Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 51 (2020) 938–942

Procedia MANUFACTURING

www.elsevier.com/locate/procedia

30th International Conference on Flexible Automation and Intelligent Manufacturing (FAIM2021)
15-18 June 2021, Athens, Greece.

Legal challenges of digitalization and automation in the context of Industry 4.0

Dorota Habrat[a]*

[a]*University of Rzeszow, Institute of Legal Science, ul. Grunwaldzka 13, 35-068 Rzeszow, Poland*

* Corresponding author. Tel.: +48 17-872-15-68. *E-mail address:* dhabrat@ur.edu.pl

Abstract

The article presents challenges and legal risks that may appear in the industry in connection with the implementation of the Industry 4.0 concept. An interdisciplinary analysis was carried out for the needs of managers and engineering staff. The specificity of digitalization and automation, as well as relationships implicate legal challenges, has been shown. Technology pillars were selected and levels of legal challenges were determined. The discussion included legal challenges related to Cloud computing, Internet of Things, Big data analytics, Cyber-Physical Systems and Information and Communication Technologies. The main legal problems for the technologies of digitalization and automation in Industry 4.0 were pointed out. Legal risk assessment issues for modern technologies used in Industry 4.0 were also analyzed.

Keywords: law, legal challenges, legal risk, Industry 4.0, data protection

1. Introduction

To analyze the legal challenges and risks, Industry 4.0 concept can be understood as a change of strategies, organization, business models, value and supply chains, processes, products, skills, and stakeholder relationships [1]. These changes create space for new areas of legal protection and make it necessary to include advanced and innovative solutions in the law. This interdisciplinary approach to the subject of digitalization in the industry allows managers to provide additional risk management tools and data protection in the structure of the enterprise.

Although the concept of the fourth industrial revolution appeared at the end of the 20th century [2], the Industry 4.0 concept was introduced into the industrial space in 2013 [3]. The concept of Industry 4.0 is intelligent factories that automatically adapt production conditions to the requirements of the order. In this regard, artificial intelligence is a key element because it ensures the ability of a computer or computer-controlled machine to perform various activities by analyzing people's thinking methods and techniques [4].

Analysis of the impact of Industry 4.0 on the market and effects in the area of social sciences is still an unexplored area. As part of this study, potential legal challenges posed by selected industry 4.0 technology pillars were analyzed, and legal risk factors were identified.

The research aimed to analyze potential legal challenges related to selected pillars of Industry 4.0 concept and to identify legal risk factors. Such an analysis can be one of the directions of risk analysis in the management of an enterprise implementing Industry 4.0.

2. The framework of Industry 4.0

The changes resulting from the digital revolution in the process of production and value creation are radical and constitute a real challenge for enterprises. In order not to be left behind, companies need to develop strategies in a timely

10.1016/j.promfg.2020.10.132

manner to take advantage of new digitalization opportunities, improve established processes and develop new business models. This also requires taking into account the legal effects.

The industry must seek to focus its activities on relevant statutory provisions and legal assessments. The legal protection can be used to establish measures to minimize the risk of punishment and liability for all stakeholders as well as for Industry 4.0 [5]. The most important thing is to comply with the law and agreed rules to avoid the risk of liability under criminal and civil law for both companies and their bodies. Since the digital transformation of production and value chains leads to completely new requirements that are not sufficiently covered by the existing legal framework, management risk increases. Data protection and IT security, as well as issues related to corporate responsibility, are important here.

Because aspects related to Industry 4.0 are rarely defined by law, there is no analysis in case law or legal literature. There are areas where legal questions cannot be answered. In such cases, manufacturers and developers must identify and document the potential risks that may result in liability. This will allow in the event of a dispute to prove that they have sought risk minimization before the damage under the current state of the art.

3. Discussion on the legal challenges

Cybercrime threats, global corruption and rapid technological change are challenges for companies implementing Industry 4.0 technologies. Companies must meet compliance standards to ensure that the organization's activities comply with existing regulations. Compliance standards should be understood as both compliances with legal requirements and also ethical standards. Compliance means fulfilling all the obligations of the organization. Requirements that the organization must meet include applicable law (laws, ordinances, etc.) - and there is little freedom in this regard. Besides, the organization must meet various voluntary obligations, such as industry or organizational standards, codes, principles of good governance, as well as social and ethical norms recognized in the organization.

