LEGAL PROTECTION ASPECTS OF BANK CUSTOMER DATA FOR CYBERCRIME PREVENTION

Kuspriliani Sari[1], Endang Sutrisno[2], Sanusi[3]
[1)] BJB, Indonesia
[23)] Master of Laws Study Program, Swadaya Gunung Jati University
Email: mrs.leany999@ymail.com

DOI: https://doi.org/10.33603/hermeneutika.v10i2.11314
Diterima: 01 April 2026; Direvisi:3 May 2026; Dipublikasikan: 02 Agustus 2020

Abstract. *The development of digital technology has driven the transformation of banking services towards an increasingly electronically integrated system. (Andi Prastowo, 2022). However, this progress is accompanied by an increased risk of cybercrime that threatens customers' personal data. (Indonesia Cybersecurity Annual Report 2023). This study aims to analyze the legal protection aspects of bank customer data in the digital banking system and assess the effectiveness of applicable regulations in preventing cybercrime. (Sinta Dewi Rosadi, 2022). This study uses a normative juridical method with a statutory approach, a conceptual approach, and a case approach. (Peter Mahmud Marzuki, 20219). The legal materials analyzed include the Banking Law, the latest Electronic Information and Transactions (ITE) Law, the Personal Data Protection (PDP) Law, OJK regulations, and several decisions and cases of banking data leaks. (Financial Services Authority, 2022). The research findings indicate that despite the existence of a regulatory framework, gaps in norms, overlapping authority, and weak oversight mechanisms remain, hindering optimal legal protection (Ahmad M. Ramli, 2021). Furthermore, cybersecurity practices in banking institutions do not fully meet adequate data protection standards, thus opening up opportunities for breaches, phishing, skimming, and other forms of cybercrime. This research emphasizes the importance of regulatory harmonization, improved information security, and strengthened law enforcement to ensure the protection of bank customer data in the digital era (Lawrence M. Friedman, 1975).*

Keywords: legal protection; customer data; digital banking; cybercrime; personal data protection.

I. Introduction

Banks, as part of a country's financial and payment system, play a crucial role. This crucial role is inseparable from their function as financial intermediaries, specifically those engaged in fundraising and lending activities (Kasmir, 2019). To foster public trust, banks must maintain confidentiality of client data and information (Hermansyah, 2014). In the banking sector, this is crucial for customer satisfaction and maintaining their trust. However, recently, many have complained about offers of financial products, such as insurance and additional credit cards, sent via text message or phone call. Often, they claim to be in partnership with banks, raising questions about the

possibility of banks handing over consumers' personal data to third parties without their permission. (OJK, 2022) This situation raises concerns about data security, which is vulnerable to misuse by certain individuals.

Threats to data security have emerged along with the development of information technology. These threats have led to the emergence of cybercrimes such as fraud, hacking, data tapping, email spam, and data manipulation through computer programs to access other people's data (BSSN, 2023). Furthermore, unscrupulous bankers frequently disclose customer data by selling it to various parties, including criminals who can break into accounts (Sinta Dewi Rosadi, 2021). Despite continuous advancements in security technology, hackers are still able to access and steal customer data. This situation further emphasizes the importance of customer data protection. Therefore, meaningful efforts are needed to protect customer data to prevent customer data theft and mitigate any leaks. (Dani Pandu, 2022).

Based on the principle of confidentiality, which requires banks to safeguard consumers' financial data and personal information, banks must commit to protecting customer interests. (Law No. 10 of 1998). Law No. 27 of 2022 concerning Personal Data Protection regulates confidentiality. Personal data protection is crucial because personal data breaches, both material and non-material, can endanger the public and legal entities. Regarding fraud, it is regulated in Article 378 of the Criminal Code, including fraud for profit, which carries a penalty of up to 4 years in prison. Although the Criminal Code does not specifically regulate online fraud, laws related to information technology are regulated in Law No. 11 of 2008 concerning the Electronic Information and Transactions (ITE) and revised in Law No. 19 of 2016. However, the ITE Law does not specifically mention the word "fraud" in its articles. Even in the latest law, namely Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number I1 of 2008 concerning Electronic Information and Transactions, "fraud" is not explicitly mentioned.

Although it does not explicitly discuss fraud, Articles 27 and 28 of the Republic of Indonesia Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions regulate the dissemination of electronic information containing content that violates morality, gambling, hatred, or fake news.

