NFSU JOURNAL OF LAW & ARTIFICIAL INTELLIGENCE

JLAI
Volume: 2, Issue: 1
June 2023
E-ISSN: In Process

LEGAL REFORMS IN THE AGE OF DIGITIZATION: SETTING REALISTIC GOALS.

Prof (Dr.) Sapna S[*1]
Abhishek Sharma Padmanabhan[**]

Abstract: *The anomalies surrounding the legal regulation of digital technologies and products that have emerged as a result of such technologies are the focus of this article's investigation. The active development of digital services and digital financial assets necessitated the selection of this topic, as did the need to adapt modern legislation to the demands of the digital economy. International organizations are developing different strategies for digital law, but neither in theory nor in reality there a uniform understanding of the legal nature of digital technologies and their legal control. In this article, the findings of a review study of the most important legal characteristics of digital technologies are presented. One of the conclusions is that the technical aspects of digital technologies are not sufficiently taken into account, and that an international plan for developing civil and intellectual law that addresses digital technology has to be devised.*

The authors assess the viability of incorporating new legal categories into the traditional rule of law on contracts, responsibility, and intellectual property protection by evaluating the legal personality, security, and tort categories of digital technology and products, comparing them to analogous legal institutions. The authors contend that the application of traditional law to digital technologies is severely constrained, and that many of these innovations require the development of qualitatively new legal frameworks. The article's conclusions have substantial methodological and practical importance, and they can be taken into account when attempting to change the law as it currently stands.

Keywords: *Digital technologies, Legal personality, Civil law, Intellectual Property, Rule of Law, Governance.*

1. INTRODUCTION

There is a pressing need for globally uniform, comprehensive legal protections in the digital economy due to its fast rise. In order to limit the risks associated with digitization and legitimate new assets, both physical and intangible, these protections must include trustworthy assurances of legal protection. Governments and international organizations are working hard to alter current legislation in order to keep pace with the fast improvements in digital technology[1].However, the plans that have been put forth are sectoral and only focus on a few aspects of digitization, and the solutions frequently work to advance a political goal at the expense of a unified, global legal approach.[2]. Both of these concerns need to be addressed, but the first is of more concern.

In the present research work, the authors will consider how the rule of law may be altered to deal with the legal issues posed by digital technology and its products. The theoretical and practical foundations of legal personhood and digital technology protection are explored in this article. This article explores the evolution of regulation in the domain of digital programming makers and viewers have obligations. Additionally, it explains how intellectual property rights may be safeguarded in the digital era.

The essay evaluates status regulation, responsibility establishment, and unique technological components such as Artificial Intelligence, Internet of Things, Block chain, big data, etc., to reveal the authors' paradigm for investigating the legal status of digital technology. The current study emphasizes both the limited adaptation of traditional standards in the regulation of digital technology and the

[1] * Professor of Law and HOD, School of Law, CHRIST (Deemed to be University);
Email : sapna.s@christuniversity.in
** Assistant Professor of Law, School of Law, CHRIST (Deemed to be University);
Email: sharmapabhishek@gmail.com

[1] Catterwell, R, *Automation in contract interpretation*. 4 Harv.J.L. & Tech. 81,112 (2022)

[2] Chen, J., Edwards, L., Urquhart, L., & McAuley, D., *Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption.*8 High Tech. L.J 98,101 (2021)

tendency of the legal system to marginalize the digital world. New legal frameworks for digital technologies may be required as a result of the growth of the digital economy and the technical capabilities of specialized technology.

2. APPROACHES FOR REGULATING THE DIGITALIZATION

There are only two possibilities for the future of law in an increasingly digital environment. The first way is geared at countries and international organizations, and it focuses on fulfilling tasks that are quite specific in nature (financial intelligence and acceptance of technical regulations, for example). The second approach is a methodological methodology that can provide global, full solutions to handle the issue at hand.

2.1 The utilitarian approach

A utilitarian technique differs from others in that it concentrates on a single issue. International organizations are working under the stringent direction of their member nations to implement legislative measures that limit the dangers connected with the usage of certain digital assets[3].This pattern of certain nations or groups of countries taking the lead and others being shut out may be seen in a number of political frameworks. The utilitarian approach has a tendency to bring up personal interests[4].

