International Journal of Educational Review, Law & Social Sciences (IJERLAS)

International Journal of Educational Review, Law And Social Sciences (IJERLAS Journal) | ISSN (e): 2808-487X
Volumes 6 No. 1 (2025)

IMPLICATIONS OF PERSONAL DATA LEAKS FROM THE PUBLICATION OF JUDICIAL DECISIONS IN THE SUPREME COURT DECISION DIRECTORY ON PERSONAL DATA PROTECTION

Roni Evi Dongoran[1], Nurini Aprilianda[2], Faizin Sulistio[3]
E-mail: Evisiregar71@gmail.com, nurini.aprilianda@ub.ac.id, faizin@ub.ac.id

Received	: 15 September 2025	Published	: 18 November 2025
Revised	: 10 October 2025	DOI	: https://doi.org/10.54443/ijerlas.v6i1.4450
Accepted	: 31 October 2025	Link Publish	: https://radjapublika.com/index.php/IJERLAS

Abstract

The publication of court decisions in the Indonesian Supreme Court Decision Directory is a form of public information disclosure. However, in practice, these publications often contain the personal data of the parties involved, such as their National Identification Number, full address, and the identity of victims, even in cases where this information should be redacted. This situation creates the potential for personal data leaks that could open up opportunities for information misuse, violate privacy rights, and pose security risks. This study aims to analyze the implications of personal data leaks originating from the publication of court rulings in the Supreme Court's ruling directory on personal data protection in the era following the enactment of Law-Law Number 27 of 2022 concerning Personal Data Protection and the issuance of the Supreme Court Chief Justice's Decree Number 2-144/KMA/SK/VIII/2022 concerning Public Information Service Standards in Courts. The research method used is normative juridical with a legislative, case analysis, and conceptual approach, supplemented by a study of examples of publicly published decisions. The results of the study show that there are still discrepancies between the practice of publishing decisions and the obligation to protect personal data. These findings indicate the need to strengthen editorial policies, obscuring standards, and internal monitoring mechanisms so that the openness of judicial information does not sacrifice the privacy rights of the public. This study is expected to contribute to improving the governance of decision publication and strengthening the personal data protection regime in Indonesia.

Keywords: personal data leaks, publication of court decisions, personal data protection, public information disclosure, Supreme Court decision directory.

INTRODUCTION

The rapid development of information and communication technology has created various opportunities and challenges. Various sectors of life have utilized information technology systems such as *electronic education (e-education)* in the field of education, *electronic health* (*e-health*) in the field of health, *electronic government* (*e-government*) in the field of government, including information technology utilized in the field of public information disclosure by the Supreme Court. In order to respond to demands for public information disclosure and to realize transparent justice, as well as to make it easier for the general public to access court decisions, the Supreme Court of the Republic of Indonesia has created an innovation called the Decision Directory, which is an online tool for the general public to obtain court decisions. This innovation is an effort by the Supreme Court to fulfill the public's right to information as affirmed in the amended 1945 Constitution.

As a medium for publishing decisions that can be accessed electronically, the main purpose of the Decision Directory is to provide easy access for the public to information about court decisions, which is intended for the benefit of legal practitioners, academics, and the general public. With the Judgment Directory, the Supreme Court hopes that the public will have easier access to judgments related to cases they are facing and provide a space for searching judgments that can be used as references for parties with an interest in the legal world. The breakthrough regarding the Judgment Directory was welcomed by the public. The Supreme Court was considered responsive in meeting the demands for public information disclosure as mandated by Law Number 14 of 2008 concerning Public

[1] Master of Law, Brawijaya University PSDKU Jakarta
[2] Faculty of Law, Brawijaya University, Malang
[3] Faculty of Law, Brawijaya University, Malang

Information Disclosure ("Public Information Disclosure Law"). However, over time, this breakthrough in transparency has faced serious challenges, particularly regarding the protection of the privacy of the parties involved in the case. In many cases, published decisions contain sensitive information such as personal data, both specific and general. In practice, such data can trigger social stigma in society, which certainly has an impact on the parties concerned, such as the personal data of parties in divorce cases and cases related to morality, which can be easily accessed by the public in the Supreme Court Decision Directory.

