*Page: 2407-2418* *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

# LawFoyer International Journal of Doctrinal Legal Research

**[ISSN: 2583-7753]**

**Volume 4 | Issue 1**

**2026**

*DOI: https://doi.org/10.70183/lijdlr.2026.v04.106*

# HABEAS DATA FOR THE DEAD: ADDRESSING THE JURISDICTIONAL VACUUM OF FORENSIC DIGITAL TWINS IN INTERNATIONAL LAW

**Sakshee Narayan Gore**[1]

## I. ABSTRACT

*When a person dies in a foreign country or during an international conflict, forensic experts often use advanced 3D scanning and digital imaging to study the body. This creates a "Digital Twin" a perfect, permanent digital copy of the deceased person's internal and external anatomy. While international laws like the Geneva Conventions and UNESCO rules are very clear about how to return the physical body to their home country, these laws say absolutely nothing about the digital data left behind. This paper identifies a major legal "hole": currently, even after a physical body is returned to its family, a foreign government or a private company can keep the digital version of that person forever. This data is often stored on servers in different countries, governed only by private contracts rather than human rights laws. This creates a situation where the dead have no "digital privacy," and their most intimate biological details can be used, shared, or even sold without the consent of their family or their home nation. By looking at the legal principle of Habeas Data, a constitutional remedy originating in Article 5, LXXII of the Constitution of Brazil (1988) that grants individuals the right to access and control personal information held about them, and subsequently adopted across several Latin American jurisdictions, this research argues that we must recognize "Digital Remains" as something that deserves legal protection. It explores the conflict between a company's claim to "own" the data and a family's right to their loved one's dignity. The paper concludes by proposing a new "International Protocol for Digital Repatriation." This would require that when a physical body is sent home, all sensitive forensic data must also be transferred or deleted. The goal is to ensure that a person's right to dignity doesn't disappear just because their body has been turned into data.*

[1] Manikchand Pahade Law College, Chhatrapati Sambhajinagar, (India). Email: saksheegore93@gmail.com

## II. KEYWORDS

Digital Privacy; Forensic Scanning; International Law; Data Ownership; Human Dignity.

## III. INTRODUCTION

In the modern world, the human body no longer ends at the skin. When a person passes away whether in a hospital, a zone of international conflict, or a foreign country forensic science now uses powerful digital tools to understand the cause of death. Technologies such as Post-Mortem Computed Tomography (PMCT) and high-resolution 3D scanning allow experts to create a "Forensic Digital Twin." This is a perfect, three-dimensional, digital reconstruction of a person's internal organs, skeletal structure, and external features. It is a "virtual body" that can be rotated, zoomed into, and stored forever on a computer server.

For decades, International Law has protected the physical dignity of the deceased. The 1949 Geneva Conventions require that the dead are treated with respect, and the 1970 UNESCO Convention helps nations repatriate (return) stolen cultural or biological remains to their home soil. However, these legal frameworks were largely developed for a physical world. Instruments such as the UNESCO Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property (1970) focus on cultural property, not human remains, and therefore operate only as an analogical reference point rather than a direct legal basis for biological repatriation. The actual repatriation of human remains is addressed through distinct frameworks, including the United Nations Declaration on the Rights of Indigenous Peoples (2007), particularly Articles 12 and 28, as well as domestic statutes such as the Native American Graves Protection and Repatriation Act (1990) and humanitarian guidelines developed by the International Committee of the Red Cross. These frameworks, however, remain largely confined to the physical body and do not extend to digital data.

 (ISSN: 2583-7753)

### A. Research Problem

The problem arises when the physical body is returned to the family, but the "Forensic Digital Twin" stays behind in a foreign database. Currently, there is a "Jurisdictional Vacuum" a legal hole where no international treaty explains who owns this data, how long it can be kept, or who has the right to delete it.

