International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 25-12-2023, Accepted: 09-01-2024, Published: 24-01-2024
Volume 6, Issue 1, 2024, Page No. 46-52

The impact of international law differences on cyber security and artificial intelligence applications

Gulde Alparslan
Faculty of Law, University of California Los Angeles (UCLA) School of Law, United States

Abstract
This research aimed to analyze the effects of international law differences on cyber security and artificial intelligence applications. Content analysis and descriptive scanning models were used in the research. A PESTEL analysis was conducted to evaluate the political, economic, social, technological, environmental and legal effects of international law differences on cyber security and artificial intelligence applications. According to the results obtained, differences in international law have negative political and economic effects both on the establishment and implementation of cyber security and on the maintenance of artificial intelligence applications in daily life. On the other hand, in social, technological, environmental and legal terms, international legal differences have positive effects on the continuity of cyber security and artificial intelligence applications and have a developing and driving force. It can be stated that there is an increasing need for studies, field practices and collaborations, especially in the field of international law, and that it is necessary to support the studies to be carried out in this field.

Keywords: International law, artificial intelligence, cyber security, globalization

Introduction

Although the basis of law is the duty to protect the universal and innate rights and freedoms of individuals, the concept of property and the cultural and social structures of individuals and societies internationally cause legal processes to differ [1-3]. In fact, although law originally and fundamentally represents a concept that protects and safeguards the rights of individuals, differences can be seen in both the applications, notions and methods of law, as the perception of rights and freedoms varies according to societies [4-6].

Social and cultural differences are important factors underlying legal system differences; it is possible to state that the definitions and limitations of rights and freedoms cause these differences [7, 8]. At this point, it is necessary to mention the difference between law and justice. As it is known, law is a discipline that ensures the implementation of the rules within a society, preserves the balance of power between the powerful and the weak, but fulfills this protection function within the framework of existing legal regulations. On the other hand, justice aims to be fair and eliminate inequalities between the parties depending on the circumstances. From this point of view, it is not possible to say that everything that is legal is fair or that everything that is fair is legal [9]. A practice may be fair but not lawful. Conversely, an unfair practice may be legal. In short, law regulates the implementation of existing systems and the negativities that arise during the implementation phase, and is a more application and field-based discipline than justice [10, 11]. Therefore, legal processes are closely related to cultural, social and administrative norms and may differ depending on the society.

In fact, there may be differences between societies in the perception of justice. At this point, it is possible to consider the facts that will be subject to justice as fundamental rights and freedoms and rights arising from society and the way of government. Along with the concepts of settled life and property, management systems have also developed differently [12, 13]. Nowadays, forms of government such as monarchy, theocracy, democracy or oligarchy still exist in many countries around the world, and individual rights and freedoms in these forms of government differ for various reasons, especially the structure of the state [14, 15]. One of the important facts brought about by the globalization process is that the interaction between people is much more effective, faster and more abundant than in the past. While societies interacted with each other for different reasons such as trade or wars or disasters in the past, today's increasing communication and transportation opportunities enable different cultures and societies to interact much more easily [16, 17]. As a result, legal process differences are increasingly being questioned and the concept of international law is developing as a scientific discipline that is increasingly coming to the fore.

Security is one of the most important concepts, both from the most primitive form of law to today's modern international law and in all administrative processes. In fact, from the idea of universal humanism to the rights and freedoms of individuals, from the concept of property to social rights, and in the balance between administrative power and the governed, security is one of the most important concepts [18, 19]. Although individuals respect the rights and freedoms of other individuals as a natural right, the main underlying psychological reason is the establishment of a system that will protect them against an attack on their own rights and freedoms. In this respect, security appears as one of the integral parts and duties of law. Security is an important issue that is required not only in daily life and concrete matters, but also in almost every field, including intellectual and industrial production. Especially today, as virtual environments come to the fore and become widespread in all areas of life, the desire to protect basic trust and rights under the name of cyber security emerges.

Many definitions have been made regarding cyber security, and the basic common point of these definitions is the protection of personal data and intellectual industrial virtual

productions, which are a part of the rights and freedoms of individuals in virtual and digital environments [20, 21]. Even if it is not possible to physically limit the rights and freedoms of individuals in virtual environments, there are security-related situations in terms of morale and virtual rights. In addition, the protection of personal data is one of the important points of cyber security in terms of security as well as personal rights and freedoms. Therefore, cyber security has an important place in digital environments and international law.

Digital copyrights are regulated by DSM Directive 2019/790/EU, which was published in 2016 and went into effect in 2019. However, there are significant gaps in the laws governing smart productions and autonomous systems created by artificial intelligence, as well as who owns the system or work. Although the goal of DSM Directive 2019/790/EU is to create a unified digital market, the problem of copyright in AI applications demonstrates that this legislation is also insufficient. There is currently insufficient legislation or information on copyright implementation with reference to the AI Act. Similar flaws in copyrights and artificial intelligence are highlighted in a 2023 publication by the US Copyright Office. The current copyright laws are insufficient, particularly for intelligent things made by self-governing systems.