In such circumstances, the author sees a conflict between the importance of public information disclosure and the protection of personal data of parties involved in legal proceedings. The Supreme Court's efforts to make it easier for the public to obtain information categorized as public information actually conflicts with the right to personal data protection of parties involved in legal proceedings.[4] This is certainly an issue that requires serious attention, especially for the Supreme Court, considering that the protection of personal data is a human right that is part of personal protection, so it is necessary to provide a legal basis for the security of personal data based on the 1945 Constitution of the Republic of Indonesia.

Historically, the terms privacy and personal data are not new concepts. Although the International Covenant on Civil and Political Rights (ICCPR) does not explicitly mention the term 'personal data', in terms of substance, the protection of personal data can be considered an integral part of an individual's privacy or personal life. The protection of personal data is not only regulated in the European Union's regional convention (General Data Protection Regulation/GDPR), but also in various other regions, such as Africa (African Union Convention on Cyber Security and Personal Data Protection) and Asia. The ASEAN Declaration of Human Rights explicitly states that personal data is an integral part of privacy, although the explanation is not very detailed.

Currently, the Supreme Court has issued Supreme Court Chief Justice Decree No. 2-144/KMA/SK/VIII/2022 on Public Information Service Standards in Courts ("SK KMA 2-144"), which has been adjusted to several recent regulations related to information disclosure. The provisions on personal data protection in SK KMA 2-144 can be seen from the provisions regarding the obligation of courts to obscure information that is excluded as public information. The definition of public information as defined in SK KMA 2-144 is information that is produced, stored, managed, sent, and/or received and coordinated by the court in relation to the administration and performance of the duties and functions of the court, as well as other information related to the public interest[5] .

Essentially, in KMA Decree 2-144, cases that must be obscured are limited to criminal cases involving indecency, crimes related to domestic violence, crimes in which the identities of witnesses and victims must be protected according to the law on the protection of witnesses and victims, cases involving indecency, and other criminal offenses which, according to the law, must be tried in closed session. Meanwhile, for civil cases, the scope is limited to marriage cases and other cases arising from marriage disputes, child adoption, wills, and civil, religious civil, and administrative cases which, according to the law, must be tried in closed session. In addition, the information that is obscured in these cases is also limited to personal data such as names and aliases, identity card/passport numbers, occupations, places of work and relevant employee identities, schools or educational institutions attended, the identity of witnesses, the identity of judges, court clerks, public prosecutors, investigators, witnesses, and experts in terrorism cases, the identity of children, and the number of evidence documents.

The provisions regarding the redaction of information excluded from public information seem like a breath of fresh air for the protection of personal data of parties involved in a case, but problems arise when faced with the implementation of information redaction provisions that do not work properly. In many cases, both civil and criminal, which are published through the decision directory, there is still a lot of information that should have been obscured but has not been obscured, most of which relates to the personal data of the parties to the case, which is highly vulnerable to misuse, such as for committing fraud and other crimes.

In essence, the author argues that every party involved in cases in all judicial institutions under the Supreme Court has the right to protection of their personal data. However, in practice, it can be seen how easy it is for the public to obtain such personal data from the Judgment Directory. This is the basis for the research conducted by the author, which focuses on analyzing the implications of personal data leaks originating from the publication of judges' decisions in the Supreme Court's Decision Directory on personal data protection.

[4] See consideration letter a of Law Number 27 of 2022 concerning Personal Data Protection

[5] See point I number 5 of Appendix I to the Decision of the Chief Justice of the Supreme Court of the Republic of Indonesia Number: 2-144/KMA/SK/VIII/2022 dated August 30, 2022