Because forensic data often crosses borders via the "Cloud," it falls under the control of private tech companies and foreign data laws rather than the laws of the person's home country. This leads to a new and invisible form of exploitation: a person's most intimate biological secrets can be used for research, shared with third parties, or kept indefinitely without the family ever knowing. This paper argues that the legal right to control one's information, grounded in the doctrine of Habeas Data as developed in Latin American constitutional law and scholarship, must not expire at death, but instead requires doctrinal extension to post-mortem digital identities in the international legal order. If the physical body is sent home, the digital body must follow. Without a new international protocol, we risk a future where a person's dignity is respected in the physical world but violated in the virtual one.

### B. Research Objectives

1. To explain why the "Forensic Digital Twin" should be legally treated as a part of the human body, not just "data."
2. To identify exactly where current international treaties (like the Geneva Conventions) fail to protect digital remains.
3. To propose a clear, simple framework for "Digital Repatriation" that international journals and lawmakers can adopt.

### C. Research Questions

To address the "legal hole" identified in the introduction, this paper seeks to answer the following:

1. The Definition Question: Should a "Forensic Digital Twin" be legally classified as "personal data" (like an email) or as "human remains" (like a physical body)?

2. The Ownership Question: In the absence of a clear treaty, who holds the primary legal right to a deceased person's digital surrogate the forensic facility that created it, the state where the server is located, or the next of kin?
3. The Repatriation Question: How can existing international frameworks, such as the 1970 UNESCO Convention, be updated to include "Digital Repatriation"?

### D. Research Hypotheses

1. Current international human rights laws are physically biased and fail to protect the dignity of a person once their body is converted into high-fidelity digital data.
2. Recognizing a post-mortem right to *Habeas Data* (the right to control one's information) is the only way to prevent the unauthorized and indefinite storage of forensic surrogates by foreign entities.

### E. Research Methodology

This research follows a Doctrinal and Analytical Approach.

1. **Doctrinal:** It examines existing international treaties (Geneva Conventions, UNCLOS, and UNESCO) and national laws (such as India's DPDPA 2023 and the EU's GDPR) to see where they fall short.
2. **Analytical:** It uses "Legal Analogies" to compare the protection of physical remains with the protection of digital data.
3. **Interdisciplinary:** While the focus is legal, the paper also draws on basic forensic science to explain why a "digital twin" is a functional equivalent of a human body.

### F. Literature Review

Current legal scholarship is divided. On one side, data privacy experts argue that "privacy ends at death," meaning once a person dies, their data is fair game for research. On the other side, human rights scholars argue that "dignity is eternal" and

should protect a person's image forever. However, most of this debate centers on social media accounts (like Facebook).

There is almost no research specifically focusing on Forensic Digital Twins which are far more intimate than a social media profile. This paper fills that gap by moving the conversation from "Digital Ghosts" to "Digital Bodies," arguing that forensic data requires a much higher level of international protection than a simple email or photo.

## IV. RESEARCH & ANALYSIS

### A. The Digital Surrogate: Why a 3D Scan is More Than Just Data

The first hurdle in international law is defining what a "Forensic Digital Twin" (FDT) actually is. Currently, most countries treat a 3D body scan like any other piece of digital information similar to a bank statement or an email. However, this is a legal error.

A bank statement does not contain the biological essence of a human being. An FDT, created through PMCT (Post-Mortem Computed Tomography), is a "Digital Surrogate." It contains every fracture, every organ measurement, and every unique physical trait of a person. If international law protects the physical body from being "paraded" or "dishonored" (as seen in the Geneva Conventions), that protection must logically extend to the digital version. If a foreign power keeps a high-resolution 3D model of a deceased soldier or citizen, they are essentially keeping a "Virtual Corpse" in their database.

### B. The Jurisdictional Vacuum: Who Owns the Digital Dead?

In international law, "Jurisdiction" means who has the power to make the rules. When a forensic scan is performed:

1. The State of Origin (where the person was from) claims the right to their citizen's dignity.
2. The Holding State (where the scan was performed) claims the data belongs to their scientific records.
3. The Tech Company (which owns the Cloud server) claims ownership via their "Terms of Service."