Although there are studies on the relationship between differences in international law and cyber security, there are not enough studies on the effects of differences in international law on cyber security and artificial intelligence globally. Therefore, this research aims to analyze the effects of international law differences on cyber security and artificial intelligence applications.

Development and Applications of the Concept of International Law

Despite of the fact that international law is a concept with historical roots in scope, it has become a concept that has gained importance today with the developments in internet and transportation technologies and the greater interaction of different nations [22, 23]. In ancient societies, communication and interaction did not occur for different reasons than today, except for trade, war or disputes. However, today, there is a high level of cooperation and relations between different cultures in many fields, from tourism to trade, from cultural and social relations to industrial and economic cooperation. This situation has caused the scope and importance of the concept of international law to increase.

While the basic development of international law progresses with the interaction between people and societies, it has gained serious momentum with the transition to first the industrial society and then the information society, following economic reasons and technological developments after the industrial revolution [24, 25]. In general, considering that the main function of law is to regulate issues related to the balance of power between individuals, more interaction will require more legal processes and practices. For this reason, it is possible to state that the interactions of different cultures and societies, the rapprochement of nations and their unity, especially commercial relations, lay the groundwork for the basic development and applications of international law.

In practice, the most important issues of international law are trade, travel, insurance and citizenship rights [23]. In addition, international law is increasingly turning into a more comprehensive structure with sub-fields of application on many issues, including company mergers, activities of multinational and multicultural companies, taxation, tax return and public services. It can be stated that with globalization and global public awareness, the science and practices of international law have changed in a way to minimize these differences.

The Relationship between Cyber Security and Artificial Intelligence in International Law

While the most important functions of law are to protect people's rights and freedoms, security is one of the most important and indispensable areas of law [26]. The rights and freedoms of individuals, as well as the rights and freedoms of legal structures where individuals come together, and even of countries or regions, need to be protected, and law plays an important role both in terms of protection and in terms of punishment, especially the function of deterring possible violations.

The concept of cyber security includes crimes and violations committed in virtual environments, which occur with virtual environments and are described as cyber, and the security measures taken against them [27, 28]. Technological advances have increased not only the access and use of institutions and organizations serving individuals and individual values, but also the opportunities and possibilities of criminal parties. Moreover, in the cyber environment, individuals' potential to commit crimes may be psychologically easier than in the physical environment, and individuals can commit crimes by hiding their psychological structures and personalities as well as their own identities. Therefore, cyber security can actually be thought of as the criminal code of international law or the entirety of applicable regulations. At the same time, cyber security comes to the fore as a sub-topic of the concept of national security.

In the context of international law, cyber security is an area where it is aimed to prevent crime, punish committed crimes and highlight the principle of deterrence. However, there are serious problems in many issues such as differences in legal regulations between countries, technological proficiency levels, participation in crime, pursuit of crime, and punishment [29, 30]. Today, international initiatives are making many regulations for a more reliable virtual environment and a more effective use of individual rights and freedoms in the near future.

In artificial intelligence applications, cyber security becomes a more complex structure with more sub-domains. Although artificial intelligence applications vary in their fields and purposes, they are basically based on the machine learning system, which receives information through the virtual environment and makes learning and inferences accordingly. At this point, artificial intelligence applications in terms of cyber security constitute a serious discussion area, since the physical boundaries of cyber environments or virtual environments are not clear and vary. Although international initiatives are being taken regarding artificial intelligence today, it can be stated that there is not yet sufficient data and information for cyber security and legal evaluations on an international scale.

PESTEL analysis of Cyber Security and Artificial Intelligence Applications in International Law

Based on the literature review on the effects of international law differences in terms of ensuring artificial intelligence applications and cyber security, artificial intelligence applications are examined from political, economic, social, technological, environmental and legal perspectives.

1. Research Model

By using descriptive scanning model and content analysis methods in the research; scientific research on international law differences, cyber security and artificial intelligence applications, and data on field applications have been compiled. Then, PESTEL analysis was carried out to make a political, economic, social, technological, environmental and legal evaluation of the issue. PESTEL analysis shows the political, economic, social, technological, environmental and legal applicability of any subject, accompanied by literature and field information. Analysis takes its name from the initials of these fields. It is an effective and valid method that is frequently used in qualitative or semi-quantitative analyses.

2. Data Collection Process and Analysis

In the research, studies from the scientific literature, including Web of Science, Scopus and peer-reviewed scientific studies of institutes, and judicial decisions and official regulations were evaluated as primary and secondary data sources. The obtained resources were evaluated using content analysis methods and document scanning methods and analyzed in accordance with each PESTEL dimension.