LITERATURE REVIEW

Previously, there have been several authors who have researched the protection of personal data in court decisions, but in this study there is a very fundamental difference, namely in terms of the subject matter researched by the author. In previous studies, authors have basically focused their research on legal protection for parties in divorce and indecency cases whose personal data is not anonymized in Published decisions and examined the urgency of additional criminal penalties for the announcement of court decisions after the policy of publishing decisions through the decision directory. In this study, the author will examine the implications of the leakage of personal data of the parties to the case originating from the judge's decision published in the Supreme Court Decision Directory on the protection of personal data, whereby the author's research is not only on divorce, indecency, or cases whose hearings are closed, but concerns all types and classifications of decisions in the Decision Directory, including petition cases. In addition, in this study, the author will also discuss the intersection between public information disclosure and personal data protection in court decisions published through the Decision Directory. Another thing that distinguishes this study is that in conducting the analysis, the author uses a legislative approach as well as a case approach. Through a legislative approach, this study aims to provide an overview of how Indonesian positive law regulates the protection of personal data of parties to a case. Through a case study approach, it is hoped that this study can provide an overview of how easy it is for the general public to access the personal data of parties to a case through court decisions published in the Supreme Court's decision directory, which has the potential to cause legal problems in the future as technology continues to develop rapidly.

METHOD

In conducting this research, the author uses normative legal research, which can be defined as a scientific procedure for obtaining truth based on the logic of legal science from a normative perspective[6] . Normative legal studies refer to legal theory and legal philosophy. The author will analyze and identify the implications of personal data leaks originating from the publication of judges' decisions in the Supreme Court Decision Directory on personal data protection and how Indonesian positive law regulates personal data protection in judges' decisions published through the Supreme Court Decision Directory. In conducting this research, the author analyzed Law Number 27 of 2022 concerning Personal Data Protection, Law Number 14 of 2008 concerning Public Information Disclosure, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, and the Decree of the Chief Justice of the Supreme Court Number 2-144/KMA/SK/VIII/2022 concerning Standards for Public Information Services in Courts. In addition to legislation, the materials for this research also come from legal literature such as Academic Manuscripts of Related Legislation, Dissertations, Theses, Research Reports, Journals, Articles, and scientific papers related to the author's research topic.

RESULTS AND DISCUSSION

Implications of Personal Data Leaks Originating from the Publication of Judicial Decisions in the Supreme Court Decision Directory on Personal Data Protection

Freedom of information gives everyone the freedom to seek, obtain, and disseminate information within their control. The right to information is enshrined in Article 19 of *the Universal Declaration of Human Rights* (UDHR), which states:

> "*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of* frontiers[7] "

The provisions of Article 19 of the UDHR guarantee that everyone has the freedom to express their opinions, which includes two things. First, everyone has the freedom to maintain their opinions without interference from others. Second, everyone has the right to seek, receive, and impart information and ideas through various media without restriction. The implementation of the right to information in terms of dissemination of information can refer to *General Comment number* 34 published by *the United Nations Human Rights Committee* in 2011.

The right to information is limited to three activities, namely seeking, obtaining, and disseminating information. Everyone is free to carry out these three activities through various media without restriction. In practice, the right to information has the potential to cause problems when it conflicts with an individual's right to privacy. On the one hand, the right to information gives everyone the freedom to seek, obtain, and disseminate information, while

[6] Johnny Ibrahim, Theory and Methods of Normative Legal Research, (Malang: Bayumedia, 2012), p. 57.

[7] Cameron G. Shilling, *Privacy and Data Security: New Challenges of the Digital Age,* in Dhoni Martien, Legal Protection of Personal Data, Mitra Ilmu: 2023, p. 49

on the other hand, everyone has the right to privacy to protect themselves, including protecting their personal information or data[8] . Law Number 27 of 2022 concerning Personal Data Protection ("Personal Data Protection Law") defines personal data as data about an identified or identifiable individual, either individually or in combination with other information, either directly or indirectly, through electronic or non-electronic systems, whereby the protection of such personal data is a human right that forms part of the protection of personal privacy, as emphasized in the preamble to the law. Furthermore, it is also emphasized that personal data protection is intended to guarantee citizens' rights to personal protection and to foster public awareness and ensure recognition and respect for the importance of personal data protection[9] .

The existence of the Personal Data Protection Law is mandated by Article 28G paragraph (1) of the 1945 Constitution, which states that "Every person shall have the right to protection of their personal life, family, honor, dignity, and property under their control, as well as the right to feel secure and protected from the threat of fear to do or not do something that is a fundamental right." The issue of Personal Data Protection arises from concerns about violations of Personal Data that may be experienced by individuals and/or legal entities. Such violations can cause material and non-material losses. Information disclosure and privacy protection essentially have the same goal, which is to encourage accountability from the government to its people, more specifically in this case accountability from judicial institutions to people seeking justice. The right to privacy and information disclosure play an important role in ensuring that public officials remain accountable to the people they serve. Therefore, one of the challenges in this era of digitalization is how the state can balance the need to protect privacy while at the same time maintaining information and data disclosure, especially information and data held by state institutions such as the Supreme Court.

