IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Study On Legal Challenges Of Digitalization In The Context Of Industry

DR. PANKAJA T.C.,
Assistant Professor,
R. L. Law College, Davangere, Karnataka, India.

Abstract: The article discusses problems and potential legal issues that may arise if the Industry concept is put into practice. For the requirements of management and engineering employees, an interdisciplinary analysis was conducted. It has been demonstrated how the peculiarity of digitalization and automation, as well as relationships, imply legal issues. Levels of legal difficulties were identified and technology components chosen. Legal issues pertaining to cloud computing, the internet of things, big data analytics, and cyber-physical systems were discussed. The primary legal issues with Industry digitalization and automation technologies were highlighted. Legal risk assessment concerns for Industry technology were also examined.

Keywords: Industry, digitalization, legal challenges and risks

Introduction:

The fundamental changes brought about by the digital revolution in the methods of production and value generation represent a significant challenge for businesses. Companies must create plans quickly to take advantage of emerging digitalization opportunities, enhance current procedures, and create new business models if they don't want to fall behind. Additionally, the legal implications must be considered.

The industry must endeavor to concentrate its efforts on pertinent legislation provisions and legal evaluations. The legal protection can be utilised to build safeguards that reduce the danger of fines and liabilities for Industry and also for other stakeholders. To prevent the possibility of legal responsibility under both criminal and civil law for both businesses and its bodies, it is crucial to follow the law and established standards. Management risk rises as a result of totally new requirements brought on by the digitalization of production and value chains that are not appropriately addressed by the current legal system. Here, it's crucial to consider data protection, IT security, and corporate responsibility-related issues. There is no examination of Industry in case law or legal literature because legal definitions of related concepts are rare. There are some circumstances where legal queries cannot be resolved. Producers and developers are required to recognise and record any potential risks that could give rise to liability in such situations. This will make it possible to demonstrate in the event of a dispute that they attempted risk reduction prior to suffering damage in accordance with the state of the art.

The Industry idea can be interpreted as a change in plans, organisations, business practices, value and distribution networks, procedures, commodities, competencies, and stakeholder's interactions to examine the legal issues and dangers. The need for cutting-edge and creative legal solutions is necessitated by these changes, which open up new areas of legal protection. Managers are able to add more risk assessment tools and data security to the firm structure thanks to this interdisciplinary approach to the topic of digitization in the sector.

The goal of the study was to identify legal risk factors and examine potential legal issues associated with particular components Industry concept.

Literature Review:

According to Madison (2018), law schools need to teach students how to use technology effectively, as well as management and business skills. They also need to teach students new critical analytical skills. He makes the suggestion that perhaps legal education shouldn't be concentrated solely in law schools. Law schools should no longer only be concerned with preparing students for the bar test. Given that many of these students do not or will only briefly practise law, preparing law graduates for practise should not be the main focus instead of preparing them for a variety of abilities to increase their adaptability.

Simshaw (2018) emphasises that recent law graduates must adjust to the disruption brought on by the age of information. He talks about how automated systems, bots, and predictive analysis are altering how lawyers deliver legal services. Despite the fact that not all activities can be mechanized, AI has had a significant impact on document review, e-discovery, legal research, and in some cases, outcome prediction. According to reports, a system known as ROSS intelligence is the first artificially intelligent attorney in the universe, scanning reams of information per second, sifting through laws, cases, and secondary sources while staying current on local and international legal trends.

Legal Challenges:

Companies embracing Industry technology face problems from cybercrime threats, global corruption, and rapid technological development. Companies must adhere to compliance requirements to guarantee that their operations follow all applicable laws. Compliance criteria should be recognised to include both legal and ethical obligations. Compliance entails carrying out all of the organization's requirements. The organisation must comply with all applicable laws (rules, ordinances, etc.), and there is minimal room for discretion in this area. The organisation must also adhere to a number of voluntary requirements, such as industry or organizational policies, rules, effective governance principles, and ethical and social morals that are accepted within the organisation. In this regard, Industry will force committees and chief compliance officers to be subject to more scrutiny when significant regulatory flaws are identified. A more comprehensive compliance strategy to financial fraud controls, including cybercrime, will be required of organizations.

