International Journal of Law and Politics Studies
ISSN: 2709-0914
DOI: 10.32996/ijlps
Journal Homepage: www.al-kindipublisher.com/index.php/ijlps

IJLPS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Digital Twins and Legal Liability: Navigating Accountability in Simulated Realities

Md Wasim Ahmed[1] and Md Joshim Uddin[2]
[1]*Master's in Law, Green University Bangladesh*
[2]*Asa University of Bangladesh*
Corresponding Author: Md Wasim Ahmed, **E-mail**: ad.wasimahmed@gmail.com

| ABSTRACT
In this research protject, the focus is on how issues of responsibility are resolved when using digital twin technology within the United States. With digital twins playing a key role in healthcare, manufacturing and infrastructure, new problems concerning data integrity, cybersecurity, privacy and how reliable systems can operate tend to emerge. The paper describes the current legal situation, identifies important U.S. laws and relevant authorities and discusses the obstacles faced in the process of deciding who was at fault. The findings point out actual problems and solutions are suggested in terms of policies and technologies to close such gaps. Suggesting that comprehensive governance and a team approach are important, the study pushes for active laws, clear standards and creative improvements to make the use of digital twins safe and effective in significant industries.

| KEYWORDS
Digital twins, legal liability, data governance, cybersecurity, artificial intelligence, U.S. regulation, simulated environments

| ARTICLE INFORMATION
ACCEPTED: 01 November 2025 **PUBLISHED:** 26 November 2025 **DOI:** 10.32996/ijlps.2025.7.8.2

1.0 Introduction

1.1 Background

Digital twins are a groundbreaking phenomenon across disparate industries, revolutionizing how organizations handle design, upkeep, and operating efficacy (Singh & Tiwari, 2024). A digital twin refers to a digital replica of a physical object or a physical system, fueled by real-time data as well as smart analytics. This technology makes it possible to better comprehend complex systems, allowing organizations to optimize performance while reducing risks. The digital revolution brought about cutting-edge technologies that are transforming how industries function, innovate, and manage risk (Teller, 2021). At the top of this list are digital twins, a complex, data-driven virtual replica of physical assets, systems, or processes, encompassing the behavior, condition, and dynamics thereof. With organizations across sectors increasingly deploying Internet of Things (IoT) devices, cloud computing, and artificial intelligence (AI), digital twins have found themselves at the core of predictive analytics, operating efficiency, and strategic development. A *Gartner 2021 survey* found that 13% of organizations using IoT projects had previously applied digital twins, with modeled predictions assuming a fivefold increase by 2027 (Milosevic & Van Schalkwyk, 2023).

The U.S. Department of Energy (DOE) and the *National Aeronautics and Space Administration* (NASA) have been actively engaged in researching and applying digital twin models for infrastructure critical to U.S. security, aerospace systems, and nuclear reactors (Harris et al., 2024). The growing use of digital simulations, however, brings with it immense legal, ethical, and accountability implications—especially if digital twins are to impact real-time decision-making within critical, high-risk contexts. These in turn require a thorough appreciation of digital twins themselves, their scope of operations, and how they impact U.S. regulations and industry (Helbing & Sanchtez, 2023).

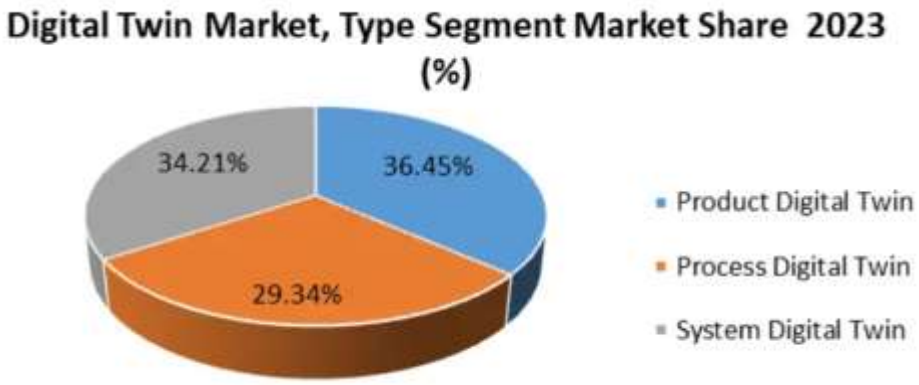

Figure 1: Visualizes Type Segment Market Share [Source: Maximize Market Research]