In this context, openness, information, and data are closely related to privacy protection, both in terms of mutual dependence and conflicting nature. However, these two rights essentially play different roles, with only a few areas where they are interrelated and may give rise to potential conflicts. The Supreme Court, as a state institution that administers the judicial system in Indonesia, essentially collects a large amount of data related to the personal information of parties involved in both criminal and civil cases. The problem is that sometimes the public requests access to this data and information for various reasons. Freedom of information laws in many countries, including Indonesia, generally exclude access to personal information. However, given the complexity of the issue between privacy protection and freedom of information, information managers at the Supreme Court and subordinate judicial bodies are generally still faced with the difficult question of what types of information should actually be protected and cannot be made accessible to the public.

The Supreme Court, as one of the judicial authorities in Indonesia that examines, adjudicates, and decides cases, strives to fulfill the public's right to access information, particularly information regarding cases it handles, including those handled by subordinate judicial bodies, while maintaining the privacy rights of the parties involved by issuing Supreme Court Decree 2-144, which serves as a guideline for the Supreme Court and its subordinate judicial bodies.under its jurisdiction, while maintaining the privacy rights of the parties involved by issuing KMA Decree 2-144, which serves as a guideline for Information and Documentation Management Officers (PPID) at every level of the Court to provide and/or serve the public's need for public information available at the Supreme Court and judicial bodies under it.

As discussed above, one of the Supreme Court's efforts to meet the public's need for information regarding judges' decisions at every level of the judiciary is through the Decision Directory, which is an online tool that contains judges' decisions at every level of the judiciary and can be accessed by the general public from anywhere and at any time. Currently, the Supreme Court also continues to develop the electronic 'Decision Directory', which is one of the implementations of KMA Decree 2-144, which aims to ensure that complete information is available to the public quickly and cheaply.

Decree KMA 2-144 essentially regulates the types of information that must be proactively disclosed by the court and the mechanism for its disclosure. The information in question is that which is considered important for justice seekers and the public to know, including court decisions and rulings. The author analyzes in greater depth the provisions regarding the regulation of personal data in SK KMA 2-144, which clearly states that the Court is obliged to follow service standards, institutional management of information and documentation, establish and update the Public Information List, prepare and publish Public Information service reports, submit copies of Public Information service reports to the Information Commission, and monitor, evaluate, and provide guidance on the

[8] Nenny Rianarizkiwati, Freedom of Information versus the Right to Privacy: The State's Responsibility in Personal Data Protection, 2022. p. 55
[9] See Considerations of Law Number 27 of 2022 concerning Personal Data Protection

implementation of Public Information services. These obligations are carried out with due regard for the protection of personal data as stipulated by laws and regulations and the obscuring of information.

Electronic court decisions (*digitale rechterlijke uitspraak*) or similar decisions in the digital era are not included in the category of exempted information as listed in Article 18 of Law Number 14 of 2008 concerning Public Information Disclosure ("Public Information Disclosure Law") as follows[10] :

1. Judicial decisions;
2. Decrees, decisions, regulations, circular letters, or other forms of policy, whether binding or non-binding, internal or external, as well as considerations of law enforcement agencies.

Upon closer examination, Article 3 of Law Number 11 of 2008 concerning Electronic Information and Transactions ("Electronic Information and Transactions Law") also emphasizes that such exempted information may be carried out through the use of information technology and electronic transactions, while still observing the principles of legal certainty, benefit, prudence, good faith, and freedom to choose technology or technological neutrality.