In this regard, Industry 4.0 will cause boards and chief compliance officers to be subject to greater scrutiny when serious regulatory deficiencies are revealed. There will be a greater requirement for institutions to adopt a holistic compliance approach to financial crime controls, inclusive of cybercrime [6].

The Industry 4.0 concept consists of several technology pillars (Table 1) that can be implemented individually or through various combinations [1]. This will decide not only about the different impact on the company's effectiveness but also about the scope of the legal provisions related to them, and thus implies a different legal risk. Depending on the current state of knowledge, applicable legal regulations and legal implications of technology, levels of legal challenges have been assessed, which can be associated with specific numerical values in risk analysis.

Table 1. Technology pillars of Industry 4.0

Technology pillars	Short definition/ characteristics	Level of legal challenges
Cloud computing (CC)	The network of virtual computers hosted outside our firewalls [7].	Medium
Internet of Things (IoT)	Networked interconnection of devices in everyday use that are often equipped with ubiquitous mechanism [8].	High
Big data analytics (BDA)	The large datasets that are not able to be captured, stored, managed and analyzed by typical software tools [9].	Medium
Cyber-Physical Systems (CPS)	A system that can effectively integrate cyber and physical components using the modern sensor, computing and network technologies [10].	High
Information and Communication Technologies (ICT)	Extended IT that highlights unified communications and the integration of telecommunications, as well as other technologies that are able to store, transmit, and manipulate data or information [11].	Low
Other	An open group of technologies including virtual reality, augmented reality, simulations, and other digitalization tools.	Unknown/ unspecified

Thus, the likelihood of a specific legal risk will depend on the existence of a specific pillar of the Industry 4.0 concept, taking into account the weight of the legal challenge level indicator. Below is a detailed discussion of specific technology pillars.

3.1. Cloud computing

For corporate users, who largely contribute to the development of Industry 4.0, the cloud provides some benefits and opportunities, including flexibility of sharing, access to new services, support of digital transformation, speed of implementation and cost savings. However, such organizations operate in a business environment that increasingly emphasizes the importance of cloud and data security - taking into account the technical, operational, control and legal aspects that the organization uses to ensure the desired results in information security [12]. As these issues relate more to data, they will be discussed in more detail in subsection 3.3.

Regarding other cloud technology issues, it can be seen that they offer users enormous potential in terms of convenience and ease of use. However, due to the architecture, it poses serious legal challenges. The law is based largely on the concept of territoriality, which in relation to modern technologies can cause many difficulties in interpretation. Gray in his research [13] pointed out the fact that the law of contract, tort and national regulation might all apply to a claim of breach of privacy in relation to material uploaded to the cloud. Each of the studied by him jurisdictions would approach the issues in different ways, potentially creating significant confusion. He pointed to the

need for international co-operation and agreement on these matters.

3.2. Internet of Things

The Internet of Things is a global, Internet information architecture based on the current Domain Name System. For this reason, Weber [14] proposes to tackle the relevant issues of a regulatory framework from the beginning, in particular, the implementation of an independently managed decentralized multiple-root system and the establishment of basic governance principles are to be envisaged. He formulates these conclusions based on experience with "traditional" Internet management.

It has also been pointed out in the European Union that the development of the Internet of Things cannot be left to the private sector and other regions of the world, but European legislators must be responsible for public policy issues in this matter [15]. In particular, IoT management should be developed and implemented in a manner consistent with all public policy activities related to Internet governance.

The development of the Internet was driven by the private sector, but because the Internet of Things has evolved into a global facility, Internet international management should be done with the full support, i.e. Governments, the private sector, civil society, and international organizations [14].

As the cybernetic landscape is constantly changing and evolving due to technological changes, there is an increasing sophistication of attackers, the value of potential targets and the effects of attacks [16]. This is especially true for industry.

The key problem here is the decision on the extent of restrictions on the exchange of information for fear of their security [17]. The result of too wide and preventive restrictions on enterprise communication, even if they are justified by serious concerns about information security, is the loss of interoperability. This requires intensifying work on introducing settings that reduce many security problems while maximizing interoperability. It is a multifaceted problem that requires IT protection on the one hand and legal protection on the other.