II. Research methods

1. Types of research

This research is a normative juridical legal research, namely research that focuses on the study of positive legal norms, legal principles, and legal doctrines related to the protection of bank customer data and efforts to prevent cybercrime. (Peter Mahmud Marzuki, 2019). Normative juridical research is used because the issues studied are related to the analysis of laws and regulations and their suitability to the needs of personal data protection in the digital era. (Soerjono Soekanto and Sri Mamudji, 2015). This normative research is relevant for identifying strengths, weaknesses, and legal gaps in customer data protection regulations, thereby formulating effective legal improvement recommendations (Philipus M. Hadjon, 1987).

2. Research Approach

To provide a comprehensive understanding of the legal problems studied, this study uses several approaches:

a. Statute Approach

Used to review regulations governing the protection of personal data and banking systems, including:

- Law Number 10 of 1998 concerning Banking;
- Law Number 11 of 2008 in conjunction with Law Number 1 of 2024 concerning ITE;
- Law Number 27 of 2022 concerning Personal Data Protection (PDP);
- OJK regulations regarding consumer protection and information technology security;
- BSSN regulations regarding cybersecurity.

This approach allows for analysis of legal norms, principles of legality, and the effectiveness of regulations in protecting customer data.

b. Conceptual Approach

Digunakan untuk memahami konsep inti seperti:

- legal protection;
- personal data and privacy;
- banking secrecy;
- information security (cybersecurity);
- cybercrime;
- legal responsibility of banking institutions.

Legal theories such as Legal Protection Theory, Friedman's Legal System Theory, Rawls's Theory of Justice, and Responsive Legal Theory are used to strengthen the analytical framework.

c. Case Approach

Functions to analyze data leak cases and cybercrime involving banking services, such as:

- BSI ransomware attack case (2023);
- BRI Life data leak;
- account hacking cases through phishing and skimming;
- data misuse incidents by internal parties.

Case analysis helps understand the application of law in practice as well as obstacles to law enforcement.

d. **Comparative Approach**

Used to compare international data protection models such as:

- EU GDPR
- Singapore GDPR
- *Cybersecurity Law China*

This approach provides best practices for policy improvement recommendations in Indonesia.

3. Sources and Types of Legal Materials

The research uses secondary data, including:

a. Primary Legal Materials

- Laws;
- Government regulations;
- OJK regulations; Bank Indonesia circulars;
- BSSN regulations;
- Court decisions regarding cybercrime and data breaches;

b. Secondary Legal Materials
- Books on banking law, cyber law, and personal data protection
- National and international journal articles
- Official reports from institutions (OJK, BSSN, BI)
- Legal expert opinions (doctrine)

c. Tertiary Legal Materials
- Legal Dictionary
- Encyclopedia
- Other Supporting Sources

4. Legal Material Collection Techniques

Collection of legal materials is carried out through library research, namely:

a. Researching regulations related to banking and data protection.
b. Reviewing relevant academic literature.
c. Collecting court decisions related to cybercrime.
d. Reviewing reports of banking data breach incidents.
e. Reviewing official documents issued by relevant authorities.

5. Legal Material Analysis Techniques

Analysis of legal materials is carried out using descriptive-analytical methods and deductive reasoning, through:

a. Descriptive-Analytical Analysis
Explain applicable regulations and analyze their suitability to customer data protection needs.

b. Interpretative Analysis
Using legal interpretation:
- grammatical (based on the text)
- systematic (in the entire legal system)teleological (based on the purpose of the law)

c. Deductive Reasoning
Conclusions are drawn from:
- Major premise: legal norms
- Minor premise: facts (data breach cases)
- Conclusion: legal protection analysis

This approach ensures that legal arguments are logical and consistent.

6. Research Flow

The research stages include:

a. Problem identification and formulation
b. Inventory and collection of legal materials
c. Analysis of legal regulations and theories
d. Case analysis and legal comparison
e. Preparation of findings and conclusions

This flow ensures that research is conducted systematically and methodologically.

III. Results and Discussion

Banks that can cause losses. However, for clarity, a comprehensive review is needed, and the law is necessary because customer data protection involves activities that use information technology. As the law concerns the use of information technology, Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions needs to be used as a reference so that it can become a legal umbrella to provide legal protection for victims whose data is threatened due to online activities or cybercrime. (Law of the Republic of Indonesia No. 1 of 2024).