The question that then arises is whether the Supreme Court, as the controller of the personal data of the parties involved in the case, has applied the principles as stipulated in Article 3 of the Electronic Information and Transactions Law? Do the provisions in the KMA Decree sufficiently accommodate the protection of the personal data of the parties involved in the case? It should be understood that a judge's decision is a legal product that contains a lot of personal data. In criminal cases, in addition to the personal data of the defendant, there is also the personal data of witnesses, victims, and experts who are presented at the trial, while in civil cases, in addition to the personal data of the plaintiff and defendant, it also contains the personal data of witnesses, experts, and other important documents, which makes it easy for irresponsible parties to misuse such personal data. Many previous studies have discussed how criminal fraud can easily occur through using personal data such as a person's full name, address, and national identification number, as well as how a person's case history and criminal record affect their social life in the community.

Implications of Personal Data Leaks in Criminal and Civil Case Rulings

In criminal cases, the parties commonly listed in a verdict include the Defendant, Witnesses, Experts, Victims, and in some cases also include the Defendant's family and the Victim's family. Each of these parties has a different legal role and factual contribution in the judicial process, so that their identities and personal data are often explicitly included in the verdict document. The Defendant's personal data, for example, must be included as stipulated in Article 197 Paragraph (1) letter b of the Criminal Procedure Code ("KUHAP"), which requires the mention of the Defendant's full identity as part of the formal requirements of a judge's verdict. However, in practice, the information included is not limited to basic identity data such as name, place and date of birth, gender, nationality, and address, but may also include more sensitive data. Such additional data includes information about family members, medical history, *mobile phone* numbers, employment history, and identity documents such as identity card numbers, birth certificate numbers, and so on.

Based on the Author's search of the Supreme Court Decision Directory website, the Author found that there are still criminal case decisions that have not been redacted, such as Donggala District Court Decision Number 140/Pid.Sus/2023/PN Dgl, which is a decision on a criminal case of sexual abuse involving a child as the victim and witness. which, based on the provisions of SK KMA 2-144, should have had the identities of the child, both as the victim and witness, redacted. However, based on a review of the decision, it is known that the redaction process has not been fully implemented, as the real names of the child victim and child witness are still listed in the copy of the decision published through the Supreme Court Decision Directory. This failure to comply with the obligation to obscure identities has the potential to have serious consequences, particularly in terms of protecting the rights of child victims. The disclosure of a child's identity to the public can have psychological effects such as shame, further trauma, and social pressure, which can hinder the victim's mental recovery process. In addition, it also has the potential to cause stigmatization from the surrounding environment, which in can ultimately affect the child's growth and development and hinder their social reintegration efforts. Thus, negligence in obscuring the identity of children not only violates the principle of confidentiality as stipulated in laws and regulations, but also contradicts the spirit of child protection in the criminal justice system in Indonesia.

The leakage of data belonging to parties to a case through a judge's decision can be categorized as a violation of personal data misuse because even though a judge's decision is a legal product categorized as public information,

[10] Endah Dewi Nawangsasi Sukarton, *Privacy Protection in the New Normal Digital Lifestyle Era Related to Cyber Power,* PT Refika Aditama:2022, p.77

violations of the privacy rights of parties to a case should not be ignored, especially by a judicial institution. The disclosure of personal data also has a negative impact on defendants and former prisoners. With the publication of verdicts that reveal their full identities, defendants who have served their sentences often experience difficulties in social reintegration. *Labeling* theory explains that individuals who have been labeled as criminals will find it difficult to be accepted back into society, thus potentially repeating criminal acts due to social marginalization. In this case, publishing verdicts without obscuring identities can reinforce stigma and discrimination, which is contrary to the objectives of the correctional system.

The implications of personal data leaks in criminal cases not only harm the individuals involved, but also have the potential to weaken the criminal justice system itself. Transparency, which is intended to increase accountability, can actually become a form of human rights violation if it is not balanced with adequate privacy protection. Unlike criminal cases, which focus more on protecting victims, witnesses, and defendants, civil cases have broader implications for personal data leaks in the social and economic spheres. Civil judgments often contain sensitive information such as residential addresses, identity numbers, family data, and financial transaction details. The disclosure of such information to the public can be exploited by irresponsible parties to commit fraud, identity theft, or other cybercrimes. In domestic dispute cases, for example, the personal data of children or spouses can become public consumption, even though this has the potential to cause trauma and prolonged conflict. Thus, personal data leaks in civil cases are not only economically detrimental but can also disrupt social stability and family harmony.