The above pie Chart illustrates market share distribution in terms of three major digital twin segments: Product Digital Twin, Process Digital Twin, and System Digital Twin. The data demonstrates that Product Digital Twins form the largest segment with a share of 36.45% in the market. This indicates a robust industry interest in simulation models of individual products, which are commonly utilized in product design, simulation, and predictive maintenance. The second largest segment by a close margin is System Digital Twin with a market share of 34.21% (MMR, 2024). This large percentage indicates ramping adoption of digital twins representing complete systems or systems-of-systems, crucial in complex infrastructures like intelligent grids, aircraft systems, and manufacturing facilities. The workflow simulation and operational processes are represented by Process Digital Twins with a share of 29.34% in the market (MMR, 2024). This reflects the need for efficiency in processes and ongoing optimization in business domains like oil and gas, logistics, and supply chain during production. The fairly even distribution in the three segments suggests the growing maturity of digital twin technology across applications, with the value being realized not only in product development but even in systemic and procedural optimization. The segmentation also points toward future diversified growth potentially being driven by holistic integration of AI and IoT technologies at different tiers of digital twin use cases.

2.0 Understanding Digital Twins

2.1 Definition and Overview

According to Mocanu & Sibony (2023), A digital twin refers to a dynamic, real-time virtual replica of a physical object or process to simulate, analyze, and optimize its real-world equivalent. Using data from embedded sensors, artificial intelligence software, and high-performance computing, this technology mimics physical assets in a virtual space. Emerging from simulations used by NASA for space missions in the early 2000s, digital twins have become potent diagnostics, lifecycle, and performance forecasting tools. In the United States, the National Institute of Standards and Technology (NIST) describes digital twins as part of cyber-physical systems while highlighting how they contribute to industry resilience, cybersecurity, and smart manufacturing through programs like the Smart Manufacturing Systems Design Hub (Milhai e al., 2022).

2.2 Applications of Digital Twins

Digital twins are being implemented across a broad spectrum of industries in the United States, each designed to address domain-specific challenges. In healthcare, for instance, patient-specific digital twins at the Mayo Clinic personalize patient care with tailored treatment plans and predict surgical outcomes. At *General Electric (GE)* in manufacturing, digital twins are used to track and optimize the performance of jet engines and turbines, leading to a conservative estimated 20% savings in maintenance costs and a 10% boost in uptime (Casas & Pi, 2024). The DOE uses digital twins in the energy industry to control electrical grid systems and simulate integration with renewable energy. Digital twins are applied in city-level urban planning projects in Chicago and New York to simulate traffic flow, energy use, and climate impact in real-time, informing more sustainable infrastructure development. Up to $1.3 trillion in economic value can be generated by digital twins by 2030, according to *McKinsey & Company*, with the U.S. likely to outstrip global investment in this area thanks to its superior digital infrastructure quality and strong innovation environment (Cellina et al., 2023).

According to Gore et al. (2025), the global digital twin market was valued at approximately USD 2.26 billion in 2017 and is expected to grow at a compound annual growth rate (CAGR) of 38.2% between 2018 and 2025. This anticipated expansion is largely driven by the increasing use of digital twin technology across various industries to optimize production layouts, boost

efficiency, and reduce operational expenses. Nechesov et al. (2025), indicated that the advancement of transformative technologies such as Artificial Intelligence (AI) and Machine Learning (ML) has significantly reshaped the digital twin landscape. In addition, the growing reliance on connected devices, high-speed internet, and cloud-based platforms across organizations has fueled the adoption of Internet of Things (IoT) solutions. As a result, demand for digital twin technologies continues to rise, supporting more effective and intelligent operational management.

