Computer Law and Security Review*, 51 (2023), 105872 https://doi.org/10.1016/j.clsr.2023.105872

Farhad, Mohsin Ali, 'Consumer Data Protection Laws and Their Impact on Business Models in the Tech Industry', *Telecommunications Policy*, 48.9 (2024), 102836 https://doi.org/https://doi.org/10.1016/j.telpol.2024.102836

Febbrajo, Alberto, *Law, Legal Culture and Society*, *Law, Legal Culture and Society*, 2018 https://doi.org/10.4324/9781351040341

Guamán, Danny S, David Rodriguez, Jose M del Alamo, and Jose Such, 'Automated GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Applications', *Computers & Security*, 130 (2023), 103262 https://doi.org/https://doi.org/10.1016/j.cose.2023.103262

Guo, Shuai, and Xiang Li, 'Cross-Border Data Flow in China: Shifting from Restriction to Relaxation?', *Computer Law & Security Review*, 56 (2025), 106079 https://doi.org/https://doi.org/10.1016/j.clsr.2024.106079

Haarberg, Frøydis Lønborg, 'What Do We Know about Children's Representation in Child Protection Decisions? A Scoping Review', *Children and Youth Services Review*, 160.March (2024) https://doi.org/10.1016/j.childyouth.2024.107588

Hu, Zhangxiang, 'Layered Network Protocols for Secure Communications in the Internet of Things', *University of Oregon: Eugene, OR, USA*, 2021

Hutomo, Priyo, and Markus Marselinus Soge, 'Perspektif Teori Sistem Hukum Dalam Pembaharuan Pengaturan Sistem Pemasyarakatan Militer', *Legacy: Jurnal Hukum Dan Perundang-Undangan*, 1.1 (2021), 46–68 https://doi.org/10.21274/legacy.2021.1.1.46-68

Imakura, Akira, Tetsuya Sakurai, Yukihiko Okada, Tomoya Fujii, Teppei Sakamoto, and Hiroyuki Abe, 'Non-Readily Identifiable Data Collaboration Analysis for Multiple Datasets Including Personal Information', *Information Fusion*, 98 (2023), 101826 https://doi.org/https://doi.org/10.1016/j.inffus.2023.101826

Ismail, Hamzah, Finley Febiyanto, Kevin, and Jurike V. Moniaga, 'Methods to Prevent

Privacy Violations on the Internet on the Personal Level in Indonesia', *Procedia Computer Science*, 216.2022 (2022), 650–54 https://doi.org/10.1016/j.procs.2022.12.180

Isus, Raichuk, Kateryna Kolesnikova, Iulia Khlevna, Timinskyi Oleksandr, and Kubiavka Liubov, 'Development of a Model of Personal Data Protection in the Context of Digitalization of the Educational Sphere Using Information Technology Tools', *Procedia Computer Science*, 231 (2024), 347–52 https://doi.org/https://doi.org/10.1016/j.procs.2023.12.215

Kant, Immanuel, *Kant: The Metaphysics of Morals* (Cambridge University Press, 2017)

Karjalainen, Tuulia, 'The Battle of Power: Enforcing Data Protection Law against Companies Holding Data Power', *Computer Law and Security Review*, 47.August 2018 (2022), 105742 https://doi.org/10.1016/j.clsr.2022.105742

Kaya, G.K., S. Ustebay, J. Nixon, C. Pilbeam, and M. Sujan, 'Exploring the Impact of Safety Culture on Incident Reporting: Lessons Learned from Machine Learning Analysis of NHS England Staff Survey and Incident Data', *Safety Science*, 166 (2023), 106260 https://doi.org/10.1016/j.ssci.2023.106260

Kollnig, Konrad, Lu Zhang, Jun Zhao, and Nigel Shadbolt, 'Privacy in Chinese IOS Apps and Impact of the Personal Information Protection Law', *Computer Law and Security Review*, 55.February 2020 (2024), 106041 https://doi.org/10.1016/j.clsr.2024.106041

Kuang, Linghong, Wenlong Shi, and Jing Zhang, 'Hierarchical Privacy Protection Model in Advanced Metering Infrastructure Based on Cloud and Fog Assistance', *Computers, Materials and Continua*, 80.2 (2024), 3193–3219 https://doi.org/https://doi.org/10.32604/cmc.2024.054377