In its 2019 proposals, the Financial Action Task Force (FATF), for example, recommends States to impose legal limits on crypto assets in order to prevent the laundering of illegal monies. In this regard, the recommendations from the Basel Committee on Banking are consistent with those of the Financial Stability Board. The usage of crypto assets necessitates the supervision of banks in the avoidance of potential risks. The Payment Services Directive Two (PSD2), which requires that financial and technical companies have access to client information, was updated by the European Union (EU), and the EU also proposed specific legal frameworks for digital payment services.[5]

When considering technical regulations, it is essential to keep the International Organization for Standardization in mind (ISO). The ISO has published ISO/IEC JTC 1/SC, which has four Artificial Technology (AI) standards and plans to produce another twelve, and it is planned to deliver 21 standards in the future. The ISO is involved in defining international frameworks for artificial intelligence (AI), the Internet of Things (IoT), and cloud computing.[6]. Unmanned aircraft systems (UAS) have also been given ISO worldwide norms in 2019. The necessity for a European framework law on drone use was emphasized in a resolution on the safe operation of unmanned aircraft systems that the European Parliament voted in 2015[7].

In the past, international organizations have also taken part in globalendeavors. As an example, the Organization for Economic Cooperation and Development (OECD) has outlined a set of general principles for the regulationof artificial intelligence and provides uniform direction on how ICO law should be implemented and changed[8].

According to the documents, it is recommended that each country's law should contain the following.

i. Focusing artificial intelligence on promoting inclusive growth, sustainable development, and social welfare.

ii. The use of AI technology to promote inclusive growth, long-term development, and well-being;

iii. Human involvement should be strengthened wherever it is needed to uphold a just society, and the rule of law, human rights, democratic values, and cultural diversity should be upheld and promoted.;

iv. Disclosure of knowledge concerning AI systems in a transparent and responsible manner;

v. constant risk assessment and risk mitigation for the dependabilityand safety of technology;

vi. Developers' and users' accountability in the functioning of digital technology.

The G20 endorsed this approach, establishing five criteria for AI regulation that are substantially in line with the OECD standards

[3] Chessman, C. F, *Not quite human: Artificial Intelligence, animals, and the regulation of sentient property*. 8 J. Sci. & Tech. L 99,114 (2022)

[4] Mowbray, A., Chung, P., & Greenleaf, G, *Utilising AI in the legal assistance sector-testings role for legal information institutes*, 8 Pace Int'l L. Rev 12, 25 (2019)

[5] Chung, J., & Zink, A, Hey *Watson, can I sue you for malpractice? Examining the liability of artificial intelligence in medicine,* 6 Mich. Telecomm. & Tech. L. Rev 78, 85 (2023)

[6] Custers, B. H. M., & Leeuw, F, *Legal Big Data: Applications for legal practice and legal research*, 9 Rich. J.L. & Tech. 62,72,(2021)

[7] Neznamov, A. V., & Naumov, V. B. *Regulation for the robotics and cyberphysical systems regulation,* 2 Penn St. L. Rev 25,31 (2001)

[8] Edwards, F. R., Hanley, F., Litan, R., & Weil, R. L. (2019). *Crypto Assets Require Better Regulation*, 14 Rutgers Computer & Tech. L.J, 61,74 (2021)

in its ministerial declaration. The European Commission proposals for digital law-making were a major source of inspiration for this new approach to financial regulation.

The Fintech legislation is fragmented, and a call was made to provide equitable legal conditions for technology firms and put an end to this[9]. There was a strong emphasis on the need to adapt current legislation to new technological developments. Maintaining both personal and depersonalized data, assuring system transparency, and adhering to digital ethics were among the recommendations. Implementing the security agenda is actively handled by the United Nations (UN). The General Assembly Resolution advocated for boosting national laws and preserving information security in response to the increased frequency of cybercrime. The UN General Assembly's 74th session also has a report to pay attention to[10].

The concerns connected to the widespread usage of low-cost smart gadgets, holes in information decryption, etc. are highlighted as needing legal controls[11].Assimilation of technical specialists into the legislative process, modernization of domestic cybercrime laws, and the development of legal instruments for international criminal regulation are all areas where research suggests reform should be concentrated.

The Council of Europe Convention on Cybercrime serves as the basis for EU directives and framework decisions on several aspects of the digital economy[12]. As a result of legal activities, civil and financial law provides a foundation for criminal law laws and considerably increases the level of responsibility for crimes committed in the information technology industry[13].

2.2 The methodological approach

A global and all-inclusive form of legal regulation is something that the, Methodological Approach, the second strategy takes into account. It is vital to comprehend the underlying principles of digitization. For example, the ethical, social, technical, and political dimensions of digitalization may be handled by embracing a global perspective[14].