For privacy protection, as privacy regulations around the world have been in operation, the transfer and usage of private data ought to be subject to privacy regulations [18]. Janeček argued in his research [19] that ownership allocation must employ some indiscriminate test that does not treat data subjects as a privileged category of potential owners. At the same time, he showed how this approach could be easily combined with protection. Between two indicators of IoT systems exists key interaction consisting of user privacy on the one hand, and identification technologies used to link and personalize services on the other [20]. Sahmim and Gharsellaoui [8] presented the issues of computer security against potential privacy and security issues that may affect system performance. They showed that laws, rules and regulations to enhance global security should be developed because current government regulations are not well suited to such computer systems.

The Internet of Things is a unique legal challenge in the field of security. This translates into the need for a new, flexible approach to data security and functionality. Connecting the device to the Internet creates the risk of the impact of related threats.

The extremely wide use of sensitive internet-connected facilities requires increased legal security. This will require a change in legal regulations to protect, among other entrepreneurs. Of course, the difficulty will depend on the scope of legal protection that should keep up with the rapidly evolving environment of threats inherent in information technology.

3.3. Big data analytics

Big data has a major impact on businesses in the era of Industry 4.0 since the revolution of networks, platforms, people and digital technology have changed the determinants of firms' innovation and competitiveness [9]. Generating large data sets determines technological development. However, there are problems with data security and privacy due to their huge volume, high speed, high diversity as well as large-scale cloud infrastructure, range of resources and data formats, acquisition of stream data, migration between clouds and others.

Large data sets constitute a legal risk for companies processing and storing data of natural persons. Privacy and data protection provisions will apply to a company if a big data set contains any personal data. The problem will arise when the big data will relate to know-how or other sensitive information, such as constructions, structures or production technologies.

One of the biggest legal challenges for entrepreneurs seeking big data sets is compliance with data protection laws and regulations. Big data also brings specific legal risks related to data, such as data licensing issues, intellectual property ownership, and competition law issues over control of large, big data sets [21].

The important issue in the huge data is the European Data Protection Act (GDPR) which changed privacy laws [22,23]. The regulation applies directly and is not need to be implemented through each Member State's national laws. However, Member States retain discretion in some areas. The GDPR brings with it a greater compliance burden for businesses processing and storing big data and increased accountability obligations. Organizations will be required to introduce internal record keeping and some businesses may need to appoint a data protection officer [24].

3.4. Cyber-Physical Systems

The concept of cyber-physical systems refers to engineering systems that are based on the integration of physical systems with control, computing and communication technologies [25]. Modern vehicles can be cyber-physical systems using advanced sensors and computing power, the combination of which has led to the development and implementation of advanced driver assistance systems [26].

Among other general principles concerning the development of robotics and artificial intelligence for civil use the European Parliament in the Resolution of 16 February

2017 with recommendations to the Commission on Civil Law Rules on Robotics (2018/C 252/25) calls on the Commission to propose common Union definitions of cyber-physical systems, autonomous systems, smart autonomous robots and their subcategories by taking into consideration the following characteristics of a smart robot. Considers that the civil liability for damage caused by robots is a crucial issue which also needs to be analyzed and addressed at Union level in order to ensure the same degree of efficiency, transparency and consistency in the implementation of legal certainty throughout the European Union for the benefit of citizens, consumers and businesses alike.

It is necessary to create a special legal status for a smart autonomous robot. The most sophisticated robots will have the status of electronic persons, which will require separate consideration in law [27]. Fosch-Villaronga and Millard [28] suggested that the concept of legal personality should be extended to robots, mainly to provide a mechanism for applying directly to robots' various obligations that currently apply only to individuals and legal persons such as companies.

Measures for an appropriate level of operational security of the cyber-physical system in an industrial environment should be specific legal provisions regarding standardization, intellectual property rights, data ownership, employment and liability.

3.5. Information and Communication Technologies

The information and communication technology (ICT) industry is at the forefront of Industry 4.0 as an important factor in technological change and progress. With the accelerated pace of technological innovation in the ICT sector, the size of this sector is becoming much larger today than it was a decade ago [29]. This translates into legal challenges in ensuring privacy.

