The Legal Problems of Deleting Prisoner Records from the Prison System after Release

Nidawan Pawcsuntorn

Faculty of Law, Rangsit University, Pathum Thani, Thailand
E-mail: nidawan.p@rsu.ac.th

Abstract

From the theoretical perspective of data privacy and the right to erasure, this paper explores the legal issues surrounding the deletion of prisoners' information from the prison system upon their release. The analytical-descriptive methods of documentary research were utilized to examine ideas, theories, laws, court rulings, practices, foreign laws and regulations, and international standards.

The result shows no legal provision imposes specific requirements on the prison system to carry out data erasure in practice. As such, inmates' records stay inside the penal system and are likely to be utilized or shared. This has serious implications for ex-offenders, such as employment discrimination and racism and hinders their efforts to reintegrate into society. The result of the research also suggests further revisions to the Corrections Act B.E. 2560, including the removal of prisoners' records from the system within five years of their release.

Keywords**:** *Data privacy, Prisoners' data, Right to erasure*

1. Introduction

Theoretically, prisoners retain the human rights and dignity provided by the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, such as the right to defend against arbitrary arrest or detention and the prohibition against cruel, inhuman, or degrading treatment or punishment. Prisoners are entitled to other basic rights and freedoms, including privacy, family life, freedom of expression and religious practice, access to an attorney, correspondence, etc. Moreover, the penitentiary environment is restrictive and far apart from the perceptions of the general public and society. Nonetheless, the state must promote the rights and liberties of prisoners, a fundamental principle of a free society (Gilmour, 2019). This paper argues that, among the various prisoner rights, the rights of the individual must be safeguarded by removing prisoner data from the correctional service following their release. This concept is based on the preservation of inmates' data privacy. Prison administration must gather inmates' data in accordance with the prison's goal, which is to enforce jail terms and develop convicts' habits through rehabilitation and punishment programs, including preparing prisoners for reintegration into society (Department of Corrections, 2017). The correctional system collects a wide range of information about convicts from time of their admission until their release. Consequently, prisoner files may contain not only a prisoner's criminal record but also the data on identifications, fingerprints, warrant information, authorizing admission, medical records, behaviors, etc., as outlined in Rule 7, 8 of the United Nations Standard Minimum Rules for the Treatment of Prisoners (United Nations, 2015).

Despite the legal provisions that protect the rights and dignity of prisoners, it is likely that inmates' rights are violated. According to Leila Zerrougi, Chair/Rapporteur of the United Nations Working Group on Arbitrary Detention, the importance of prisoner data lies in the fact that justice cannot be ensured without precise written information regarding an individual's imprisonment (United Nations, 2008). The European Court of Human Rights rules that admission to detention must be properly recorded to ensure the fundamental rights of the person according to Article 5 of the European Convention on Human Rights (ECHR) (El-Masri v. the former Yugoslav Republic of Macedonia [GC], 2012, § 233) (European Court of Human Rights, 2022). The prisoner record is also a tool for examining detention in light of human rights. For instance, prisoner medical records can likely identify the physical state and the possibility of abuse. It also indicates the performance of correctional services; according to a United Nations assessment, roughly 44,000 Nigerian prisoners (3.7% of all prisoners) are still incarcerated due to the loss of prisoner file records (United Nations, 2006).

Published online: Copyright © 2016-2023 Rangsit University

Failure to delete prisoners' information after their release might have negative consequences if the information is used or revealed in a deceptive manner. For instance, if a former prisoner's criminal history ends up in the hands of would-be employers, creditors, or the community in which they reside, without sympathy, it can lead to job discrimination and racism, undermine former prisoners' efforts to reintegrate into the workforce and society, and likely result in their return to prison (Squitieri, 2016). Thus, a law protecting inmates' personal information while they are confined in prisons and after their release is urgently required. A systematic approach for managing prisoner files in correctional facilities can prevent data breaches during incarceration.

This article investigates the current status of Thai laws pertaining to the protection of prisoners' rights regarding post-incarceration data records. In addition, it suggests a means to improve the laws if they are unfavorable.