Whether or not there are specific Industry principles in place will determine the likelihood of a given legal issue. A comprehensive explanation of many technological topics is provided here.

i. Cloud Computing:

The cloud offers some advantages and prospects for business users, who play a significant role in the development of industry, including freedom in collaboration, access to innovative technologies, assistance for digitalization, quickness of adoption, and cost reductions. While taking into account the technological, functional, administrative, and legislative components that the organisation uses to secure

the intended results in information security, these businesses work in a business climate that progressively stresses the importance of cloud and data security.

It is clear from looking at other cloud technology issues that they present customers with a tonne of promise in terms of convenience and usability. However, the architecture presents significant legal difficulties. The law is largely dependent on the idea of territoriality, which can be quite difficult to comprehend in light of contemporary technology.

ii. Internet of Things

The present Domain Name System is the foundation of the worldwide Internet information architecture known as the Internet of Things. The private industry was responsible for driving the growth of the Internet, but now that the Internet of Things has become a worldwide facility, all relevant parties—including govts, the corporate sector, civil society, and international organizations—should be involved in its international management.

Due to technology advancements, the cybernetic environment is continually altering and evolving, which increases the complexity of attacker, the worth of possible targets, and the consequences of attacks, particularly in the case of industry.

Choosing how much to prohibit information sharing out of concern for its privacy is the main issue here. Even when warranted by significant worries about information security, excessively preventive limits on business communications lead to a loss of interoperability. This necessitates stepping up efforts to implement settings that minimise several security issues while maximising interoperability. It is a complicated issue that need for both IT security and legal protection.

A distinctive legal issue in the security field is the Internet of Things. This results in the requirement for a fresh, adaptable method of data security and functionality. The likelihood of linked dangers being impacted is increased when a device is connected to the Internet.

Increased legal security is necessary due to the highly widespread use of critical internet-connected facilities. Changes to the law will be necessary to safeguard entrepreneurs among others. Of course, how challenging it will be will rely on how broad the legal safeguards are that should keep up with the always changing landscape of risks associated with information technology.

iii. Big-data Analytics

In the era of Industry, where networks, systems, users, and digital technology have revolutionized how organizations innovate and compete, big data has a significant impact on businesses. Technological advancement is determined by the production of enormous data sets. However, data security and privacy issues do exist, due to their enormous volume, large bandwidth, and great diversity, and also huge cloud infrastructure, a variety of resources and data structures, collection of data streams, cloud migration, and other factors.

Large data sets pose a legal danger to businesses that handle and store personal data on natural persons. If a big data set contains any personal information, privacy and data protection rules will be applicable to the business. The issue will develop if big data is connected to confidential material or know-how, such as building plans, structures, or manufacturing techniques. Compliance with data protection rules and regulations represents one of the major legal obstacles for business owners looking for large data sets. Additionally, there are special legal hazards associated with big data, including those relating to data

licencing, intellectual property ownership, and competition law concerns about the control of massive, big data sets.

The European Data Protection Act (GDPR), which altered privacy laws, is a major problem in the vast amount of data. The legislation is directly applicable and doesn't have to be imposed via national legislation of each Member State. Member States do, however, still have discretion in several matters. Companies that process and store massive data will have a harder time complying with the GDPR, as well as face stricter accountability requirements. Internal record keeping will be mandated for organizations, and some companies may be needed to designate a data protection officer.

iv. Cyber-Physical Systems:

Cyber-physical systems are engineering concepts that describe systems that rely on the fusion of physical processes with controls, computation, and communications technology. Modern vehicles can be cyber-physical systems with cutting-edge sensors and processing capacity, and the development and use of sophisticated driver aid systems is a result of this. The European Parliament called for the Commission to suggest familiar Union definitions of cyber-physical systems, autonomous systems, smart autonomous robots, and their subcategories in its Resolution of February 16, 2017, with suggestions to the Commission on Civil Legal Principles on Robotic systems, among many other basic rules regarding the development of robotics and artificial intelligence for legal use. considers that the civil liability for harm done by robots is a critical problem that also should be investigated and discussed at the Union level in order to guarantee the same level of effectiveness, openness, and reliability in the application of legal certainty throughout the European Union for the benefits of citizens, customer, and companies alike.

A smart autonomous robot requires a unique legal standing, which must be established. The most advanced robots will have the legal status of electronic beings, necessitating distinct legal examination.