Regarding consumer data protection, law enforcement demands firm legal certainty so that the law can be implemented correctly. (Satjipto Rahardjo, 2006). One of the main objectives of the law is to provide legal certainty so that every legal action can be carried out clearly and can be accounted for. (Hans Kelsen, 1961). Conversely, if a legal action lacks certainty, this can trigger various polemics that are difficult to prevent in society. Therefore, in an effort to provide legal certainty and also its implications for legal protection for customers, a comprehensive review is needed to describe existing laws and regulations. (Peter Mahmud Marzuki, 2019). In this case, the main focus of the review is the Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions. This is because Law of the Republic of Indonesia Number 1 of 2024 contains values that regulate online activities, making it a suitable legal basis for addressing cybercrime, including online fraud and customer data protection (Ahmad M. Ramli, 2021). In other words, the law can be used to handle cases related to customer data protection and to handle leaked customer data (Sinta Dewi Rosadi, 2021).

On the other hand, the law does not specifically regulate fraud or customer data protection (Law No. 1 of 2024). This means a comprehensive review is needed to address these aspects. Examining Law No. 11 of 2008 concerning Electronic Information and Transactions, it can be stated that there are still legal loopholes, particularly in articles related to cyberporn, online gambling, defamation, extortion, the spread of fake news, and online provocation (H. Yudhi Setyawan, 2021). These gaps create obstacles in its implementation, where law enforcement is often less thorough and less proportional in applying the articles governing these prohibited acts (SAFEnet, 2023). Therefore, an in-depth review is needed to determine whether the latest law is able to close the legal loopholes in the previous regulation. This effort aims to ensure that Law of the Republic of Indonesia No. 1 of 2024 can provide legal certainty and legal protection, particularly in the aspect of customer data protection (ELSAM, 2024).

An important aspect to consider is that cybercrime activities such as customer data theft or online fraud certainly involve information technology. This could mean that the use of general articles governing fraud, such as the Criminal Code, is insufficient. Considering the use of media as a means of committing criminal activity, the latest Law of the Republic of Indonesia Number 1 of 2024 is the relevant law to regulate such activities, making it appropriate to refer to it. However, as explained, the law does not explicitly regulate online fraud or data leaks to defraud customers. Therefore, there are obstacles to the use of this law, requiring a legal review to fully understand it so that the law functions as a legal umbrella to provide legal certainty and protection. Normative legal certainty occurs when a regulation is drafted clearly and logically, thus providing definite rules. Meanwhile, protection is the right

of every citizen and the obligation of the state to provide protection for the community (Soerjono Soekanto, 2017).

A data breach at Bank Syariah Indonesia (BSI) occurred on May 8, 2023, when all digital services were disrupted for four days due to a ransomware attack by the LockBit 3.0 group. This attack resulted in the copying and encryption of customer data and passwords prior to the incident. Many customers complained of lost funds, highlighting the weaknesses in BSI's security systems. This incident highlights the importance of protecting customer data amidst increasing cyber threats to the banking sector.

A data breach at Bank Syariah Indonesia (BSI) occurred on May 8, 2023, when all digital services were disrupted for four days due to a ransomware attack by the LockBit 3.0 group. This attack resulted in the copying and encryption of customer data and passwords from prior to the incident. Many customers complained of lost funds, highlighting the weaknesses in BSI's security systems. This case highlights the importance of protecting customer data amidst increasing cyber threats to the banking sector. Such data breaches are typically caused by organized cyberattacks, internal breaches of security protocols, or negligence in information management. In addition to the risks of data breaches, such as identity theft, fraud, and financial abuse, such incidents can undermine customer trust and significantly tarnish a banking institution's reputation. Data breaches are a very serious issue because they can have various detrimental consequences for both banking institutions and customers.

In addition to the BSI case, several data breaches have also occurred in other financial sectors. In July 2021, hackers claimed to have the data of two million customers and hundreds of thousands of documents from PT Asuransi BRI Life, which they claimed originated from the BRI Life Syariah system. In October 2021, 378 GB of data belonging to Bank Jatim containing customer and employee information was sold on an illegal forum, although the bank stated that its core systems remained secure. Meanwhile, the fintech platform Cermati.com was also hacked, resulting in the leak of approximately 2.9 million user accounts, including personal data such as addresses and income. Furthermore, in early July 2024, a claim was made on the BreachForums forum by the account NexusxHaxor, who claimed to have compromised the data of 370,000 Bank Tabungan Negara (BTN) customers. However, BTN denied the allegations and assured that customer data remains secure and protected by an integrated information technology security system.