Murphy in her research [30] considers the role of technological and legal solutions ICT-technologies in the context of the fight between privacy and supervision. She discusses how technological changes pose a challenge to privacy protection. It also indicates that there is growing interest not only in legal but also in technological solutions to problems related to privacy. However, it points to the important role of governments in legislating effectively for ensuring privacy. Moreover, one of the characteristic features of internet communication is the role of intermediaries in communication. In legal discourse, online intermediaries are often discussed from the perspective of the intermediary's responsibility [31].

4. Legal risk analysis

The global exposure to the legal risk created by the Internet, and indirectly also by Industry 4.0, combined with often conflicting rights and obligations, and limited possibilities of law enforcement, means that corporations may question the need to comply with all applicable laws [31].

Tupa et al. [32] show that the majority of typical risk factors in the production area are associated with information security. These threats are associated with cyberattacks, such as loss of data integrity, etc. They also state that risk may occur more frequently in Industry 4.0. The risk management process must also change, which is due to, among others, the availability of real-time data. This requires the adaptation of existing instruments and tools.

The use of innovative technologies means that the open catalog of solutions to the risk of legal risks is included. The following are examples of the legal risks which can occur in conjunction with Industry 4.0 [5]:

- Personal injury
- Damage to property
- Breach of contract
- Misuse of personal data
- Loss of control on machines
- Violation of employees' rights
- Risk of injury or damage
- Infringement of intellectual property

For example, Cloud Computing, Big Data Analytics and ICT may be associated with the risk of misuse of personal data and infringement of intellectual property. Data may relate to design, "know-how", control or other product-related information. This is especially dangerous in the case of e.g. military parts subject to export controls. Additionally, in the case of the Internet of Things and Cyber-Physical Systems, the catalog of potential legal risks is broader, as there is a possibility of damage to sensors or other elements of supervisory and control systems in autonomous machining systems, including loading and unloading systems. This can result in a complex problem of legal liability in the field of personal inquiry, damage of property or loss of control on machines. This is where corporate criminal liability may be involved.

Determining the probability of the total occurrence of a given legal risk in the structure of a digitized enterprise will depend on the possibility of the risk occurring for a given technological pillar and the number of functioning Industry 4.0 technological pillars that cause this risk. It follows that the wide implementation of digitalization and automation is subject to high legal risk. Its reduction can be done by reducing the likelihood of risk for a given technology. In most cases, this is possible but requires international legislative cooperation. There are also areas of risk unpredictability, but this is the price of industrial development.

5. Conclusions

The analysis of the legal challenges of digitalization and automation in the context of Industry 4.0 took into account the interdisciplinary nature of the problem. This allowed for the formulation of several general conclusions having a multifaceted reference to the studied subject:

- It is necessary to comply with the law and agreed rules to avoid the risk of criminal and civil liability because of the digital transformation of production results in completely new requirements affecting the increase of management

risk, especially in the field of data protection, IT security, as well as issues related to corporate responsibility.

- Technological pillars implemented individually or in groups to accomplish the concept of Industry 4.0 decides not only to increase the efficiency of the company but also to increase legal risk.
- Legal solutions should refer to individual technological pillars of Industry 4.0, as they are characterized by specific features. The discussion showed a number of problems arising from individual technologies. Especially in the case of clever autonomous robots, there is a difficult problem of legal liability.
- Determining the legal risk in the structure of a digitized enterprise will depend on the scope of digitalization and automation. Reducing the risk of a given technology is an effective way to reduce the total risk. International legislative cooperation is required in this respect, which is reflected in the introduced provisions in the European Union.

References

[1] Büchi G, Cugno M, Castagnoli R. Smart factory performance and Industry 4.0. Technol Forecast Soc Change 2020;150:119790. doi:10.1016/j.techfore.2019.119790.

[2] Rostow WW. Essays on a Half Century: Ideas, Policies, And Action. New York: Westview Press; 1988.

[3] Kagermann H, Wahlster W, Helbig J. Securing the future of German manufacturing industry: Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final Rep Ind 40 Work Gr 2013:1–84.

[4] Kurt R. Industry 4.0 in Terms of Industrial Relations and Its Impacts on Labour Life. Procedia Comput Sci 2019;158:590–601. doi:10.1016/j.procs.2019.09.093.

[5] Hilgendorf E, Seidel U. Legal challenges facing digital value chains – structured solution paths for SMEs. Begleitforschung AUTONOMIK für Industrie 4.0; 2016.