A thorough understanding of the current state of digital technologies and their effects on humans is necessary, even though the utilitarian approach prioritizes the development of multiple sectoral rules and initiatives. It is the methodological approach that focuses on values and commitments; as it advises finding a balance between technology improvements and the choosing of a social model. A legal basis and a genuine digital foundation are thus required[15].

An all-encompassing legislative framework must be put in place. If internationalproblems are to be resolved, it has to be seen if existing legal structures or creation of a new legal system are more successful. A legal challenge against the rule of law in the digital realm is not allowed. In the digital economy, inclusive development and international cooperation are essential. A strategy for digital legal transformation as well as models for reducing digitalization risks must be developed in order to accomplish this. Many concerns cannot be addressed since there is no comprehensive international legal framework[16]. New digital technology and goods, as well as how current legal instruments could be altered to fit new legal occurrences, all need strategic solutions.

Unfortunately, neither the scientific community nor international organizations are addressing these issues. The need for a unified theoretical framework for digital governance is greater than ever. Legal safeguards for digitization will be provided at both the international and nationallevels in the future. International organizations are attempting to put in place a comprehensive security strategy using a global methodological framework[17]. Using digital technology to solve social and economic problems and build international trust are just a few of the benefits that may come from widespread usage. When it comes to digitalization, the Organization for Security

[9] Entin, V. L, *Copyright in virtual reality (newopportunities and challenges in digital age),* 14 Temp. Envtl. L. & Tech. J 12, 25 (2022)

[10] Fernández-Villaverde,J, *Simple rules for a complex world with artificial intelligence,* 15 UCLA Bull. L. & Tech 11, 19 (2021)

[11] Fosch Villaronga, E., & Millard, *Cloud robotics law and regulation,* 14 U. Ill. J.L. Tech. & Pol'y 94,103 (2020)

[12] Ponkin, I. V., & Redkina, A. I, *Artificial intelligence from the point of view of law.,* 22 N.M. L. Rev 95,101 (2016)

[13] Giudici, G., Milne, A., & Vinogradov, D, *Cryptocurrencies:Market analysis and perspectives,*8 Va. J.L. & Tech 95,103 (2021)

[14] Goanta, C, *Big law, big data. Law and Method*, 12 J. Marshall J. Computer & Info 42, 52 (2019)

[15] Rahmatian,A, *Originality in UK copyright law*, 44 Law & Hum. Behav 98, 101 (2017)

[16] Gomes, S. *Smart contracts: Legal frontiers and insertion into the creative economy*, 15 Rutgers Computer & Tech. L.J 13, 9 (2018)

[17] Hacker, P., Krestel, R., Grundmann, S., & Naumann, F, *Explainable AI under contract and tort law: Legal incentives and technical challenges.* 12 Santa Clara Computer & High Tech. L.J 22, 17 (2017)

and Cooperation in Europe (OSCE) is well-versed. With the OSCE's political/military wing, confidence in cyberspace has been established. One of the most useful tools for fostering cross-border cooperation is the digital economy. In order to avoid conflict and enhance the lives of citizens, trust and confidence must be fostered via economic stability and collaboration.[18] Connectivity, accountability, and transparency are all set to soar in the digital economy[19]. It has the potential to generate growth and development that is both broad-based and long-term.

The OSCE is equally concerned about the protection of the private sector in the human dimension and across dimensions. That's why guidelines and suggestionsthat strike a balance between digital security issues (such stopping radicalization or criminal activity) and the private sector's and people' ability to freely generatedigital content are needed. These are part of the organization's international initiatives. The OSCE Mission in Bishkek has created and launched a Master's Program in Digital Jurisprudence for the first time ever with the aim of training experts in the area of digital technology law[20]. Participants in the program include state and municipal government attorneys, business legal counsel, and digital security attorneys. The five guiding principles of EU CII protection constitute the foundation of this document. Prepare for the worst-case situation in advance, identify threats early, mitigate damage, restore data and collaborate with other nations to harmonize and unify national laws are some examples.

3. EMERGING FORMS OF DIGITALIZATION AND ISSUES IN THEIRREGULATION

Contemporary scientific research does not adequately investigate digital technology's legal standing and the things it produces. Experts' attention isfocused on technical and practical concerns, as seen below. Regulators in the AI area are concerned with the technology's suitability for application in certain disciplines, such as law, or with pushing legal reforms[21]. The debate rages on as to whether or not artificial intelligence should be considered a civil rights issue or just a matter of academic inquiry.