In March 2023, Mandiri Sekuritas experienced a data breach due to a ransomware attack by the LockBit group, which targeted the company's internal systems. While the exact size of the leaked data was not disclosed, this incident highlighted cybersecurity vulnerabilities in the Indonesian financial sector. Meanwhile, Bank Mandiri itself had not reported any customer data breaches as of the end of 2023, as stated in its Sustainability Report. In early 2022, Bank Indonesia (BI) experienced a cyberattack by the Conti ransomware group, resulting in the breach of more than 52,000 documents totaling 74.82 GB of data. This incident highlighted the need to improve the protection of the country's strategic data, in accordance with the provisions of Government Regulation No. 71 of 2019 and BSSN Regulation No. 8 of 2020. The Institute for Policy Research and Advocacy (Elsam) emphasized the importance of a thorough investigation and the implementation of stricter cybersecurity standards to prevent similar incidents in the future.

In April 2024, there was an alleged leak of Bank SulutGo (BSG) customer account transaction data involving information on the disbursement of funds from a collaboration between the media and the Minahasa Communication and Information Agency (Diskominfo). The data, which should be confidential and accessible only to authorized parties such as the

Supreme Audit Agency (BPK) or internal bank personnel, was allegedly leaked through the involvement of BSG internal personnel. Several aggrieved customers demanded a thorough investigation and accountability for this privacy violation. A 25-year-old woman named Dewi Rahmawati reported that her personal data was used without permission by the HR department of the company where she had previously applied to open a job, to open a BNI Bank account and register it for an online loan service (pinjol) with transactions reaching Rp10 million. BNI stated that it had investigated the case and emphasized that opening an account without the customer's physical presence was not in accordance with their official procedures. The case revealed the misuse of personal data by irresponsible parties and demonstrated the serious risk of customer data leaks due to the actions of employees who exploit data access for personal or other purposes.

This data breach phenomenon demonstrates the gap between das sollen (normative ideality), the legal regulations mandating the protection of personal data, and dasein (reality), or the reality on the ground, which demonstrates the failure to effectively implement such protection. The validity of a legal system needs to be compared with the reality on the ground to determine how well it is enforced. Various regulations are available, such as Law Number 10 of 1998 concerning Banking, Law Number 27 of 2022 concerning Personal Data Protection, and Law Number 1 of 2024 concerning the second amendment to the Electronic Information and Transactions (ITE) Law. However, legal loopholes and multiple interpretations remain, preventing optimal legal protection for customers. For example, although the ITE Law covers online activities, its articles are not explicitly stated (Hans Kelsen, 1967).

IV. Conclusion and Suggestions

Conclusion

This research shows that legal protection of bank customer data in the face of cybercrime threats still faces various challenges, including regulatory, implementation, and oversight. Although Indonesia has a legal framework in place, including the Banking Law, the Electronic Information and Transactions (ITE) Law, the Personal Data Protection Law, and regulations from the Financial Services Authority (OJK) and the National Cyber and Cyber Security Agency (BSSN), these regulations are not fully capable of addressing the complexity of cyberattacks and the increasing risk of data breaches in digital banking services. Fragmented norms, inconsistent regulations, weak implementation of information security standards, and low customer digital literacy contribute to the high potential for personal data misuse and cybercrime.

Furthermore, banks' legal protection practices are suboptimal, particularly in terms of prevention, early detection, and response to data breaches. Several cases of data breaches and account breaches demonstrate persistent weaknesses in information technology infrastructure, limited oversight mechanisms, and unclear legal accountability when incidents occur. Therefore, protecting bank customer data requires a more integrated, responsive, and adaptive legal approach to the dynamics of digital technology and increasingly sophisticated cyber threats.

Suggestion

1. Strengthening Regulation and Legal Harmonization
   The government needs to harmonize regulations in the Banking Law, the Electronic Information and Transactions (ITE) Law, and the Personal Data Protection Law to avoid overlapping or legal gaps. Harmonization is necessary to ensure that definitions

of personal data, security standards, and legal accountability mechanisms are clearer, more consistent, and can be implemented effectively.