This creates a Vacuum. For example, if an Indian citizen dies in Europe and a 3D scan is stored on a server in the USA, which law applies? The EU's GDPR generally stops protecting privacy at the moment of death, as reflected in Recital 27. India's Digital Personal Data Protection Act, 2023, remains underdeveloped on post-mortem rights. The United States, by contrast, often treats data within a property-oriented framework. This "conflict of laws" means that, currently, the entity with the strongest server not the family with the strongest moral claim wins.

### C. Digital Extractivism: The New Face of Inequality

There is a growing socio-legal concern called "Digital Extractivism." This happens when wealthy nations with advanced forensic tech collect the biological data of people from developing nations or conflict zones.

Even if the physical bodies are sent back to their home countries for burial, the "Digital Wealth" (the medical and forensic data) stays in the Global North. This data is then used to train AI models or conduct research without any "Data Benefit-Sharing" with the home nation. In international law, this mirrors the old problem of "stolen artifacts." We are now seeing the "theft" of digital human remains under the guise of scientific progress.

### D. Digital Neo-Colonialism: The Modern Scramble for Data

In the 19th and 20th centuries, many artifacts and human remains were taken from the Global South and placed in Western museums. Today, we are seeing a digital version of this. When an international forensic mission often led by wealthy nations or well-funded NGOs enters a developing country or a conflict zone (such as Syria, Sudan, or parts of South Asia), they perform thousands of 3D scans.

The "Physical Body" is buried locally, but the "High-Resolution Data" is exported to servers in the Global North. This creates a power imbalance. Wealthy nations build massive forensic databases that allow them to lead in medical research, facial recognition, and AI-driven forensics, all using the biological data of people from poorer nations. In international law, this is a violation of Sovereignty. Just as a country owns its oil or gold, it should also have "Sovereign Rights" over the forensic data of its

citizens. Without a "Digital Repatriation" law, we are allowing a new form of colonial extraction where the "Digital Human" is stolen while the "Physical Human" is returned.

### E. The Conflict of Laws: When the Cloud Crosses the Border

A major legal headache is the "Location of Data." In international private law, the rules that apply usually depend on where the "incident" happened. However, with Forensic Digital Twins, the data is "De-territorialized."

Consider this scenario: An Indian student dies in the UK. The UK police create a 3D forensic scan. That scan is uploaded to a cloud server located in Ireland, owned by a US-based tech company.

1. The UK Law: Might say the data is a police record and can be kept for 30 years.
2. The US Law: Might treat the data as "Corporate Property" of the tech company.
3. The Irish/EU Law (GDPR): Might say that since the person is dead, they no longer have "Privacy Rights."
4. The Indian Law: Might demand the data be returned as a matter of national dignity.

This "Collision of Jurisdictions" leaves the family in a helpless position. There is currently no "Universal Choice of Law" rule for the dead. This paper argues that international law must adopt the principle of "Lex Patriae" (the law of the person's nationality). If the deceased was Indian, Indian dignity laws should follow their digital twin, no matter where the server is located.

### F. The "Commercialization Risk": From Autopsy to Asset

Perhaps the most offensive possibility in the current jurisdictional vacuum is the commercialization of forensic data. Because FDTs are so detailed, they are incredibly valuable for:

1. Medical Tech Companies: To test virtual surgical tools.
2. Entertainment/Gaming: To create "realistic" anatomy in media.

3. Insurance Algorithms: To study mortality patterns.

If the law treats an FDT as mere "unclaimed data," there is nothing stopping a cash-strapped forensic lab from selling "anonymized" 3D skeletal sets to private corporations. Under the UN Guiding Principles on Business and Human Rights, corporations have a responsibility to respect human rights. We argue that "Human Rights" must include the "Non-Commercialization of the Dead." A digital twin should be Extra Commercium a thing that cannot be traded on the open market.