In civil cases, court decisions generally contain administrative, contractual, or family details. If no redaction is carried out, sensitive personal data may be exposed and cause serious consequences. First, in family cases such as divorce, child custody, and inheritance disputes, published decisions often include the full identities of family members, including minors. This has the potential to cause psychological trauma to children because their family circumstances are exposed openly to the public. In addition, the disclosure of household data can invite social stigma that is detrimental to certain parties, especially in societies that still view divorce as taboo. In cases involving agreements or debts, published decisions may contain detailed information about the addresses, identity numbers, or financial data of the parties. This data is highly vulnerable to misuse for criminal purposes, such *as identity theft*, online fraud, or other cybercrimes. In the digital age, where personal data has high economic value, such information leaks can cause significant financial losses to the parties involved. In business or commercial disputes, published verdicts often include strategic information related to company assets, business agreements, or trade secrets. If this information is made public, it can harm the interests of the corporation and reduce its competitiveness in the market. Furthermore, this situation also has the potential to give rise to new commercial conflicts, as interested parties can use this information for specific purposes.

Based on the author's research, several examples of civil case decisions or rulings published in the Decision Directory that do not fully accommodate the provisions of SK KMA 2-144 include the Tigaraksa Religious Court Decision Number 762/Pdt.P/2025/PA.Tgrs dated October 6, 2025, Bulukamba District Court Decision Number 213/Pdt.P/2025/PN Blk dated September 16, 2025, and Denpasar District Court Decision Number 430/Pdt.G/2025/PN Dps dated June 4, 2025. From the author's review of three examples of civil case decisions/rulings published in the Supreme Court Decision Directory, it was found that personal data was freely accessible to the public without adequate restrictions. This personal data includes, among other things, National Identification Numbers (NIK) and the names of parties involved in divorce cases. This condition shows that the publication of decisions has not fully taken into account the principle of personal data protection as it should. In fact, SK KMA 2-144 explicitly stipulates that NIK is part of personal data that should be obscured in the publication of decisions. However, this regulation still causes ambiguity because it does not explicitly explain whether the obligation to obscure applies to all types of cases or only to certain sensitive cases, such as child cases or domestic violence cases.

Furthermore, in divorce cases, the names of the parties are also classified as personal data that must be kept confidential to protect the privacy and dignity of the individuals concerned. However, based on one example of a Denpasar District Court decision analyzed, the author found negligence in the redaction process, where the names of the parties were still listed in full along with the marriage certificate mentioned in the decision. This kind of negligence often occurs because the party assigned to redact personal data focuses more on the parties' identities at the beginning of the ruling without examining the entire contents of the document. As a result, even though the ruling has been formally edited, its substance still contains information that could reveal the personal identities of the parties involved in the case. This situation illustrates the weak implementation of personal data protection policies in the judicial system, which has the potential to cause legal and social implications for individuals whose data is exposed to the public.

In this context, judicial institutions have a significant responsibility to ensure that every published decision does not conflict with the principles of personal data protection. The obligation to redact identities is not merely administrative in nature, but rather a manifestation of moral and legal responsibility to protect privacy rights as guaranteed by the Personal Data Protection Law. Failure to redact information can be classified as a violation of the principle of prudence in the management of public information. Therefore, stricter supervision and periodic evaluation of the decision publication mechanism are necessary to ensure that any published document does not cause harm to the parties that should be protected. The disclosure of personal information has the potential to cause negative impacts such as privacy violations, data misuse, and even social stigma for the individuals concerned. From the perspective of personal data protection law, this type of leak can be categorized as institutional negligence in maintaining the security and confidentiality of the data under its control. Although the publication of court decisions is a manifestation of the principles of public information disclosure and judicial transparency, these principles should be implemented in a manner that is balanced with the principle of personal data protection.