Laxton, Debra, Linda Cooper, and Sarah Younie, 'Translational Research in Action: The Use of Technology to Disseminate Information to Parents during the COVID-19 Pandemic', *British Journal of Educational Technology*, 52.4 (2021), 1538–53 https://doi.org/https://doi.org/10.1111/bjet.13100

Lee, Jaeung, Melchor C. de Guzman, Jingguo Wang, Manish Gupta, and H. Raghav Rao, 'Investigating Perceptions about Risk of Data Breaches in Financial Institutions: A Routine Activity-Approach', *Computers and Security*, 121 (2022) https://doi.org/10.1016/j.cose.2022.102832

Li, Wenlong, and Jiahong Chen, 'From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China', *Computer Law & Security Review*, 54 (2024), 105994 https://doi.org/https://doi.org/10.1016/j.clsr.2024.105994

Li, Yuanxin, and Darina Saxunová, 'A Perspective on Categorizing Personal and Sensitive Data and the Analysis of Practical Protection Regulations', *Procedia Computer Science*, 170 (2020), 1110–15 https://doi.org/https://doi.org/10.1016/j.procs.2020.03.060

Lin, Jiacheng, Xianwen Dai, Ke Nai, Jin Yuan, Zhiyong Li, Xu Zhang, and others, 'BRPPNet: Balanced Privacy Protection Network for Referring Personal Image Privacy Protection', *Expert Systems with Applications*, 233 (2023), 120960 https://doi.org/https://doi.org/10.1016/j.eswa.2023.120960

Livingstone, Sonia, Kruakae Pothong, Ayça Atabey, Louise Hooper, and Emma Day, 'The Googlization of the Classroom: Is the UK Effective in Protecting Children's Data and Rights?', *Computers and Education Open*, 7.June (2024), 100195 https://doi.org/10.1016/j.caeo.2024.100195

Llanos, Jose Tomas, Madeline Carr, and Omer Rana, 'Using the Blockchain to Enable Transparent and Auditable Processing of Personal Data in Cloud- Based Services: Lessons from the Privacy-Aware Cloud Ecosystems (PACE) Project', *Computer Law & Security Review*, 51 (2023), 105873 https://doi.org/https://doi.org/10.1016/j.clsr.2023.105873

Locke, John, *Two Treatises of Government* (Cambridge university press, 1967)

Loideain, Nóra Ni, and Rachel Adams, 'From Alexa to Siri and the GDPR: The Gendering of Virtual Personal Assistants and the Role of Data Protection Impact Assessments', *Computer Law and Security Review*, 36 (2020), 1–14 https://doi.org/10.1016/j.clsr.2019.105366

———, 'From Alexa to Siri and the GDPR: The Gendering of Virtual Personal Assistants and the Role of Data Protection Impact Assessments', *Computer Law & Security Review*, 36 (2020), 105366 https://doi.org/https://doi.org/10.1016/j.clsr.2019.105366

Lubis, Muharman, and Dini Oktarina D. Handayani, 'The Relationship of Personal Data Protection towards Internet Addiction: Cyber Crimes, Pornography and Reduced Physical Activity', *Procedia Computer Science*, 197.2021 (2021), 151–61 https://doi.org/10.1016/j.procs.2021.12.129

Maple, Carsten, *Security and Privacy in the Internet of Things*, *Journal of Cyber Policy*, 2017, II https://doi.org/10.1080/23738871.2017.1366536

Marelli, Massimo, 'The Law and Practice of International Organizations' Interactions with Personal Data Protection Domestic Regulation: At the Crossroads between the International and Domestic Legal Orders', *Computer Law & Security Review*, 50 (2023), 105849 https://doi.org/https://doi.org/10.1016/j.clsr.2023.105849

'Marriott Breached Again', *Computer Fraud & Security*, 2020.4 (2020), 3 https://doi.org/https://doi.org/10.1016/S1361-3723(20)30035-X