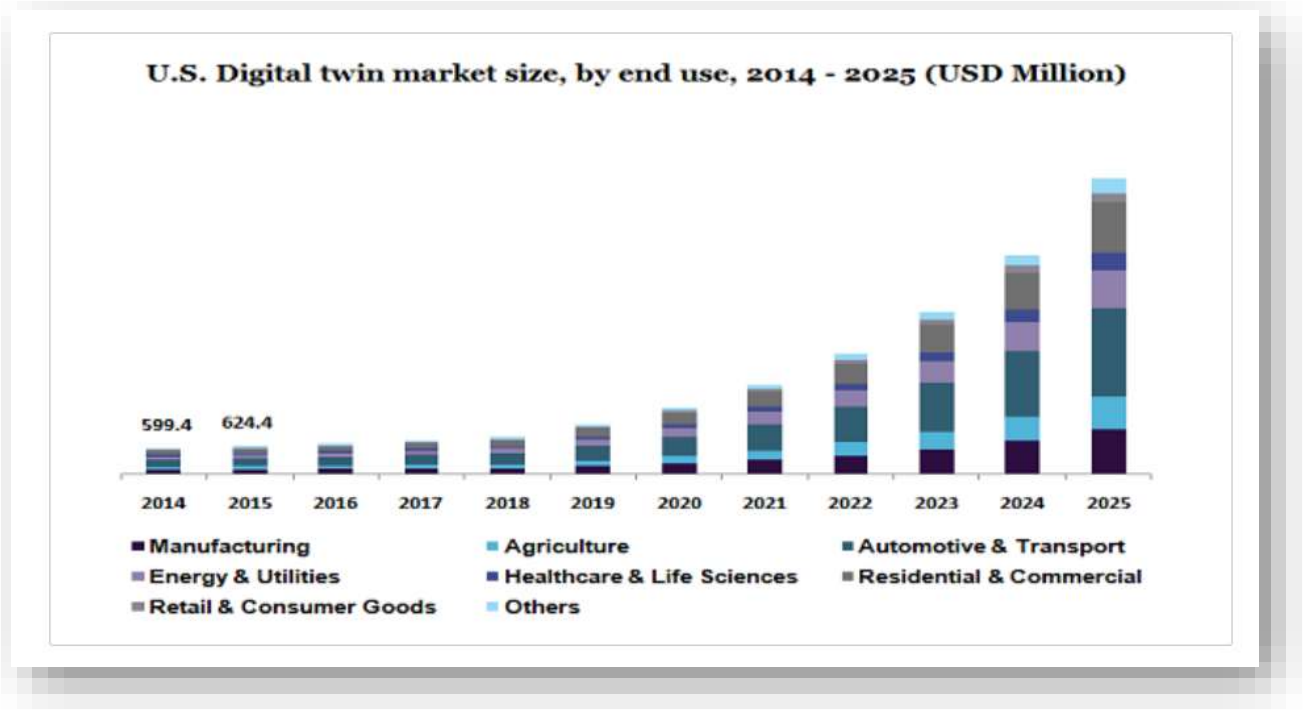

Figure 2: Digital Twins Market Trends [Sources: Million Insights]

The graph above shows exponential growth in multiple sectors embracing digital twins over an 11-year timeline. The market size stood at about $599.4 million in 2014, slightly increasing to $624.4 million in 2015. However, from 2018 onwards, a visible acceleration in growth can be observed, with increases year by year. The market for digital twins in the United States by 2025 can be expected to exceed $3 billion, demonstrating the sharply rising use of digital simulation technology. Of multiple end-use sectors, Automotive & Transport emerges as the leading contributor, closely followed by Healthcare & Life Sciences and Energy & Utilities, both of which have registered steep increases in investment and deployment. The Manufacturing segment, while having been part of it throughout since the start of this timeline, however, seems to depict incremental growth more slowly than newer verticals. Remarkably, Residential & Commercial and Retail & Consumer Goods start to contribute heavily from about 2020 onwards, demonstrating a market trend toward increased use of digital twins in smart buildings and customer journey optimization. This multiplicative sector expansion indicates how digital twin technology is becoming a building block technology across industry and mass market contexts. The post-2020 sharp growth can be explained at least partially by how digital transformation was speeded up by the COVID-19 pandemic, compelling industries to turn toward remote monitoring, predictive analytics, and real-world system modeling, to keep going during this time despite no physical presence. The graph indicates how digital twins are shaping up to be a central element in the U.S. digital economy, with deep implications for future policy, investment, liability regimes.