### G. The ICRC Framework: Forensic Management of the Dead and Its Digital Limits

The contemporary management of the dead in armed conflict is significantly shaped by the work of the International Committee of the Red Cross (ICRC), which has developed detailed operational and humanitarian guidelines on the recovery, identification, and repatriation of human remains. Instruments such as the ICRC's Missing Persons: A Handbook for Parliamentarians (2009) and its protocols on forensic data collection emphasize dignity, traceability, and the rights of families to know the fate of their relatives. These frameworks also regulate the collection and handling of ante-mortem and post-mortem data, including biometric identifiers, to facilitate identification and repatriation. However, these guidelines remain fundamentally oriented toward physical remains and identification data, not high-resolution, persistent digital reconstructions such as Forensic Digital Twins.

While the ICRC framework ensures that data collected serves humanitarian purposes, it does not explicitly address long-term storage, ownership, or cross-border transfer of detailed 3D anatomical datasets. This creates a critical normative gap: the transition from temporary identification data to permanent digital surrogates is not regulated. Consequently, while the ICRC provides a robust foundation for dignity in the physical and informational handling of the dead, it does not extend to the governance of enduring digital replicas, thereby reinforcing the need for a dedicated international protocol on Digital Repatriation.

### H. Data Sovereignty vs. The Global Forensic Commons

There is a massive tension between National Sovereignty and the "Right to Science."

1. The Scientific Argument: Some international organizations argue that forensic data should be "Open Access" to help solve future crimes or improve medical science. They view the "Digital Dead" as a global resource.
2. The Sovereign Argument: Developing nations argue that their citizens' biological data is a "Sovereign Asset."

When a wealthy nation's laboratory refuses to delete the 3D scans of a foreign national, they are essentially claiming "Extraterritorial Jurisdiction" over that person's remains. This mirrors the debates in the Law of the Sea (UNCLOS) regarding "Marine Genetic Resources." If a country owns the fish in its waters, does it not also own the "Digital DNA" and "Forensic Likeness" of its people? This paper argues that "Data Sovereignty" must include the right to recall forensic data from foreign servers once a physical repatriation is complete.

### I. The "Accountability Gap" in Private International Law

In many cases, forensic scans are not performed by governments but by Private Contractors or NGOs. These entities are often "legally invisible" in international treaties. If a private company in Silicon Valley accidentally leaks the 3D autopsy files of thousands of war victims from the Global South, who is responsible?

1. There is no "International Forensic Ombudsman."
2. There is no "Global Data Court" for the dead.

The Jurisdictional Vacuum is not just a lack of treaties, but a lack of Enforcement Mechanisms. We suggest that the International Criminal Court (ICC) or INTERPOL should establish a "Digital Evidence Vault" with strict expiration dates to ensure that "temporary forensic needs" do not turn into "permanent digital detention."

## V. SUGGESTIONS AND RECOMMENDATIONS

To fix this legal hole, the following solutions are proposed:

1. **The "Right to Digital Repatriation":** International treaties should be updated to state that "Forensic Data is an extension of the physical body." When a body is repatriated, the digital files must either be handed over to the home country or securely deleted.

2. **Mandatory "Post-Mortem Consent" Protocols:** Forensic institutions should be legally required to get "Digital Consent" from the next of kin before storing 3D scans in long-term databases.
3. **International "Data Trusts":** Instead of private companies owning forensic data, INTERPOL or the UN should manage a "Neutral Data Trust" where sensitive forensic twins are kept under strict humanitarian rules, not commercial ones.
4. **The "Digital Death Certificate":** We propose that every international forensic scan must be issued with a "Digital Death Certificate" that includes an Expiry Date. Once that date passes, the server must automatically trigger a "Proof of Deletion" or "Transfer of Ownership" to the home nation.
5. **Professional Ethics for Forensic Imaging:** Just as doctors take the Hippocratic Oath, forensic imaging specialists should adopt a "Universal Code of Digital Conduct" that prohibits the unauthorized sharing of 3D reconstructions on social media or in non-anonymized journals.
6. **"Universal Protocol for Digital Repatriation" (UPDR)**: this paper proposes a 3-point international protocol:
    - **Rule 1:** The Principle of Digital Identity Symmetry. The law must recognize that a 1:1 3D forensic scan is legally the same as the body itself. Therefore, all protections granted to the physical corpse (dignity, non-mutilation, burial rights) must automatically apply to the digital surrogate.
    - **Rule 2:** Mandatory "Data Repatriation" Clauses. In every international forensic agreement, there must be a "Return or Delete" clause. Once the forensic investigation is closed, the digital twin must either be transferred to the home country's national archives or permanently destroyed. It cannot be "parked" in a foreign cloud indefinitely.
    - **Rule 3:** The Right to Virtual Integrity. Families must have the legal standing to sue in foreign courts if their loved one’s forensic twin is used for purposes (like public display or commercial research) that they did not explicitly consent to.