2. Improving Cybersecurity Standardization in Banking
   Banks need to implement higher information security standards, such as zero trust security, end-to-end encryption, regular security audits, AI-based cyberthreat detection, and multi-layered authentication systems. Compliance with OJK and BSSN standards must be strengthened as a form of preventative legal protection.
3. Strengthening the Role of OJK, BI, and BSSN
   Oversight agencies need to improve their capacity for monitoring, enforcing compliance, and investigating data breach incidents. Coordination between agencies must be strengthened to ensure swift, targeted monitoring and incident handling, and adherence to national cybersecurity standards.
4. Improving Customer Digital Literacy
   Banks need to regularly conduct cybersecurity education, including anti-phishing, anti-skimming, and digital device security campaigns. Data protection depends not only on the bank as the data controller, but also on the safe behavior of customers as data owners.
5. Developing Stronger Accountability Mechanisms
6. The government and banking institutions need to ensure clear mechanisms for compensation, investigation, and customer recovery in the event of a data breach. Transparency in handling data breaches must be strengthened through mandatory and measurable data breach notification.
7. Strengthening Law Enforcement against Cybercrime

Law enforcement officials need to improve their competency in digital forensics, cyber intelligence, and cybercrime investigation to ensure effective legal proceedings. Firm action will have a deterrent effect and increase public trust. (Sinta Dewi Rosadi, 2021).

V. Bibliography

Adams, Bradley J. 2003. Establishing personal identification based on specific patterns of missing, filled, and unrestored teeth. Journal of Forensic Sciences.

Ahern, Mike, et al. 2005. Disaster Victim Identification in Mass Fatalities. Australian Journal of Emergency Management.

Aldridge, J. 2017. "Forensic Odontology in Mass Disaster Scenarios: Review of International Practice." Forensic Research & Criminology International Journal.

Alley, R. et al. 2010. The Use of Dental Records in Postmortem Identification: A Global Review. London: Academic Press.

Anderson, M. 2019. "Disaster Governance and Multi-Agency Coordination." International Journal of Disaster Risk Reduction.

APHA (American Public Health Association). 2018. Public Health Response to Mass Fatality Incidents. Washington, DC.

Bentham, Jeremy. 1907. An Introduction to the Principles of Morals and Legislation. Oxford: Clarendon Press.

Berketa, J. 2019. "Dental Modifications and Identification." Journal of Forensic Odontology.

Black, Sue, and Adrian Aggrawal. 2020. Forensic Science: A Very Short Introduction. Oxford University Press.

Bloom, S. 2020. “The Role of Health Systems in Mass Fatality Management.” Health Security Journal.
Brake, S. 2021. Postmortem Forensic Procedures in Disaster Medicine. Cambridge University Press.
Carter, J. and Williamson, M. 2016. Forensic Odontology in Mass Disasters. New York: Springer.
Cattaneo, C. 2015. “Forensic Anthropology and DVI in Global Disasters.” Forensic Science International.
Center for Disaster Philanthropy. 2022. Disaster Trends Worldwide.
Challener, E. 2018. Strengthening Identification Systems in Low-Resource Countries. WHO.
Davis, R., et al. 2019. “Dental Evidence in Human Identification.” Journal of Forensic and Legal Medicine.
DVI Standing Committee. 2018. Disaster Victim Identification Guidebook. Geneva.
Dyke, M. 2015. Mass Fatalities: Managing the Response. CRC Press.
Ellingham, S. 2015. “Global DVI Casework and Emerging Challenges.” Australian Journal of Forensic Sciences.
Enos, W. 2001. Forensic Dental Evidence: Identification and Bite Marks. CRC Press.
Federal Bureau of Investigation (FBI). 2017. Disaster Victim Identification: Technical Procedures.
Fong, K. 2020. “Health Facility Preparedness in Mass Casualty Incidents.” Global Health Research.
Frank, C. 2021. “Dental Resilience to Extreme Conditions.” International Journal of Dental Research.
Gustafson, G. 1966. Age Determination on Teeth. Basel: Karger.
Grajales, G. 2019. “The Role of Dental Charting in Modern DVI.” Forensic Science Review.
Hale, G. 2018. Odontograms: Practice and Standardization. London: Elsevier.
Harding, J. 2021. “Mass Fatality Identification Gaps in Southeast Asia.” Asia-Pacific Forensic Review.
Hinchliffe, J. 2010. Forensic Odontology: An Essential Guide. Wiley-Blackwell.
Hughes, T. 2019. “Challenges to DVI in Developing Nations.” Journal of Homeland Security and Emergency Management.
Hyde, R. 2013. Forensic Dentistry. Oxford University Press.
ICRC (International Committee of the Red Cross). 2019. Management of the Dead after Disasters: A Field Manual.
Interpol. 2018. Disaster Victim Identification Guide. Lyon: Interpol General Secretariat.
Interpol. 2020. DVI Best Practice Manual. Lyon.
Johnson, R. et al. 2021. “Odontological Identification in Burned Bodies.” Forensic Science International: Reports.
Jones, B. 2016. Mass Disaster Forensics. Cambridge University Press.
Kaplan, A. 2020. “Health and Human Rights in Disaster Contexts.” Human Rights Quarterly.
Kieser, J.A. 2013. Forensic Odontology: Principles and Practice. Springer.
Kirk, S. 2019. “Odontogram Integration into National Electronic Health Systems.” Global Health Informatics Review.
Larsen, C. 2019. “The Importance of Antemortem Dental Records.” Dental Traumatology Journal.
Levin, P. 2017. Human Identification: Theory and Practice. CRC Press.
Logan, J. 2014. Practical Forensic Odontology. Wiley.