3. Legal Framework Surrounding Digital Twins

3.1 Current Legal Environment

Rathod et al. (2024), reported that the development of digital twin technology has accelerated in the United States ahead of the emergence of a parallel regulatory framework, leaving uncertainty regarding a framework for accountability, privacy, data management, and responsibility. Digital twins, which are based on real-time information drawn from physical assets, systems, or conditions, blur the distinction between simulated and real outcomes and pose a challenge to conventional legal responsibility. As of 2025, there remains no all-encompassing federal legislation addressing the usability or responsibility of the use of digital

twins. Rather, the legal framework today depends on a patchwork of unrelated statutes addressing the protection of information, intellectual property, cybersecurity, and product responsibility (Peldon et al., 2024).

The United States legal system tends to frame emerging technology through the umbrella of preexisting paradigms in the form of tort law, contract law, and standards of care. Where, for example, a predictive maintenance breakdown occurs and a digital twin model makes an erroneous projection regarding the performance of equipment—causing damage or loss—it becomes uncertain whose responsibility it would be: the software designer, the info vendor, or the end user who runs the system (Stapleton, 2022). It has been noted by legal scholars and institutions, including the Brookings Institution and the *American Bar Association (ABA),* to be of the utmost importance to introduce regulatory certainty in the near term, particularly since the application of digital twins increases in sectors of critical infrastructure, healthcare, and self-driving technology where mistakes result in significant damage (Vetrivel e al., 2024).

Zolick & Maisel (2023), asserted that liability is becoming an increasing worry, especially when digital twins assist in product simulations that shape real-world decisions. It can be hard to determine who is accountable for mistakes in a digital twin system which is why there should be precise risk and responsibility clauses in any contracts made. Moreover, the fact that simulation software and digital twin data belong to proprietary companies hinders data exchange and compatibility, supporting the aims of NIST to create security, trust, and compatibility for digital twins (Wang & Hurdon, 2021).

3.2 Pertinent Laws and Regulations

As per Singh & Tiwari (2024), to date, there is no specific legal framework dedicated to digital twins. However, existing data regulations, particularly the *General Data Protection Regulation* (GDPR), are applicable. Digital twins do not introduce unique challenges in this context; when personal data is processed, the obligations outlined by the GDPR come into play. While we will not cover all aspects of the GDPR, some key provisions are particularly relevant. Article 5 (Chapter 2) establishes a general framework that includes obligations such as transparency, fairness, reasonable data retention, and data accuracy. Articles 6 and 7 highlight the necessity of obtaining consent from data subjects for data processing, along with the right to withdraw this consent at any time. This consent is crucial, especially since Article 9 states that processing health data is generally prohibited unless the patient provides consent (Teller, 2021). Additionally, Article 17 of the GDPR ensures a right to erasure, allowing individuals to file complaints or seek legal remedies if they believe their rights have been infringed, as outlined in Chapter 8.

Yet another most pertinent is the *Health Insurance Portability and Accountability* Act (HIPAA) since digital twins are being employed in healthcare to model patients and simulate treatments. According to HIPAA, organizations are responsible for safeguarding all patient information used within the application of the digital twin to preclude breaches (Stapleton, 2022). Within the energy and utility industries, the *Federal Energy Regulatory Commission* (FERC) and the North *American Electric Reliability Corporation* (NERC) mandate cybersecurity requirements potentially extending to the digital twin models operating or simulating the management of the grid (Casas & Pi, 2024).

Moreover, the *National Institute of Standards and Technology* (NIST) has proposed a *Cyber-Physical Systems Framework* with guidance for risk management of the risks related to the simulation using digital twins (Gore et al., 2025). From the perspective of product liability, the law of defamation and torts applies to the use of digital twins in manufacturing and transport should a breakdown of the model cause damage in the real world. Yet, in the absence of a leading case law directly addressing the issue of digital twins, both corporations and regulatory bodies exist in a state of legal ambiguity, emphasizing the necessity for targeted laws and judicial interpretation (Cellina et al., 2023).

4. Legal Liability in the Context of Digital Twins

Harris et al. (2024), posited that legal liability when it comes to digital twins poses a multifaceted issue extending over various modes of legal responsibility to reflect the intricate interaction between tangible assets and their computational duplicates. Digital twins, which are interactive virtual representations mimicking tangible objects or systems, are being increasingly utilized for critical decision-making across industries ranging from healthcare to manufacturing and urban development. As per Helbing & Sanchez (2023), this increased usage increases the stakes for risk in the event of erroneous projections, defective simulation, or a data breach, and therefore calls for an accurate grasp of the forms of liability and sample case studies to navigate the new legal landscape.