Drones and other cutting-edge technology are debated in the context of specialized law reform, transportation, health care, information, and other fields.Many studies have been conducted on formalizing and regulating smart contracts so that the intentions of the parties are disclosed on stock exchanges.In addition, the topic of crypto currency asset management is addressed here Financial law principles such as taxes and the regulation of digital payment instruments are the subject of a considerable lot of study. Legal implications of big data include, but are not limited to, its use in legal processes, its regulationby legislation, its modeling, and its evaluation for possible legal ramifications[22].

An exhaustive examination of the legal ramifications of digitization would take much too long, so instead the present research will concentrate on two pressing issues that need national and international attention. As part of a larger inquiry into the transformation of legal frameworks, attention is directed at the legal standing of digital technology as an object of civil rights and any specific contractual interactions in the digital economy[23]. There is also a discussion on the adoption of new technology, such as IoT, AI, big data and machine learning (ML), drones as wellas other technologies. There are two approaches to consider how law will change in the future as we enter the digital era: either by reconsidering current legal frameworks or by completely replacing them with more general and abstract models.

The conflict between these two alternatives is most obvious when looking into how digital technology might be protected and given a legal status. In order tobe deemed protected, digital technologies must be able to operate as subjects of civil and intellectual rights[24].It's crucial to think about the implications of releasing copyright and real right from the shackles of traditional legal institutions if such a thing is allowed. Those who oppose emancipation argue that artificial intelligence and machine learning cannot serve as the basis for legislation or as a

[18] Holden, P, *Flying robots and privacy in Canada*, 22 Wash. U. L. Rev 92,101 (2012)
[19] Sanz Bayón, P, *Key legal issues surrounding smart contract applications*. 9 J. Telecomm. & High Tech. L 98,101 (2015)
[20] Huang, R., Yang, D., & Loo, *The development and regulation of crypto assets: Hong Kong experiences and a comparative analysis*, 16 Widener L. Review 21, 26 (2015)
[21] Kaminski, M. E, *Robots in the home: What will we have agreed to?*,12 Willamette L. Rev 95,102 (2019)
[22] Lauts, E. B, *Legal regime for Artificial Intelligence modern information technologies and law*, 12 Wis. L. Rev, 101,112 (2022)
[23] Sixt, E., & Himmer, K, *Accounting and taxation of cryptoassets*, 9 J. Bus. & Tech. L 98, 102 (2017)
[24] Konert, A., Smereka, J., & Szarpak, L, *The use of drones in emergency medicine: Practical and legal aspects*, 25 U. Pitt. L. Rev, 99,101 (2018)

replacement for it. The term for this is " consolidating learning." Others who support digital emancipation, on the other hand, see emancipation as an unavoidable conflict between public and private interests in the digital age and think that digital technologies need to attain functional autonomy and commercial utility in order to create their legal identities.[25]. Russia's current legislation recognizes digital rights as a kind ofcivil rights alongside property rights[26]. As a property right, intellectual property rights may be used as a foundation for denying that digital items can be protected by copyright. Their definition and use are limited since they are defined as the right to obligation or other rights that may only be used, disposed of, or managed inside the information system. In the absence of digital technology, it will be interesting to watch how these rightsare put into practice in real-world settings (such as large data consolidation and analysis, machine learning findings, etc). Unlike Russian law, English law viewsdigital rights as a property right, not an information right[27]. Since digital rights are fundamentally monetary in origin, this strategy is consistent with the idea that they should be protected as if they were physical goods.

English law provides clear responses to questions about the legal status of self-learning software that incorporates "experience" in order execution, ownership rights to products created by such software or robots, and property or other responsibilities for adverse consequences of digital technologies.

4. MODEL FOR EFFECTIVE REGULATION OF DIGITALIZATION – SUGGESTIONS

However, learning from other countries' digital economy successes and failures will not be enough to ensure long-term success in the digital economy. A one- size-fits-all approach is essential when it comes to civil issues concerning digital technology, products, and rights.

Here are some methodological concerns that we feel are necessary for this technique:

1) A digital product's materiality or monetary value cannot be taken into account when deciding whether it qualifies as a civil rights object. Digital objects can be seen as both intellectual property and proprietary, and thus have a broad legal nature;

2) Evaluations of digital technology ought to be based on a legal framework that permits adherence to the connection's legal requirements and can strike a balance between private and public interests in circulation.;

3) It is imperative that a worldwide strategy for regulating digital technology as an issue of civil rights take into account the objective decoupling of digital law from existing legal frameworks. Meaning that multifunctionality of items, technical saturation, task management uncertainty, and potential risks associated with their integration into civilcirculation severely restrict traditional legislation's ability to adapt to digital technologies. This is a major problem for traditional legislation.