MacDonald, C. 2017. “Teeth as Resilient Identifiers in Extreme Events.” Journal of Anatomy.
Macho, G. 2019. “Dental Morphology and Variation in Identification.” International Journal of Morphology.
Madhusudan, N. 2020. “Odontology in Large-Scale Disasters.” Clinical Forensic Odontology.
Martinez, P. 2018. Global Challenges in DVI. Routledge.
Matsumoto, H. 2015. “Identification Challenges in Tsunami Victims.” Forensic Science International.
McGivern, H. 2019. Disaster Medicine Essentials. Elsevier.
Morgan, O. 2006. “Mass Fatality Management.” WHO Technical Note.
Nathanson, P. 2016. “Dental Autopsy Methods.” Journal of Forensic Dental Sciences.
Ngugi, D. 2020. “Limitations of Identification in Low-Resource Settings.” Global Forensic Studies Journal.
OECD. 2019. Disaster Risk Governance: Policy Framework.
O’Donnell, C. 2018. “Postmortem Dental Examination Standards.” Australian Forensic Journal.
Omar, R. 2021. “Digital Odontogram Systems: A Review.” Health Informatics International.
Pillay, A. 2020. Forensic Odontology for the Modern World. CRC Press.
Ponnusamy, S. 2018. “Odontogram Accuracy and DVI Efficiency.” Journal of Forensic Odontology.
Pringle, R. 2021. Disaster Science and Identification. Cambridge University Press.
Rao, A. 2016. “Teeth as Tools for Human Identification.” Forensic Research Journal.
Reesu, G. 2015. “Role of Forensic Odontology in Mass Disasters.” Journal of Forensic and Legal Medicine.
Richards, G. 2007. Identification of Human Remains. Totowa: Humana Press.
Ritchie, L. 2018. Disaster Governance: Social and Legal Dimensions. Routledge.
Senn, D. and Paul Stimson. 2010. Forensic Dentistry. CRC Press.
Silva, R. 2020. “International DVI Protocol Developments.” Global Forensic Science Review.
Smith, J. 2022. Mass Fatality Forensic Operations. Elsevier.
Stauffer, S. 2019. “Resilience of Dental Structures Postmortem.” Journal of Dental Research.
Sulaiman, A. 2021. “Management of Dead Bodies in Emergencies.” WHO Eastern Mediterranean Health Journal.
Swift, B. 2018. Handbook of Disaster Victim Identification. New York: Springer.
Taylor, K. 2019. “Odontological Challenges in Burn Cases.” Burns Journal.
Thompson, T. and Black, S. 2006. Forensic Human Identification. CRC Press.
Turk, J. 2018. “Global DVI Standards and Verification.” International Forensic Review.
United Nations. 2015. Sendai Framework for Disaster Risk Reduction 2015–2030. UNDRR.
Vanderkolk, J. 2020. Forensic Human Identification Methods. Elsevier.
Vining, B. 2022. “Electronic Dental Records in Mass Disasters.” Forensic Informatics Review.
Warren, M. 2017. “Dental Profiling in Mass Casualty Incidents.” Journal of Forensic Sciences.
WHO. 2014. Management of Dead Bodies after Disasters: Field Manual.

WHO. 2021. Disaster Preparedness and Response in Health Systems.
Williams, G. 2018. “Human Dignity and Rights after Death.” Journal of Law and Bioethics.
Zanini, P. 2017. “Odontometric Variability in Identification.” Anthropological Review.
Zhang, T. 2020. “Digital DVI Systems and Forensic Integration.” International Journal of Disaster Response.