4.1. Types of Liability

According to Milhai et al. (2022), liability for digital twins can be narrowed down into product liability, negligence, contractual liability, and intellectual property infringement. **Product liability** occurs when a digital twin, as part of the product life cycle, results in damage because of defects in design, simulation, or accuracy in its data. If, for instance, a digital twin employed in aerospace design predicts flawed stress tolerances resulting in physical failure, the manufacturer might be liable for damages.

Negligence claims are prevalent, particularly in the healthcare sector, where patient conditions are simulated by digital twins to inform treatment. It is tough for courts to apply conventional tort doctrine to these situations, notably establishing causation—that the error of the digital twin resulted in damage—and damages when damage transcends purely monetary damage, e.g., wrongful publication of genetic information (Milosevic & Van Shalkwyk, 2023). **Contractual liability** arises from contracts between entities participating in the creation, sharing, and consumption of digital twin information. Unclear definitions of data ownership, usage terms, and guarantees for data integrity can lead to defaults and disputes. **Liability for intellectual property** increases, as digital twins involve copyrighted material, proprietary algorithms, and trade secrets. High-profile lawsuits against AI systems for the unauthorized use of works protected by copyright emphasize the risks of copyright infringement and the importance of dispositive of clear data identification and consent in the creation of digital twins (Mocanu & Sibony, 2023).

4.2 Case Studies

Peldon et al. (2024), argued that while there are no legal precedents relating to digital twins, some real-world experiences give a glimpse into the approach courts and regulators might take to liability. One illustrative instance concerns *GE Aviation,* which employs digital twins to a significant extent to analyze jet engine performance. Back in 2019, a discrepancy in a predictive maintenance model raised worries over engine health analysis. Though no accident occurred, GE was put to an internal audit and regulatory examination by the *Federal Aviation Administration* (FAA) regulatory arm, demonstrating how variations in digital twin outputs lead to potential exposure to liability. A further instance concerns the healthcare field, where patient-specific digital twins are employed at the *Mayo Clinic* to predict the response to treatment (Rathod et al., 2024). Where a treatment plan drawn from a digital twin model creates adverse reactions, issues of liability may revolve around the appropriateness of the use of the digital twin, the precision of the data, and the inclusion of the use of the technology in the patient's informed consent. As digital twins increasingly become a part of safety-critical applications, these initial instances emphasize the requirement for new regulatory frameworks and guidance by the courts focused on the special risks entailed in simulated conditions (Nechesov et al., 2025).

A significant example of intellectual property liability includes copyright suits filed against AI firms including *GitHub Copilot and Stability AI* for allegedly utilizing third-party copyrighted code and images improperly and without permission. Although these matters are not specifically about digital twins, they highlight the potential legal risk when third-party information is used for digital models without permission, a situation that has a close relationship with the creators of digital twins who depend on enormous sets of information for model training (Singh & Tiwari, 2024). Challenges in healthcare arise when digital twins are used in patient treatment. It has been challenging for courts to make solid claims of liability when a digital twin model collapses and when patient information is inappropriately released since conventional tort and contract law tend to be inadequate to manage these new types of harm (Stapleton, 2022).

Lastly, in industrial contexts, the United Kingdom government's support toward intricate digital twins to simulate infrastructure and population behavior lets loose the potential for disputes over data ownership and responsibility for action taken based on a digital twin projection, requiring the importance of solid contractual schemes and models of liability. Overall, these cases collectively confirm that it is not just about technical precision, but rather the moral use of the information, transparency, and solid legal contracts (Vetrivel et al., 2024).

5. Challenges in Accountability Establishment

5.1 Technical Challenges

Zoltick & Maisel (2023), reported that a major technical challenge is the quality and interoperability of the data. Digital twins rely on real-time information from sensors, internet of Things (IoT) devices, and legacy systems, which tend to be plagued by inaccuracies, inconsistencies, or gaps. Low-quality data can result in erroneous simulations: Gartner puts the annual value of bad data to U.S. organizations at $12.9 million, with the ripple effects in industries such as healthcare (e.g., incorrect risk predictions about patients) and manufacturing (e.g., unjustified equipment upkeep). Wang & Hurdon (2021), highlighted that interoperability problems further complicate the issue of responsibility since digital twins often combine different systems with incompatible protocols or formats. Industrial digital twins, for instance, can struggle to correlate information from proprietary software and cloud platforms, creating fragmented results. The GAO finds the current network backbone of the United States lacking the bandwidth and latency tolerance necessary for large-scale digital twins, especially healthcare applications with the need for high-performance computing.