Current laws on the protection of prisoners' rights in this area are still ineffective and must be revised. The Official Information Act B.E. 2540 governs the protection of inmates' personal information because the Personal Data Protection Act B.E. 2562 (Article 4) exempts prisoner data utilized in the judicial system and the Corrections Act B.E. 2560 (Article 36) outlines the procedures for prisoner data collecting in prisons. Unfortunately, such Acts lack the measure of data deletion upon the release of convicts. This paper proposes that Thailand should have legal and correctional system-appropriate regulations for erasing former inmates' jail records. Hence, the Department of Corrections, as the data keeper, will be able to be responsible for the deletion of data at the proper time. As data subjects, former prisoners can defend their data privacy rights in accordance with international standards and boost their potential to successfully reintegrate into society upon release from jail.

2. Objectives

This study is limited to the personal data of prisoners held by the Thai Ministry of Justice and does not include the data of prisoners held by private individuals or other companies,

1) Review the theoretical concepts of deleting prisoners' personal data from the prison system in international standards and foreign laws and regulations.

2) Analyze the legal problems of deleting the personal data of prisoners from the penitentiary system after release from prison in Thailand.

3) Recommend legal measures for the deletion of personal data of prisoners from the penitentiary system after release from prison for Thai authorities.

3. Materials and methods

The methodology of the study is a document review using analytical-descriptive methods, examining concepts, theories, laws, court judgments, and practices related to the protection of prisoners' personal data. Four categories of documents will be examined: 1) International standards; United Nations, European Union laws and regulations, and European Court of Human Rights decisions related to the deletion of prisoners' personal data. 2) Foreign laws; the Federal Republic of Germany, the United Kingdom. Commonwealth of Australia (Victoria), and Canada 3) Thai laws; Official Information Act B.E. 2540 and Personal Data Protection Act B.E. 2562 and laws related to the Thai penitentiary system, including Corrections Act B.E. 2560 and related regulations 4) Other relevant laws and documents such as books, textbooks, academic articles, electronic media, etc. The study relies on the international standard as a theoretical guideline for the design of laws and generally suggests a way to improve Thai laws.

The study on data protection of prisoners is based on four foreign laws: 1) The Federal Republic of Germany recognizes and protects the rights of prisoners under the civil law system. It is also the pioneer country and has significantly influenced data protection law in Europe. The German Prison Act contains provisions for the protection of prisoners' data. 2) The United Kingdom, which unlike Germany is governed by the common law system, protects prisoners' data through the UK's General Data Protection Regulation (UKGDPR) and Data Protection Act 2018, the application of the European Union’s General Data Protection Regulation (GDPR). UKGDPR, similar to GDPR, governs private and government data, and plays an

Published online: Copyright © 2016-2023 Rangsit University

important role as a model for global data protection law. In addition, the UK Prison Service Instructions and Regulations are important as they provide the essential details for protecting prisoner data held and managed by the UK Prison Service. 3) The Commonwealth of Australia (Victoria), which is subject to the common law system, is relevant to the protection of prisoners' rights and also provides protection of prisoner data under the Victoria Corrections Law. 4) Canada, unlike these countries, is a mixed law system that guarantees prisoner data protections under the Corrections and Conditional Release Act and Regulations.

4. Results and discussion

4.1 Theoretical concepts of protecting prisoners' personal information: The deletion of prisoners' data from the penitentiary system after their release from prison according to international standards is:

4.1.1 The United Nations Standard Minimum Rules for the Treatment of Prisoners (SMRs) (United Nations, 2015) embraces the concept of protecting prisoners' personal data in many ways. For example, they state that all prisoner records must be kept confidential and made available only to those whose professional duties require access to such records. Each prisoner shall be granted access to the files (Rule 9, SMRs). It is also proposed that the United Nations Handbook on the Management of Prisoner Files detail data collection procedures, categories of data, the purpose of prisoners' personal information, and measures to protect prisoners' data. Although the United Nations rules are not legally binding, they are an international standard that member countries such as Thailand have adopted and enforce as domestic laws (Schwebel, 1979).