Milkaite, Ingrida, Ralf De Wolf, Eva Lievens, Tom De Leyn, and Marijn Martens, 'Children's Reflections on Privacy and the Protection of Their Personal Data: A Child-Centric Approach to Data Protection Information Formats', *Children and Youth Services Review*, 129.December 2020 (2021), 106170 https://doi.org/10.1016/j.childyouth.2021.106170

Mollaeefar, Majid, and Silvio Ranise, 'Identifying and Quantifying Trade-Offs in Multi-Stakeholder Risk Evaluation with Applications to the Data Protection Impact Assessment of the GDPR', *Computers & Security*, 129 (2023), 103206 https://doi.org/https://doi.org/10.1016/j.cose.2023.103206

Montenarh, Jonas, and Simon Marsden, 'Unmasking the Oligarchs – Using Open Source Data to Detect Sanctions Violations', *Journal of Economic Criminology*, 3.February (2024), 100055 https://doi.org/10.1016/j.jeconc.2024.100055

Mourby, Miranda, Elaine Mackey, Mark Elliot, Heather Gowans, Susan E. Wallace, Jessica Bell, and others, 'Are "Pseudonymised" Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK', *Computer Law and Security Review*, 34.2 (2018), 222–33 https://doi.org/10.1016/j.clsr.2018.01.002

Mutiara, Upik, and Romi Maulana, 'Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi', *Indonesian Journal of Law and Policy Studies*, 1.1 (2020), 42 https://doi.org/10.31000/ijlp.v1i1.2648

Navickas, Katrina, 'Legal and Historical Geographies of the Greenham Common Protest Camps in the 1980s', *Journal of Historical Geography*, 82 (2023), 11–22 https://doi.org/10.1016/j.jhg.2023.07.002

Niffari, Hanifan, 'Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain', *Jurnal Hukum Dan Bisnis (Selisik)*, 6.1 (2020), 1–14 https://doi.org/10.35814/selisik.v6i1.1699

Noor, Hendry Julian, Kardiansyah Afkar, and Henning Glaser, 'Application of Sanctions Against State Administrative Officials in Failure to Implement Administrative Court Decisions', *BESTUUR*, 9.1 (2021), 72 https://doi.org/10.20961/bestuur.v9i1.49686

Pascual, Hugo, Jose M del Alamo, David Rodriguez, and Juan C Dueñas, 'Hunter: Tracing Anycast Communications to Uncover Cross-Border Personal Data Transfers', *Computers & Security*, 141 (2024), 103823 https://doi.org/https://doi.org/10.1016/j.cose.2024.103823

Pauletto, Christian, 'Options towards a Global Standard for the Protection of Individuals with Regard to the Processing of Personal Data', *Computer Law & Security Review*, 40 (2021), 105433 https://doi.org/https://doi.org/10.1016/j.clsr.2020.105433

Phillips, Benjamin, 'UK Further Education Sector Journey to Compliance with the General Data Protection Regulation and the Data Protection Act 2018', *Computer Law & Security Review*, 42.105586 (2021), 1–13 https://doi.org/https://doi.org/10.1016/j.clsr.2021.105586

Pleger, Lyn E., Katharina Guirguis, and Alexander Mertes, 'Making Public Concerns Tangible: An Empirical Study of German and UK Citizens' Perception of Data Protection and Data Security', *Computers in Human Behavior*, 122.February 2020 (2021), 106830 https://doi.org/10.1016/j.chb.2021.106830

Pratono, Aluisius Hery, and Ari Sutanti, 'The Ecosystem of Social Enterprise: Social Culture, Legal Framework, and Policy Review in Indonesia', *Pacific Science Review B: Humanities and Social Sciences*, 2.3 (2016), 106–12 https://doi.org/10.1016/j.psrb.2016.09.020

Purtova, Nadezhda, and Robin L Pierce, 'Citizen Scientists as Data Controllers: Data Protection and Ethics Challenges of Distributed Science', *Computer Law & Security Review*, 52 (2024), 105911 https://doi.org/https://doi.org/10.1016/j.clsr.2023.105911

Qaid, Hanif, Ari Widyanti, Sheila Amalia Salma, Fitri Trapsilawati, Titis Wijayanto, Utami Dyah Syafitri, and others, 'Speed Choice and Speeding Behavior on Indonesian Highways: Extending the Theory of Planned Behavior', *IATSS Research*, 46.2 (2022),