Shaping accountability in the space of digital twins comes with a plethora of technical issues, mainly because of the complexity and multi-layered nature of these systems. A digital twin isn't an application in isolation—it consists of a highly interdigitated collection of real-time input feeds, machine learning models, Internet of Things (IoT) sensors, cloud computing resources, and simulation software (Casas & Pi (2024). The plethora of components and players makes fault determination even harder when

something has gone awry. If a digital twin analyzing a production line of a smart factory fails to pick up an imminent system failure, the fault could be with an incorrect sensor input, a buggy algorithm, a misstep in inter-module communication, or even old firmware. Liability determination over a system this distributed—much less one with third parties involved—becomes a technically intimidating task (Gore et al., 2025).

According to a 2023 *Deloitte study*, more than 60% of the US companies using digital twins cite integration complexity and data precision as belonging to the major technical obstacles. And besides, the dependence on machine learning (ML) models in the context of a digital twin makes it a matter of algorithmic opacity and "black box" behavior, where AI decision logic becomes hard to follow and audit (Cellina et al., 2023). This opacity makes it even harder for the responsible designer, lawyer, or regulator to point fingers in the event of a failure. Developing standards around the validation and verification of digital twins remains a work in progress; while organizations such as the *National Institute of Standards and Technology (NIST)* engage in the development of frameworks for secure AI and cyber-physical systems, their widespread uptake remains an ongoing endeavor (Harris et al., 2024).

Milhai et al. (2022), underscored that cybersecurity risks weaken accountability as well. Digital twins' interconnectivity with IoT devices and cloud services widens attack surfaces, threatening data thefts or sabotage. A hacked healthcare digital twin might reveal patient information or provide erroneous treatment suggestions with life-critical outcomes. Though NIST and ISO offer starting points, their standards are not designed to address the special security requirements of digital twins, leaving gaps in encryption, authorization controls, and incident response procedures.

5.2 Ethical Issues

Helbing & Sanchez (2023), articulated that ethical considerations involve data privacy, algorithmic fairness, and equity. Where healthcare-related digital twins manipulate protected health information (PHI), they must be HIPAA and CCPA-compliant, but these regulations do not address the synthetic or dynamically derived data, leaving consent and ownership ambiguous. A patient's digital twin, for instance, may be inferring sensitive genetic risk factors in the absence of consent, compromising autonomy and transparency. Algorithmic fairness represents another major concern: should the training data be under-representative of a population; the resulting digital twin outputs could be discriminatory. The GAO cautions that unfair predictive models in healthcare risk exacerbating treatment disparities in accessibility and outcomes (Mocanu & Sibony, 2023).

Aside from the technical realm, digital twins pose grave ethical dilemmas making it even harder to allocate responsibility. One issue concerns personal privacy and consent, particularly in healthcare and home services (Nechesov et al., 2025). If personal or biometric information—e.g., a model of a patient's physiology or a resident's behavior in a smart building—is to be used to create a digital twin, the ethics come in ensuring the person has given consent, comprehends the impact, and has a measure of control over the modeling and application of their information. In reality, the collection of data is typically opaque, with end-users not knowing the scope of monitoring or what their information contributes to the simulation (Peldon et al., 2024).

The Electronic Frontier Foundation (EFF) states the US still has no sweeping federal law covering data privacy, and therefore state-to-state and industry-to-industry ethics vary. Moreover, ethics in the application of the digital twin to make decisions impacting human lives, like predictive policing or insurance policy risk, creates new moral and legal conundrums (Rathod et al., 2024). Biases in the training information used to create the twin may create discriminatory results, but legal and ethical responsibility frameworks are poorly developed. This double layer of ethics, along with the opacity of technology, makes it a legal and moral difficulty to allocate responsibility in the increasing realm of the digital twin (Singh & Tiwari, 2024).