The rules provide for the retention of "inactive files," such as information on released prisoners or those who died while in custody. In addition, member states are proposed to establish protocols for archiving prisoner files by specifying the length of time such data may be archived and/or destroyed. However, in the absence of state laws, prisons should have regulations or specific procedures for the retention of such files separate from the active records of the prisoners' detention (United Nations, 2008).

4.1.2 The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) provides for the protection of the personal data of EU citizens and ensures the free flow of information between its members. The GDPR covers "processing," which is "any operation or set of operations which is performed upon personal data or on a set of personal data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." The GDPR also applies to all public and private sectors that process data in the EU, as well as those that hold the personal data of EU citizens, whether they are based inside or outside the EU, including those that offer goods or services in the EU. Data processing is governed by seven principles: 1) lawfulness, fairness, and transparency, 2) purpose limitation, 3) data minimization, 4) accuracy, 5) storage limitation, 6) integrity and confidentiality, and 7) Accountability (Articles 3-5, GDPR).

Under the GDPR, when the Department of Corrections processes prisoner data, it follows the principles and "storage limitation," which means that "data shall be kept no longer than is necessary for the purposes for which the personal data are processed; personal data may be kept longer provided that the personal data are processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes." (Article,5, 89, GDPR).

More importantly, the GDPR states that the "right to erasure" or the "right to be forgotten" is the right of data subjects, such as former prisoners, to request the erasure of personal data concerning them when that data no longer needs to be collected. The data controller is then responsible for deleting this data without delay, following appropriate procedures, and taking into account the technical and technological measures in place and the cost of implementation. This includes removing the link or copies or prohibiting any reproduction of this personal data of the data subject (Articles 14-21, GDPR). Before this concept was codified, however, it was debated for a long time in Europe as part of a broad new proposed data protection and the extension of data privacy rights (Rosen, 2012).

4.1.3 European Union law, Directive (EU) 2016/680 or the Police and Criminal Justice Authority Directive (LED) protects personal data as the principles set forth in the GDPR, but LED includes specific purposes for crime prevention. LED classifies personal data into four categories, namely (1) the person who

Published online: Copyright © 2016-2023 Rangsit University

committed or believes he or she committed the crime, (2) those convicted of a crime, (3) the victim, and (4) those involved in the crime.

Similar to the GDPR, LED requires states to provide reasonable time limits for the deletion of personal data or periodic review of the need to retain personal data. Procedural measures must ensure that these time limits are met (Article 5, LED). It also establishes the right to the erasure of personal data and restriction of the processing (Article 16, LED).

4.2. The concepts of protection of personal data of prisoners and the measures of erasure after the release of prisoners of the United Kingdom, the Federal Republic of Germany, Canada, the Commonwealth of Australia (Victoria), and Thailand.

Table 1 Comparison of the measures of prisoners' personal data protection and the erasure of prisoners' personal data after prison release.

	Prisoners' data protection	**Prisoner's personal data deleting measures**
United Kingdom. (Data Protection Act 2018.) Prison Service Instruction (PSI 04/2018).	Protection in the processing of prisoners' personal data. (Section 25, SCHEDULE 1).	Right to Erasure. (Section 47) (GDPR application). Deleting of prisoners' data 6 years from the termination or release for determinate sentences or 99 years from the date of birth of lifers. (PSI 04/2018).
Federal Republic of Germany (The Prison Law 1976).	Protection in collecting, using, and processing prisoners' personal data. (Section 179-187).	Deleting of Prisoners' data after 2 years of the release. (Section 184).
Canada (Corrections and Conditional Release Act (S.C. 1992, c. 20).	Protection in disclosure of prisoners' personal data to victims, third parties, etc. (Section 26).	N/A
Commonwealth of Australia (Victoria) (The Corrections Act 1986).	Protection in disclosure of prisoners' personal data. (Section 104ZY).	N/A
Thailand (the Corrections Act B.E. 2560).	N/A	N/A On the admission into prison, the prison authority shall register the prisoner's records with at least the following details: (1) the prisoner's first and surname, identification number, or identification document, (2) the offense, (3) the fingerprint record or the person's identity, (4) the physical and mental condition, knowledge and abilities… (Section 36).
Thailand (The Official Information Act B.E. 2540.	Protection in use, collecting, and disclosure of prisoners' personal data. (Section 24).	providing for a personal information system only insofar as it is relevant to and necessary for the achievement of the objectives of the operation of the State agency, and terminating the provision thereof whenever it becomes unnecessary. (Section 23).