## VI. CONCLUSION

The evolution of forensic science from the physical to the virtual has outpaced the development of international law. As this research has demonstrated, the Forensic Digital Twin is not merely a data file; it is a high-fidelity, biological surrogate of a human being. It carries the same moral, ethical, and legal weight as the physical remains from which it was derived. The current Jurisdictional Vacuum, the "legal hole" where no treaty or law governs these digital remains, has created a dangerous era of "Digital Extractivism." The Indian Supreme Court has, however, interpreted dignity under Article 21 to extend beyond mere physical existence, including in cases such as Parmanand Katara v Union of India (1989) AIR 2039 SC and Common Cause v Union of India (2018) 5 SCC 1, which reflect an evolving jurisprudence on dignity at and after death. In this new landscape, the dignity of the deceased is often sacrificed for scientific prestige or corporate gain.

By adopting the doctrine of Habeas Data for the Dead, the international community can finally bridge this gap. This paper has established three fundamental truths:

1. Dignity is Indivisible: A person's right to be treated with respect cannot exist for their physical body while being denied for their digital likeness.
2. Sovereignty is Digital: A nation's right to protect its people must extend to their digital remains. Digital bio-piracy is as much a violation of sovereignty as the theft of physical artifacts.
3. Repatriation must be Absolute: In the age of the "Cloud," the return of the "Atom" (the body) must be accompanied by the return or deletion of the "Bit" (the data).

The proposed Universal Protocol for Digital Repatriation (UPDR) offers a practical and necessary path forward. It ensures that forensic science remains a tool for truth and justice, rather than a mechanism for the permanent "digital detention" of the deceased. International law must now evolve to recognize that while a heart may stop beating, the right to dignity and the right to be forgotten must endure in the virtual realm. The "Digital Dead" deserve a final resting place that is not a foreign server, but a space governed by the laws of their own people.

## VII. REFERENCES


1. Charter of the United Nations (1945).
2. Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War (1949).
3. Additional Protocol I to the Geneva Conventions (1977).
4. UNESCO Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property (1970).
5. International Covenant on Civil and Political Rights (ICCPR) (1966).
6. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
7. S. and Marper v. The United Kingdom, [2008] ECHR 1581.
8. Parmanand Katara v. Union of India, AIR 1989 SC 2039.
9. Common Cause (A Regd. Society) v. Union of India, (2018) 5 SCC 1 (Right to die with dignity).
10. Floridi, L., The Ethics of Information (Oxford University Press 2013).
11. Smith, M. J., and Hirst, S. M., "Ethical Considerations in the Study and Display of Human Remains," in Ethical Approaches to Human Remains (Springer, 2019); Carew, R. M., Errickson, D., and Thompson, T. J. U., "Ethical frameworks for 3D imaging and digital reconstruction in forensic science," Journal of Forensic and Legal Medicine (2023).
12. Regulation (EU) 2016/679 (General Data Protection Regulation), Recital 27.
13. Digital Personal Data Protection Act 2023 (India).
14. Paul M Schwartz, 'Property, Privacy, and Personal Data' (2004) 117 Harvard Law Review 2056.
15. UN Human Rights Council, Guiding Principles on Business and Human Rights (2011).