Specific statutory requirements addressing standards, intellectual property rights, data ownership, employment, and liability should be included in measures for an adequate degree of operational safety of the cyber-physical system in an industrial context.

Legal risk analysis

Corporations may question the necessity of abiding by all relevant laws given the global exposure to the legal risk brought on by the Internet and, indirectly, industry, as well as the rights and responsibilities that are frequently at odds with one another and the lack of capacity for law enforcement.

In the production domain, information security is linked to the most of common risk factors. These risks, such as loss of data integrity, are connected to cybercrime. They add that industry may see an increase in risk. The accessibility of real-time data is one reason why the risk management approach must adapt. Existing instruments and tools must be modified for this.

The use of cutting-edge technologies results in the inclusion of the open catalogue of remedies for the danger of legal risks. Examples of the potential legal hazards associated with industry include the following:

- Personal harm
- Loss of property
- Default on a contract
- abuse of personal information
- control issues with machines
- infringement of workers' rights
- Risk of harm or injury
- stealing intellectual property

For instance, ICT, Big Data Analytics, and Cloud Computing may increase the danger of data misuse and intellectual property violation. Information may pertain to design, "know-how," control, or other information about a product. This is especially risky when it comes to items like military components that are subject to export restrictions. Additionally, the list of potential legal ramifications is longer in the context of the Internet of Things and Cyber-Physical Systems because there is a chance that sensors or other components of supervision and control mechanisms in autonomous machining processes, including loading / unloading systems, could be harmed. This may lead to complicated issues with legal liability in the area of personal investigation, property damage, or loss of machine control. This is where there may be business criminal liability.

The likelihood that a specific technological component will support a given legal liability and the number of operational industry technological components that support this issue will determine the probability of the risk's overall occurrence in the structure of a digitised enterprise. Therefore, there is a significant legal danger associated with the widespread adoption of automation and digitalization. It can be decreased by lowering the possibility of danger for a specific technology. This is generally feasible but necessitates collaboration among international legislative bodies. Unpredictability in risk areas also exists, but this is the cost of industrial growth.

Conclusion:

The interdisciplinary nature of the issue was considered in the investigation of the legal difficulties associated with digitization in the context of industry. The study found that applying digital concepts either individually or collectively to realise the idea of industry increases both legal risk and business efficiency. Legal answers should make reference to specific industry technical concepts because they each have unique characteristics. The conversation highlighted a variety of issues brought about by particular technology. Especially with regard to intelligent autonomous robots, there is a challenging issue of legal culpability.

Reference:

1. Lovellette E, Hexmoor H, Rodriguez K. Automated argumentation for collaboration among cyber-physical system actors at the edge of the Internet of Things. Internet of Things 2019;5:84–96.
2. Madison, M. J. (2018). An invitation regarding law and legal education, and imagining the future. U of Pittsburgh Legal Studies Research Paper No 2018-03. Retrieved from https:// papers.ssrn.com/sol3/papers.cfm?abstract_id=3122624.
3. Simshaw, D. (2018). Ethical issues in robo-lawyering: The need for guidance on developing and using artificial intelligence in the practice of law. Hastings Law Journal, 70, 173 – 213.
4. Svantesson DJB. Between a rock and a hard place -An international law perspective of the difficult position of globally active Internet intermediaries. Comput Law Secur Rev 2014;30:348–56.
5. Vassakis K, Petrakis E, Kopanakis I. Big Data Analytics: Applications, Prospects and Challenges. In: Skourletopoulos G, Mastorakis G, Mavromoustakis CX, Dobre C, Pallis E, editors. vol. 10, Cham: Springer International Publishing; 2018, p. 3–20.
6. Wachter S. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. Comput Law Secur Rev 2018;34:436–49. doi:10.1016/j.clsr.2018.02.002.
7. Zhong RY, Xu X, Klotz E, Newman ST. Intelligent Manufacturing in the Context of Industry 4.0: A Review. Engineering 2017;3:616–30.
8. https://atos.net/en/blog/industry-4-0-legal-challenges-methods-overcome
9. https://thehill.com/opinion/judiciary/3520598-in-a-digital-world-industry-4-0-meets-law-4-0/
10. https://www.mondaq.com/turkey/it-and-internet/620026/industry-40-and-its-impact-in-the-legal-world