Published online: Copyright © 2016-2023 Rangsit University

	Prisoners' data protection	Prisoner's personal data deleting measures
Thailand (Personal Data Protection Act B.E.2562).	Prisoner data used in the judicial system is exempted from the Act.	Providing a process to delete or destruction of personal data when the retention period expires. (Section 37). Right to Erasure (Section 33).

According to Table 1: The study shows that:

4.2.1 Two significant legal models for the protection of prisoners' personal data can be traced in the legal systems: First, the Federal Republic of Germany, Canada, and the Commonwealth of Australia (Victoria) protect prisoners' data under the Prison Act. Second, the United Kingdom and Thailand protect prisoners' personal data under general law or comprehensive law (under data protection law). However, unlike these countries, the United States has privacy laws for specific areas, such as the Children's Online Privacy Protection Act of 1998 (COPPA) and the Electronic Communications Privacy Act of 1986 (ECPA).

In addition, the Data Protection Act 2018 of the United Kingdom and the Personal Data Protection Act B.E.2562 of Thailand recognize the concept of data subjects' right to erasure, while the Canadian Prison Service Act and the Commonwealth of Australia (Victoria) Act do not. However, in contrast to these laws, the Prison Service Act 1976 of the Federal Republic of Germany and the Prison Regulation of the United Kingdom (PSI 04/2018) provide that correctional institutions (public task) delete prisoners' data upon their release.

4.2.2 The Prison Act, 1976 of the Federal Republic of Germany regulates the different deletion of personal data stored in computer files and paper files. Computer files must be deleted no later than two years after the prisoner's release. Information on the prisoner's surname, first name, maiden name, date of birth, place of birth, date of entry, and date of discharge is exempt from this requirement if this is necessary to locate the prisoner's personal file. However, the paper files may be transmitted or used until the expiration of two years after the prisoner's release only if this is indispensable. Personal data in paper files may be transmitted or used until the expiration of two years after the prisoner's release only if this is indispensable for the prosecution of criminal offenses, for conducting scientific research projects, for remedying an existing lack of evidence, for establishing, asserting or averting legal claims in connection with the execution of a prison sentence (Section 184, The Prison Act, 1976).

In contrast to the Federal Republic of Germany, the United Kingdom's Prison Service Instruction (PSI 04/2018) requires the deletion of prisoner data 6 years after completion or release for certain sentences or 99 years after the date of birth for lifers. However, it leaves out the arguments regarding the legally binding nature and status of PSI, including other documents issued by the Prison Service such as Prison rules, orders and regulations, etc. More importantly, given the massive detail of prison management in such documents, it is not clear whether prisoners can compel the agency to violate its legal obligations under these rules and regulations. Courts also reflect the problem differently and ambiguously-one holding that the rules have the power, the other holding that such rules are a directive to prison administrators without enforcing the law. (Loucks, 2000).

4.3 The legal problem of deleting prisoner data from the penitentiary system after release from prison in Thailand.

4.3.1 The Official Information Act B.E. 2540 defines prisoner data as "Personal Data" protected under Article 4 of the Official Information Act B.E. 2540 (Official Information Board Decision No. 59/ 2564, 171/2563,35/2564) and specifies that the Authority shall delete the data when it has achieved its objectives and it is necessary (Article 23, Official Information Act B.E. 2540). However, the deletion of prisoners' data lacks specific provisions and regulations to put this into practice, such as the deletion procedure and the end of the collection of such data.