The leakage of personal data originating from the publication of civil court decisions has significant legal implications for the responsibility of judicial institutions as data controllers. Based on the provisions of the Personal Data Protection Law, every party that controls or processes personal data is obliged to guarantee data security and prevent unauthorized access or disclosure. Thus, if judicial institutions fail to redact data that should be kept confidential, such actions can be categorized as administrative negligence that could potentially lead to legal consequences. Such negligence not only undermines public trust in judicial institutions but can also be considered contrary to the principles of *lawful processing* and *accountability* as stipulated in the PDP Law. The legal implications of personal data leaks originating from judicial decisions published in the Decision Directory can also impact the legitimacy of applying the principle of public information disclosure in the judicial environment. If not balanced with strong protection mechanisms, disclosure can shift to become a threat to individual rights. Therefore, there is a need for a more stringent internal policy of the Supreme Court in applying standards for obscuring personal data, including periodic evaluations of the decision publication system used in the Decision Directory. With these steps, the judiciary will not only fulfill its constitutional obligation to be open to the public, but also fulfill its legal and moral responsibility to protect the fundamental rights of citizens.

CONCLUSION

The extensive disclosure of personal data in court decisions has consequences for personal data protection, particularly when these decisions are published online through a decision directory. Therefore, an in-depth analysis is needed to determine the extent to which formal obligations in the drafting of decisions can be harmonized with the principles of personal data protection, especially in the context of public information disclosure in the judicial environment. SK KMA 2-144 is still not optimal in terms of providing legal protection for the personal data of the parties involved in the case because SK KMA 2-144 does not clearly and specifically state what types of personal data should be obscured in published decisions. In addition to the types of personal data, the types of cases are also still very limited by the Supreme Court, according to the author. The provisions in SK KMA 2-144 for criminal cases only regulate the obscuring of data on victims and other witnesses in certain cases. In addition, the obscuring of the identities of judges, court clerks, public prosecutors, investigators, witnesses, and experts is also limited to cases of terrorism and children in conflict with the law. Furthermore, for civil cases, the obscuring of the identities of the parties to the case, witnesses, and related parties is also limited to marriage cases and other cases arising from marriage disputes, child adoption, wills and civil matters, religious civil matters, and state administrative matters which, according to the law, are conducted in closed court. The leakage of data belonging to parties to a case through a judge's decision can be categorized as a violation of personal data misuse because even though a judge's decision is a legal product categorized as public information, violations of the privacy rights of parties to a case should not be ignored, especially by a judicial institution. Therefore, the Supreme Court needs to prioritize the protection of personal data as an important principle in line with judicial transparency, especially in criminal cases that are closely related to human dignity.

REFERENCES

Anggara, Supriyadi Widodo Eddyono, Wahyudi Djafar, *Menyeimbangkan Hak:Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia*, Institute for Criminal Justice Reform.

Danrivanto Budhijanto, *Hukum Pelindungan Data Pribadi Di Indonesia Cyberlaw & Cybersecurity*, Bandung:PT Refika Aditama, 2023.

Dhoni Martien, Perlindungan Hukum Data Pribadi, Mitra Ilmu:2023

Endah Dewi Nawangsasi Sukarton, *Perlindungan Privacy Era New Normal Digital Lifestyle Terkait Cyber Power*,2022, Bandung:PT Refika Aditama

Lembaga Kajian & Advokasi Independensi Peradilan Simetri Publik dan Privasi Menyeimbangkan Pelindungan Data Pribadi dan Keterbukaan Informasi Publik Dalam Publikasi Putusan Pengadilan, 2025

Nenny Rianarizkiwati, Kebebasan Informasi versus Hak Atas Privasi Tanggung Jawab Negara dalam Perlindungan Data Pribadi, 2022

Putusan Pengadilan Negeri Donggala Nomor 140/Pid.Sus/2023/PN Dgl Tanggal 14 September 2023

Putusan Pengadilan Agama Tigaraksa Nomor 762/Pdt.P/2025/PA.Tgrs Tanggal 6 Oktober 2025

Putusan PN Bulukamba Nomor 213/Pdt.P/2025/PN Blk Tanggal 16 September 2025

Putusan PN Denpasar ENNYNomor 430/Pdt.G/2025/PN Dps Tanggal 4 Juni 2025

Shinta Dewi, Cyberlaw "*Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional,* Bandung: PT Refika Aditama, 2022.

Surat Keputusan Ketua Mahkamah Agung Nomor 2-144/KMA/SK/VIII/2022 tentang Standar Pelayanan Informasi Publik di Pengadilan

Undang-Undang Dasar Tahun 1945 Hasil Perubahan

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik

Universal Declaration of Human Rights (UDHR)