Whether to provide digital benefits to people or declare them to be in the public domain is a crucial decision for the future of intellectual property rights in the digital arena. The legal nature of digital product rights must be defined before a decision can be taken; this is particularly true for AI in particular[28]. It is difficult to distinguish between author's and compiler's rights because digital products have objective qualities such as high repeatability of technology results and low human creativity contribution. The automation of some procedures and the difficulty to differentiate between creative and non-creative components are further difficulties. Databases, machine learning algorithms, digital platforms and platform solutions, etc., each have their own unique set of problems to deal with as well.

The issues provided by the digital economy must be addressed by the legal system if intellectual property is to be effectively protected and the interests of artists, users, and investors are to be fully honored. [29].

In order to succeed, digital technology needs a legal framework. Robots and robotic goods are sometimes offered as objects of obligation that can engage into contracts with third parties on

[25] Lee, J, *Smart contracts for securities transactions on the DLT Platform (Blockchain)*, 25 Touro L. Rev, 101,103 (2019)

[26] Lei, C, *Legal control over Big Data criminal investigation*, 40 T. Jefferson L. Rev, 99,101 (2023)

[27] Lin, C., Shah, K., Mauntel, C. & Shah, S, *Drone delivery of medications: Review of the landscape and legal considerations*, 75 Tenn. L. Rev 69, 71 (2020)

[28] Liu, Y., & Huang, J, *Legal creation of smart contracts and the legal effects*, 12 Stan. L. Rev 22, 26 (2017)

[29] Wachter, S., Mittelstadt, B., & Russell, C, *Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI*, 14 Hous. L. Rev 14, 22 (2017)

behalf of their owner and in the owner's own name. Deliveries robots have the same rights and obligations as pedestrians, but they also have to abide by the same laws. For instance, they cannot run into people and must move aside for other pedestrians. Creating a legal framework for digital technology is the next stage. Plans call for treating all robots, including those produced by the robotics sector, as human beings when engaging into agreements with third parties on the owner's behalf and in his or her name.

Delivery robots have the same rights and responsibilities as pedestrians, but they must follow the same rules: they cannot run into people and must move out of the way for other pedestrians, for example. Legal identity is characterised by customary law as a synthesis of legal ability, active capacity, and delictual dispositive capacity. Physical individuals, companies, and public legal entities are the currently recognized three categories of legal capabilities. This list has gradually expanded as necessary to include new circulating parties, and the theoretical foundations of legal identity have also been modified. A new understanding of the subject's will, interest, and motive is especially necessary for assigning legal identity to corporations[30].

Additionally, it does not seem plausible to argue that digital technologies are not legal because they do not contain a will component. The legal identity of firms, specifically from the perspective of autonomy and decision-making, should be considered when evaluating technologies. These qualities can be supplemented by the capacity for independent learning and action algorithm modification. It should be mentioned that varying levels of autonomy exist in contemporary digital technology. Should they be distinguished from one another or subject to the same legal identity rules? There isn't currently a resolution to this problem incontemporary law. Issues like public liability insurance, criteria for identifying the potential danger of robotic operations, and processes for documenting and registering new legal organizations must be addressed if AI and other digital technologies are recognized as having legal identities.

In principle, it makes sense that digital technologies would have a legal identity,yet this identity is frequently associated with that of individuals. Experts claim that robots' legal identities may be acknowledged in a manner similar to how international organizations like the UN are recognized legally. A further consideration that should not be overlooked is the independence of digital items. Humans' ability to commit crimes will depend on how much they depend on technology. When talking about how the law is changing in the digital world, it is important to bring up a number of practical points. Specifically, problemswith AI applications need to be fixed. Digital device malfunctions are notoriously difficult to pin down to a specific person or group of people. Watson for Oncology, IBM's artificial intelligence (AI) technology, is extensively contested in South Korea and experts believe that Watson's inventors and medical workers should be held accountable[31]. Security guarantees for AI and robotics are being considered along with questions of activity regulation. Chessman examines the subject of adopting animal management standards to robots, up to and including establishing liability for robot or AI abuse, in order to avoid causing human emotional pain[32]. As artificial intelligence (AI) and machine learning become more prevalent, it's becoming more difficult to determine what constraints could apply to their usage in legal operations. There are too many value judgments involved in legal decision-making, according to some academics, who also stress that norms are context-dependent and need justice in all its expressions. Because attorneys have been using digital technology for decades, this approach looks to be unduly limiting. It is in question whether or not to formalize this involvement and hold the computer accountable for the ultimate decision. It should be mentioned that automated contract interpretation is a possibility with machine learning and artificial intelligence[33].