Nevertheless, Official Information Decision No. 59/ 2564 denies the former prisoner the deletion of the criminal file (of the court verdict) from the Royal Thai Police data system because such data is no longer needed. The Board argues that under Article 25(3) of the Act (Right to rectification) provides that the data subject may request the deletion of his or her data only if the data is inaccurate. Thus, if the court judgment

Published online: Copyright © 2016-2023 Rangsit University

remains correct, it cannot be deleted from the system (Official Information Commission, 2021). However, the decision avoids mentioning Article 23 when such data arise out of necessity. As a result, the former prisoner still carries the stigma and label of a criminal record after his sentence ends.

4.3.2 Article 36 of the Corrections Act B.E. 2560, which specifies the functions and administration of the penitentiary system, mandates that prisoners' data must be gathered from the day of admission to prison until the conclusion of the sentence or the day of release. On the day of admission, the following information is collected: identifying information, fingerprints, photographs, criminal history, sentence, physical and mental health, etc. During incarceration, data is compiled about convicts' activities, as well as their behavior, personalized rehabilitation and correctional plans, medical records, and prison education. Unfortunately, the statute does not include procedures for the destruction of data upon a prisoner's release.

This study recommends that the Corrections Act B.E. 2560 be amended by including a provision on the deletion of data after the prisoner's release in the last paragraph of Article 36 of the Law: "Personal data of prisoners shall be deleted no later than five years after release," similar to the concept of the Law on the Prison Law 1976 of the Federal Republic of Germany. There is no need to maintain prisoner data in the system after five years, as it is assumed that if former inmates have not committed any crimes during that period, they are probably nice people and there is no reason to keep their information in the system.

It is the responsibility of the correctional service to delete the data (public task). However, the former detainee retains the right to erase any non-essential material collected and stored. Hence, the former prisoners' data, including criminal and other pertinent records, remain private. The method can prevent privacy abuses, reduce recidivism, and assist formerly incarcerated individuals in returning to society, pursuing employment, and caring for themselves without returning to prison. It also adheres to the data protection principle outlined in international standards such as SMRs, GDPR, and LED.

5. Conclusion

It is also crucial to delete the outdated prisoner records, particularly, the sensitive data. The use and disclosure of such data can have severe repercussions for inmates, particularly after their release. Sensitive data of prisoners, such as criminal records, must be handled with utmost care to ensure the privacy and protection of inmates' rights. The appropriate management and disposal of these records are essential to prevent any potential harm or discrimination against them. Ignoring addressing these issues risks denying them the chance to integrate into society as human beings. The Thai prison system should adopt this method as well. However, Thai law does not already provide persons with these rights, therefore Article 36 should be amended to read: *"Personal data of prisoners shall be removed no later than five years following release."* By doing so, the Thai prison system can ensure that the personal information of prisoners is not used against them in any way. This will also promote transparency and accountability within the system, ultimately leading to a more just and fair society where individuals' privacy rights are protected.

6. Acknowledgements

This work was supervised by Prof. Banjerd Singkaneti, Dr. jur. (National Institution of Development of Administration) and Assistant Professor Thanee Vorapatr, Ph.D. (Rangsit University). Prof. Vicha Mahakun, Dean of the Faculty of Law, Rangsit University, provided insightful and critical feedback on this article.

7. References

Victorian Registration. (2022). *Corrections Act 1986 of Victoria Government (Australia).* Retrieved January 14, 2023, from https://content.legislation.vic.gov.au/sites/default/files/2023-03/86-117aa159-authorised.pdf.

Department of Corrections Ministry of Justice, Thailand. (2017). *Corrections Acts B.E. 2560.* Retrieved January 14, 2023, from http://en.correct.go.th/information-statistics/information/corrections-act/.