According to Vetrivel et al. (2024), Equity issues result from the substantial costs involved in the development and upkeep of digital twins. The GAO estimates the 2023 United States digital twin market at $15.6 billion, yet smaller local governments and financially constrained healthcare organizations frequently do not have the resources to implement these technologies, exacerbating quality gaps in services. Moreover, governing frameworks for ethics continue to lag. Bruynseels et al. introduce process-oriented ethics maps to handle bias and consent in healthcare digital twins, yet implementation lingers behind technology development.

6. Future Directions

6.1 Policy Recommendations

As more of the United States' critical infrastructure, healthcare, manufacturing, and urban planning become embedded with digital twin technology, policymakers are left to tackle the widening gaps in legal and regulatory frameworks. Of greatest immediate concern is the development of thoroughgoing, sectoral guidelines for delineating accountability and responsibility for the applications of digital twins. The US Congress, along with regulatory bodies like the Federal Trade Commission (FTC) and the National Institute of Standards and Technology (NIST), should enact legislation establishing standards for transparency, dependability, and responsible usage of information in digital twins. Without a national unified law regarding the protection of

information, as the European General Data Protection Regulation (GDPR) provides, US stakeholders are left to navigate a quilt of differing state laws, such as the California Consumer Privacy Act (CCPA). A national framework for data privacy would create consistent requirements for collecting, consenting to, and warehousing personal, real-time, and even sensitive material on which digital twins depend.

Moreover, the federal government's CISA (Cybersecurity and Infrastructure Security Agency) and NIST (National Institute of Standards and Technology) must create and implement risk management procedures for cyber-physical systems, including requirements for reporting failure or security vulnerabilities concerning digital twins. Liability insurance schemes must adapt too. Insurers, assisted by institutions such as the National Association of Insurance Commissioners (NAIC), should provide custom coverage for developers and users of digital twins, including algorithmic failure and data inaccuracy. Legal transparency regarding intellectual property is equally crucial. As the trend towards mimicking proprietary processes or offerings by digital twins expands, the U.S. Patent and Trademark Office (USPTO) must provide guidance clarifying ownership rights over digital representations and models. Policymakers should further task multidisciplinary task forces—comprising ethicists, technologists, and legal scholars—to periodically analyze the social consequences of the application of digital twins and propose adaptive governance frameworks.

6.2 Technological Advances

Concurrently with legal and policy development, technology innovation will be key to ensuring the effective and safe deployment of digital twins. One of the primary areas of development includes explainable artificial intelligence (XAI) to make AI systems decision processes interpretable and explainable. Among the organizations contributing to the development of XAI in the United States are the Defense Advanced Research Projects Agency (DARPA) and IBM Research, both aimed at boosting AI-driven digital twin confidence and responsibility, particularly in applications with a high-stakes risk profile, such as aerospace and healthcare. Improvements in edge computing will, on the other hand, minimize latency in the performance of digital twins through local processing near the source, offering enhanced real-time responsiveness while reducing dependence on central cloud services. This development improves performance while lowering the risk of cyberattacks.

Another frontier is blockchain integration, delivering an immutable, timestamped history of all alterations to a digital twin, increasing auditability and tracking of liabilities. To take an instance, blockchain in production settings can capture the entire life cycle of a digital twin, with traceability during system failure. Last but not least, semantic interoperability—the capability of heterogeneous systems to comprehend and utilize traded information—will become a key requirement as digital twins become increasingly common across industry and device ecosystems. IEEE and the Industrial Internet Consortium (IIC) are already working toward creating open protocols and standards to guarantee compatibility and information integrity across platforms.

7. Conclusion

In summation, the accelerated development and application of digital twin technology in major sectors including healthcare, industry, transportation, and infrastructure across the United States has brought about enormous benefits—varying from process efficiency and predictive repair to targeted healthcare treatment and intelligent urban design. Nevertheless, the technology has its intricate legal, ethical, and technical issues that require immediate, collective action. The United States' current legal structure still has gaps and lags, providing little to no guidance on responsibility, liability, and data management in simulated settings. Through the presentation of case histories and industry metrics, system breakdowns in digital twin systems create significant damage, yet blame often gets lost in the multi-layered reality of these technologies. To address these issues practically, it requires cooperation between the federal offices, policymakers, courts and legislatures, and industry executives to create transparent regulatory frameworks, legal protections, and powerful technological frameworks. Future endeavors must involve the creation of overall national laws regarding privacy, effective rules for holding entities liable, and technical innovations in the form of explainable AI, edge computing, and blockchain-enabled responsibility frameworks. Only through a balanced and visionary strategy will the United States be able to guarantee continued improvement in real-world performance while maintaining the public's confidence, security, and juridical simplexes in a highly digitized world.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Casas, P. F., & Pi, X.t (2024). Building Society 5.0: A Foundation for Decision-Making Based on Open Models and Digital Twins. New York: Sage Printer