[6] Crime and corruption in the 4th industrial revolution — Financier Worldwide n.d. https://www.financierworldwide.com/crime-and-corruption-in-the-4th-industrial-revolution#.XmaTQ6j6hPZ (accessed March 9, 2020).

[7] Krishnan S, Chen L. Legal Concerns and Challenges in Cloud Computing 2019:12–3.

[8] Sahmim S, Gharsellaoui H. Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: A review. Procedia Comput Sci 2017;112:1516–22. doi:10.1016/j.procs.2017.08.050.

[9] 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. doi:10.1007/978-3-319-67925-9_1.

[10] Zeadally S, Jabeur N. Cyber-physical system design with sensor networking technologies. Institution of Engineering and Technology; 2016.

[11] Zhong RY, Xu X, Klotz E, Newman ST. Intelligent Manufacturing in the Context of Industry 4.0: A Review. Engineering 2017;3:616–30. doi:10.1016/J.ENG.2017.05.015.

[12] Kemp R. Legal aspects of cloud security. Comput Law Secur Rev 2018;34:928–32. doi:10.1016/j.clsr.2018.06.001.

[13] Gray A. Conflict of laws and the cloud. Comput Law Secur Rev 2013;29:58–65. doi:10.1016/j.clsr.2012.11.004.

[14] Weber RH. Internet of things - Need for a new legal environment? Comput Law Secur Rev 2009;25:522–7. doi:10.1016/j.clsr.2009.09.002.

[15] European Union. Internet of Things : an action plan for Europe. Commun From Comm To Eur Parliam Counc Eur Econ Soc Comm Comm Reg 2009:267.

[16] Weber RH, Studer E. Cybersecurity in the Internet of Things: Legal aspects. Comput Law Secur Rev 2016;32:715–28. doi:10.1016/j.clsr.2016.07.002.

[17] Allhoff F, Henschke A. The Internet of Things: Foundational ethical issues. Internet of Things 2018;1–2:55–66. doi:10.1016/j.iot.2018.08.005.

[18] Hou J, Qu L, Shi W. A survey on internet of things security from data perspectives. Comput Networks 2019;148:295–306. doi:10.1016/j.comnet.2018.11.026.

[19] Janeček V. Ownership of personal data in the Internet of Things. Comput Law Secur Rev 2018;34:1039–52. doi:10.1016/j.clsr.2018.04.007.

[20] 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.

[21] Abdullah FM. Privacy, security and legal challenges in big data. Int J Civ Eng Technol 2018;9:1682–90.

[22] European Union. General Data Protection Regulation. Off J Eur Union 2016;59.

[23] Pagallo U. The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection. Eur Data Prot Law Rev 2017;3:36–46. doi:10.21552/edpl/2017/1/7.

[24] Nolan P, Adair M. Rising To The Legal Challenges Of Big Data - Privacy - Ireland 2017. http://www.mondaq.com/Article/593400 (accessed March 5, 2020).

[25] Omidshafiei S, Agha-Mohammadi A-A, Chen YF, Üre NK, How JP, Vian JL, et al. MAR-CPS: Measurable Augmented Reality for Prototyping Cyber-Physical Systems. AIAA Infotech @ Aerosp., Reston, Virginia: American Institute of Aeronautics and Astronautics; 2015, p. 1–13. doi:10.2514/6.2015-0643.

[26] 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. doi:10.1016/j.iot.2018.12.002.

[27] Trentesaux D, Rault R. Designing Ethical Cyber-Physical Industrial Systems. IFAC-PapersOnLine 2017;50:14934–9. doi:10.1016/j.ifacol.2017.08.2543.

[28] Fosch-Villaronga E, Millard C. Cloud robotics law and regulation: Challenges in the governance of complex and dynamic cyber–physical ecosystems. Rob Auton Syst 2019;119:77–91. doi:10.1016/j.robot.2019.06.003.

[29] Chandra AC, Pouchous KI. Information and Communication Technology (ICT) Industry in the Fourth Industrial Revolution. Prospects and Challenges for Workers in Asia-Pacific. UNI-APRO ICTS Conf., 2017, p. 2–33.

[30] Murphy MH. Technological solutions to privacy questions : what is the role of law ? Inf Commun Technol Law 2016;25:4–31. doi:10.1080/13600834.2015.1134148.

[31] 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. doi:10.1016/j.clsr.2014.05.005.