However, a machine may be able to interpret some of the rules, but not all of them. There are two primary limitations: Because certain sections are more of a "matter of perception," the parties' views and circumstances must be taken into consideration while interpreting them. When it comes to reading contracts, machine learning can only supplement legal counsel, not

[30] Yu, R., & Alì, G. (2019). *What_s inside the black box? AI challenges forlawyers and researchers,*19 Harv. J.L. & Pub. Pol'y 25, 27(2012)

[31] Low, K., & Mik, E, *Pause the Blockchain legal revolution* 69 Sw. L. Rev 62, 71 (2019)

[32] Maggon, H, *Legal protection of databases: An Indian perspective.*11 S. Tex. L. Rev 96,112 (2019)

[33] Marquès, M. C, *Recreational drones: Legal framework, civil liability and data protection.* 6 St. Thomas L. Rev 98,114 (2020)

take their place. As a result, it is best to segregate human and automated decision-making. AI might handle and analyse data on its own, leaving humans free to make judgments based on their critical assessment of the processed and analysed data. In addition, the Internet of Things raises a number of issues. Users of "smart" devices may not realize that their personal information is being gathered and sent without their permission, or that it may be exchanged across borders, among other transgressions, according to lawyers.

Regulations like the EU's General Data Protection Regulations (GDPR) may place an excessive amount of obligation on device manufacturers or create new cyber security risks as a result of the Internet of Things (IoT) and smart home usage not being sufficiently taken into account in current legislation.[34]. The adoption of cloud technologies also raises the issue of protecting personal data. Since the existing stringent General Data Protection Regulation (GDPR) cannot identify data controllers or providers, nor can it reveal that the application has collected data, processing personal data in the cloud is prohibited.[35].

In terms of the legal control of digital technologies, it is impossible to avoid discussing the practical considerations involved in the operation of unmanned aircraft (drones). The protection of privacy is nevertheless a concern even if many nations' laws—including those in developed countries —include restrictions on the use of drones[36].No country in the world, in particular, provides landowners with any kind of legal protection from the potentially malicious acts of drone owners, who may use their aircraft to genuinely invade foreign territory, take pictures of everyone without their permission, or otherwise trespass on their privacy in various ways.. Additionally, the concern over the information that drones may acquire and the prospect that their owners may exploit it is unresolved.

5. CONCLUSION

This present research study found that modern legislation is barely beginning to develop standards for digital technologies. Discussions are currently centred on two potential methods at the international level: one is to encourage the growth of the digital economy (a policy known as progressive advance), and the other is to reduce the risks that are associated with using it (security strategy). World Nations are making palliative efforts to address the problem by enacting legislation and implementing national initiatives aimed at finding comprehensive answers. While acknowledging the importance of this effort, there is a pressing need for a more systematic and uniform approach to the development of digital law, with a focus on two primary issues:

(1) Is it possible to adapt current legal systems to the digital economy, or are new laws required

(2) How can a design be made for a universal transnational technologylaw?

The way contemporary law judges the legitimacy of digital technologies and its capacity to safeguard them will have a direct impact on how the first problem is resolved. Traditional law is Marginalised in light of digital development, therefore applying outdated frameworks results in fragmented regulation with no room for expansion. New, fundamentally different legal frameworks must be created and long-term implemented in order to advance in the digital economy. It is important to thoroughly research the legal status of technologies, copyright and related laws, machine liability, and insurance. Another important thing to keep in mind is that developing these models at the level of the international community rather than the level of individual nations will ensure that the rules are universal.

[34] Modh, K, *Drones and their legality in the context of privacy*, 25 Phoenix L. Rev 92, 106 (2018)

[35] Zimmerman, E, *Machine minds: Frontiers in legal personhood*, 12 Ga. L. Rev 15,22 (2018)

[36] Mohamed, S., & Zulhuda, S.*The concept of internet of things and its challenges to privacy*, 8 Ohio St. L.J 92, 101 (2017)