193–99 https://doi.org/10.1016/j.iatssr.2021.11.013

Ranjan, Aditya Kaushal, and Prabhat Kumar, 'APPS: Authentication-Enabled Privacy Protection Scheme for Secure Data Transfer in Internet of Things', *Ad Hoc Networks*, 164 (2024), 103631 https://doi.org/https://doi.org/10.1016/j.adhoc.2024.103631

Rataj, Piotr, 'Botnet Defense under EU Data Protection Law', *Computer Law & Security Review*, 56 (2025), 106080 https://doi.org/https://doi.org/10.1016/j.clsr.2024.106080

Rupp, Valentin, and Max von Grafenstein, 'Clarifying "Personal Data" and the Role of Anonymisation in Data Protection Law Including and Excluding Data from the Scope of the GDPR (More Clearly) through Refining the Concept of Data Protection', *Computer Law and Security Review*, 52.1 (2024), 105932 https://doi.org/10.1016/j.clsr.2023.105932

Sautunnida, Lia, 'Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia', *Kanun Jurnal Ilmu Hukum*, 20.2 (2018), 369–84 https://doi.org/10.24815/kanun.v20i2.11159

Setiabudhi, Donna Okthalia, Ahsan Yunus, Irwansyah Irwansyah, and Andi Rifky, 'The Role of Land Management Paradigm Towards Certainty and Justice', *BESTUUR*, 11.1 (August) (2023), 43 https://doi.org/10.20961/bestuur.v11i1.71710

Sharpe, Sybil, *National Security, Personal Privacy and the Law: Surveying Electronic Surveillance and Data Acquisition*, *National Security* (Routledge, 2019) https://doi.org/10.4324/9780429020025

Silbey, Susan S., *Legal Culture and Legal Consciousness*, *International Encyclopedia of the Social & Behavioral Sciences: Second Edition*, Second Edi (Elsevier, 2015), XIII https://doi.org/10.1016/B978-0-08-097086-8.86067-5

de Sousa Rocha, Núbia Augusto, Alexandre Nascimento de Almeida, André Nunes, and Humberto Angelo, 'Critical Points for the Processing of Personal Data by the Government: An Empirical Study in Brazil', *Computer Law & Security Review*, 54 (2024), 106023 https://doi.org/https://doi.org/10.1016/j.clsr.2024.106023

Steppe, Richard, 'Online Price Discrimination and Personal Data: A General Data Protection Regulation Perspective', *Computer Law and Security Review*, 33.6 (2017), 768–85 https://doi.org/10.1016/j.clsr.2017.05.008

Studzinska, Joanna, 'Request for Information as an Auxiliary Measure in Intellectual Property Litigation Concerning Electronic Works and the Protection of Personal Data', *Procedia Computer Science*, 207 (2022), 4276–87 https://doi.org/https://doi.org/10.1016/j.procs.2022.09.491

Sun, Panjun, Yi Wan, Zongda Wu, Zhaoxi Fang, and Qi Li, 'A Survey on Privacy and Security Issues in IoT-Based Environments: Technologies, Protection Measures and Future Directions', *Computers & Security*, 148 (2025), 104097 https://doi.org/https://doi.org/10.1016/j.cose.2024.104097

Tang, Alan, *Privacy in Practice*, *Privacy in Practice*, 2022 https://doi.org/10.1201/9781003225089

Tauda, Gunawan A., Andy Omara, and Gioia Arnone, 'Cryptocurrency: Highlighting the Approach, Regulations, and Protection in Indonesia and European Union', *BESTUUR*, 11.1 (August) (2023), 1 https://doi.org/10.20961/bestuur.v11i1.67125

de Terwangne, Cécile, 'Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data', *Computer Law and Security Review*, 40.September 1980 (2021), 3–4 https://doi.org/10.1016/j.clsr.2020.105497

Tonheim, Milfrid, Muireann Ní Raghallaigh, Ketil Eide, and Ala Sirriyeh, 'Relational and Cultural Continuity for Children in Foster Care; A Critical Explo- Ration of National Policies in Norway, Sweden, Denmark, England, Ireland and Scotland', *Children and Youth Services Review*, 2024, 108040 https://doi.org/10.1016/j.childyouth.2024.108040