Government of Canada. (1992). *Corrections and Conditional Release Act (S.C. 1992, c. 20) of Canada.* Retrieved January 14, 2023, from https://laws-lois.justice.gc.ca/eng/acts/c-44.6/.

Published online: Copyright © 2016-2023 Rangsit University

UK Registration. (2018). *Data Protection Act 2018 of United Kingdom.* Retrieved January 14, 2023, from https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

Department of Corrections Ministry of Justice, Thailand. (2017). *Mission and Authority of the Department of Corrections*. Retrieved January 14, 2023, from http://www.correct.go.th/brr/index.php/th/2017-08-09-14-29-30/2017-08-09-14-29-34.

European Court of Human Rights. (2022). *Guide on case-law of the convention-prisoners' rights*. Retrieved November 18, 2023, from https://www.echr.coe.int/Documents/Guide_Prisoners_rights_ENG.pdf.

Gilmour, A. (2019). *The Nelson Mandela rules: Protecting the rights of persons deprived of liberty*. Retrieved June 14, 2022, from https://www.un.org/en/un-chronicle/nelson-mandela-rules-protecting-rights-persons-deprived-liberty.

Loucks, N. (2000). *Prison Rules: A Working Guide*. London: Prison Reform Trust.

Ministry of Digital Economy and Society. (2019). *Personal Data Protection Act. B.E. 2562.* Retrieved January 14, 2023, from https://www.mdes.go.th/law/detail/3577-Personal-Data-Protection-Act-B-E--2562--2019

Federal Ministry of Justice, Germany. (1976). *Prison Act 1976 of The Federal Republic of Germany.* Retrieved January 14, 2023, from https://www.gesetze-im-internet.de/englisch_stvollzg/englisch_stvollzg.html

GOV.UK. (2018). *PSI 04/2018 (AI 03/2018-PI 02/2018) Records, Information management and retention policy*. Retrieved September 16, 2021, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/895486/psi-04-2018-records-information-management-retention-policy.pdf.

The Official Information Commission. (2021). *Decision No. 59/ 2564, 171/2563,35/2564.* Retrieved January 14, 2023, from http://www.oic.go.th.

The Official Information Commission. (1997). *The Official Information Act B.E. 2540.* Retrieved January 14, 2023, from https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=16045&filename=index.

Rosen, J. (2012). The right to be forgotten. *Stanford Law Review. 64*, 89. Retrieved April 20, 2021, from https://review.law.stanford.edu/wp-content/uploads/sites/3/2012/02/64-SLRO-88.pdf.

Schwebel, S. M. (1979). The Effect of Resolutions of the U.N. General Assembly on Customary International Law. *Proceedings of the Annual Meeting (American Society of International Law), 73, 301-309*. https://doi.org/10.2307/25658015

Squitieri, C. (2016). Data privacy and inmate recidivism. *Virginia Law Review Online*, 102, 104-107. https://www.virginialawreview.org/articles/data-privacy-and-inmate-recidivism/.

Intersoft Consulting. (2016). *The General Data Protection Regulation (EU) 2016/679) (GDPR).* Retrieved January 14, 2023, from https://gdpr-info.eu/.

EUR-Lex. (2016). *The Directive (EU) 2016/680, the Police and Criminal Justice Authority Directive (LED).* Retrieved January 14, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680.

United Nations Special Rapporteur on Extrajudicial. (2006). *Summary and arbitrary execution mission to Nigeria*. United Nations document E/CN.4/2006/53/Add.4. Retrieved April 18, 2021, from https://documents-dds-ny.un.org/doc/UNDOC/GEN/G06/106/40/PDF/G0610640.pdf?OpenElement.

United Nations. (2015). T*he United Nations standard minimum rules for the treatment of prisoners (the Nelson Mandela rules).* Retrieved January 14, 2023, from https://www.unodc.org/documents/justice-and-prison-reform/Nelson_Mandela_Rules-E-ebook.pdf.

United Nations. (2008). *Handbook on Prisoner File Management.* New York: United Nations Publication.

Published online: Copyright © 2016-2023 Rangsit University