[2] Cellina, M., Cè, M., Alì, M., Irmici, G., Ibba, S., Caloro, E., ... & Papa, S. (2023). Digital twins: The new frontier for personalized medicine?. Applied Sciences, 13(13), 7940.

[3] Gore, S. I., Deshmukh, K. D., Mahamulkar, V. R., & Patil, R. (2025). Ethical and Legal Implications of Digital Twin Deployment in Biomedical and Pharmaceutical Domains. In Accelerating Product Development Cycles With Digital Twins and IoT Integration (pp. 491-514). IGI Global Scientific Publishing.

[4] Haris, M., Saad, S., Rasheed, K., Ammad, S., & Oad, V. K. (2024).Navigating Ethical and Social Implications in Digital Twins and Robotics. In *Applications of Digital Twins and Robotics in the Construction Sector* (pp. 195-215). CRC Press.

[5] Helbing, D., & Sánchez-Vaquerizo, J. A. (2023). Digital twins: Potentials, ethical issues and limitations. In Handbook on the Politics and Governance of Big Data and Artificial Intelligence (pp. 64-104). Edward Elgar Publishing.

[6] Mihai, S., Yaqoob, M., Hung, D. V., Davis, W., Towakel, P., Raza, M., ... & Nguyen, H. X. (2022). Digital twins: A survey on enabling technologies, challenges, trends and future prospects. IEEE Communications Surveys & Tutorials, 24(4), 2255-2291.

[7] Milosevic, Z., & Van Schalkwyk, P. (2023, October). Towards responsible digital twins. In International Conference on Enterprise Design, Operations, and Computing (pp. 123-138). Cham: Springer Nature Switzerland.

[8] Mocanu, D. I. A. N. A., & Sibony, A. L. (2023). EU consumer law meets digital twins. Revue européenne de droit de la consommation, 1, 229-257.

[9] Nechesov, A., Dorokhov, I., & Ruponen, J. (2025). Virtual Cities: From Digital Twins to Autonomous AI Societies. IEEE Access.

[10] Peldon, D., Banihashemi, S., LeNguyen, K., & Derrible, S. (2024). Navigating urban complexity: The transformative role of digital twins in smart city development. Sustainable Cities and Society, 111, 105583.

[11] Rathod, S. B., Ponnusamy, S., Mahajan, R. A., & Khan, R. A. H. (2024). Echoes of Tomorrow: Navigating Business Realities with AI and Digital Twins. In Harnessing AI and Digital Twin Technologies in Businesses (pp. 158-174). IGI Global.

[12] Singh, P., & Tiwari, S. (2024). Digital twin and Artificial Intelligence. Washington: Worth Publishers

[13] Stapleton, D., & Stapleton, K. M. (2022). Digital Twins and Industry 4.0: A Review of Legal Implications Regarding Property Rights in Physical and Virtual Spaces. J. Transp. L. Logistics & Pol'y, 89, 95.

[14] Teller, M. (2021). Legal aspects related to digital twin. Philosophical Transactions of the Royal Society A, 379(2207), 20210023.

[15] Vetrivel, S. C., Sowmiya, K. C., & Sabareeshwari, V. (2024). Digital Twins: Revolutionizing Business in the Age of AI. In Harnessing AI and Digital Twin Technologies in Businesses (pp. 111-131). IGI Global.

[16] Wang, B. T., & Burdon, M. (2021). Automating trustworthiness in digital twins. Automating Cities: Design, Construction, Operation and Future Impact, 345-365.

[17] Zoltick, M. M., & Maisel, J. B. (2023). Societal impacts: Legal, regulatory and ethical considerations for the digital twin. In The digital twin (pp. 1167-1200). Cham: Springer International Publishing.