'UK Strategy Slated by Own Biometrics Commissioner', *Biometric Technology Today*, 2018.7 (2018), 11–11 https://doi.org/10.1016/s0969-4765(18)30096-1

Valero, Cayetano, Jaime Pérez, Sonia Solera-Cotanilla, Mario Vega-Barbas, Guillermo Suarez-Tangil, Manuel Alvarez-Campana, and others, 'Analysis of Security and Data Control in Smart Personal Assistants from the User's Perspective', *Future Generation Computer Systems*, 144 (2023), 12–23 https://doi.org/https://doi.org/10.1016/j.future.2023.02.009

Wang, Feng, Yongjie Gai, and Haitao Zhang, 'Blockchain User Digital Identity Big Data and Information Security Process Protection Based on Network Trust', *Journal of King Saud University - Computer and Information Sciences*, 36.4 (2024), 102031 https://doi.org/https://doi.org/10.1016/j.jksuci.2024.102031

Wang, Wayne Wei, 'Contextualizing Personal Information: Privacy's Post-Neoliberal Constitutionalism and Its Heterogeneous Imperfections in China', *Computer Law & Security Review*, 55 (2024), 106030 https://doi.org/https://doi.org/10.1016/j.clsr.2024.106030

Wang, Yu, 'Data Structure and Privacy Protection Analysis in Big Data Environment Based on Blockchain Technology', *International Journal of Intelligent Networks*, 5 (2024), 120–32 https://doi.org/https://doi.org/10.1016/j.ijin.2024.02.005

Wicaksono, Agung, Irni Yunita, and Gede Ginaya, 'Living Side by Side with Nature: Evidence of Self-Governance in Three Local Communities in Indonesia', *Heliyon*, 8.12 (2022), e12248 https://doi.org/10.1016/j.heliyon.2022.e12248

Xiao, Zhiqiang, Jiacheng Lin, Jiajun Chen, Haolong Fu, Yifan Li, Jin Yuan, and others, 'Privacy Preservation Network with Global-Aware Focal Loss for Interactive Personal Visual Privacy Preservation', *Neurocomputing*, 602 (2024), 128193 https://doi.org/https://doi.org/10.1016/j.neucom.2024.128193

Yang, Shuling, and Yan Hou, 'Cultivation Strategies of English Thinking Ability in the Environment of Internet of Things Shuling', *HELIYON*, 2024, e39515 https://doi.org/10.1016/j.heliyon.2024.e39515

Yang, Zenghui, Xiubo Chen, Yunfeng He, Luxi Liu, Yinmei Che, Xiao Wang, and others, 'An Attribute-Based Access Control Scheme Using Blockchain Technology for IoT Data Protection', *High-Confidence Computing*, 4.3 (2024), 100199

https://doi.org/https://doi.org/10.1016/j.hcc.2024.100199

Ye, Jun, Ling Wang, Zhiyu Wang, Zhengqi Zhang, Zheng Xu, and Jinghua Zhao, 'An Electronic Voting Scheme with Privacy Protection', *Procedia Computer Science*, 243 (2024), 1248–56 https://doi.org/https://doi.org/10.1016/j.procs.2024.09.147

Ye, Xiongbiao, Yuhong Yan, Jia Li, and Bo Jiang, 'Privacy and Personal Data Risk Governance for Generative Artificial Intelligence: A Chinese Perspective', *Telecommunications Policy*, 48.10 (2024), 102851 https://doi.org/https://doi.org/10.1016/j.telpol.2024.102851

Zheng, Guan, and Jinchun Shu, 'In the Name of Protection—A Critical Analysis of China's Legal Framework of Children's Personal Information Protection in the Digital Era', *Computer Law and Security Review*, 53.April (2024), 105979 https://doi.org/10.1016/j.clsr.2024.105979

Zinovieva, Vera, Mikhail Shchelokov, and Evgeny Litvinovsky, 'Legal Issues of Protection of Personal Data: Cases of Transport Data Leaks', *Transportation Research Procedia*, 68 (2023), 461–67 https://doi.org/https://doi.org/10.1016/j.trpro.2023.02.062