3. PESTEL Analysis Results

1. Political Evaluation of Cyber Security and Artificial Intelligence Applications in International Law

Politics, in its most general definition and function, is the set of administrative actions implemented by a certain group or person to manage societies. Undoubtedly, much more technical and detailed conceptual definitions about politics are made in the literature. However, when it comes to law and cyber security and artificial intelligence applications, it is necessary to address the struggle and balance of power between politics and law [31, 32]. Because, in the task of maintaining the balance between the administrative power or the powerful and the governed, which is one of the most basic functions of law, the powerful or administrative authority is defined by politics. Politics includes not only the current administration, but also a part of the governing power, even if it is in opposition to the administration.

From past to present, both in politics and political literature and in law literature, the relationship between politics and law has always been that politics directs the public for its own interests and consciously uses all the tools and concepts it can find, including personal rights and freedoms, for its own purposes [33, 34]. In fact, it is expected that those who believe in any subject or ideal will include other people in that belief system. However, history and information about the history of politics and today's practices are evaluated as a perception that politics is under a higher and higher purpose, where individual and group interests are at stake. Although there are differences in legal systems in the international arena, it is possible to state that political aims, methods and results are more similar.

The concept of cyber security is an issue closely related to politics. In politics, the issue of security is the primary basis and fundamental point of both the politicians and the politicians in the country's administration. However, with artificial intelligence applications, even if they are not very different politically, international legal system differences may negatively affect artificial intelligence applications. The fact that differences in the legal system come to the fore with artificial intelligence applications may cause the administration and policy developers to have difficulties in developing new policies. Therefore, differences in international law may cause negative political scenarios in terms of artificial intelligence and cyber applications.

As a result, the political evaluation of cyber security and artificial intelligence applications in international law is based on the relationship between law and politics. Although cyber security and artificial intelligence applications represent the transition process to modern society, politics is still one of the most important social phenomena of modern society today. Studies and basic criticisms on the relationship between politics and law generally focus on the fact that law is opposed to politics or that political purposes generally focus on the use of law for their own interests. From a political perspective, not only law, but also cyber security and artificial intelligence applications can be seen as a tool of social and societal manipulation and management. In this regard, international law differences have the potential to have a negative impact on cyber security and artificial intelligence applications. At this point, policy makers and legislators need to be pushed to move towards more comprehensive and transparently auditable systems.

2. Economic Evaluation of Cyber Security and Artificial Intelligence Applications in International Law

After politics, economy is one of the most important values in managing societies. In fact, in some sources and in some arguments, it is stated that the economy is the most fundamental driving and determining force of management. In all these processes and approaches, the economic crises and their consequences experienced in the world from past to present have a great impact. Throughout human history, in every economic bottleneck, the governments of states have suffered serious weaknesses and either the system or the governments have changed [35, 36]. For this reason, economy is actually one of the indispensable and most important determining concepts of management and individuals' actions.

Economic developments in cybersecurity may be important in two stages. The first of these is the cost of cyber security and the software-hardware expenses required to ensure it, and the second is the cost of the absence or lack of cyber security. Due to its structure and complex nature, cyber security stands out as a sector with high level of knowledge and high added value. Therefore, providing and maintaining cyber security economically requires serious economic contribution and budget. The cost of the absence of cyber security is also related to the protection of economic values and gains. Theoretically, in all cyber attacks, the party organizing the attack wants to gain economic, political or strategic advantage [37, 38]. All these values are identified with the economy in today's global societies. In this context, cybersecurity is actually an economically important issue. Similarly, artificial intelligence is an important issue both in

terms of cyber security requirements and costs, as well as cyber attacks and their consequences.

The economic evaluation of cyber security and artificial intelligence applications in international law may emerge in a way that legal differences and economic differences will come to the fore, which will further strengthen the relationship between economic systems. While artificial intelligence offers individuals the opportunity to access and compile information faster, it also highlights differences more. In this sense, differences in international law may bring about consequences such as a further shift of artificial intelligence applications to places with lower cost, more reliable and higher quality workforce. In this regard, it is possible to state that the effects of international legal system differences on cyber security and artificial intelligence will be negative in the short term.

3. Social Evaluation of Cyber Security and Artificial Intelligence Applications in International Law

One of the most important fundamental criteria in all norms and regulations of law is to ensure and protect order in social life. Essentially, law is a set of values that emerged with the concept of property and the transition to settled life, determining the lines between individuals' freedom areas and revealing the boundaries, relationships and possible violations between these freedom areas [39]. From this point of view, legal norms are closely related to the social structure in the national and international context. Legal regulations are both nourished by and shaped by social values and shape social norms. Therefore, it is possible to state that international law will also be related to social structures in the international context.

Although a general definition has not yet been made regarding the international social structure, it is possible to state that the concept of global public will correspond to this structure. The differences of infrastructures and units within a social structure are also reflected in the legal system. In essence, law aims to minimize differences and ensure that individuals have their rights and freedoms in the freest possible way, but without interfering with the rights and freedoms of other individuals [40, 41]. From this point of view, it is possible to argue that differences in international law will hinder the creation of global public awareness.

The issue of cyber security is an indicator of the perception of threats from legal practices to rights and freedoms, to the rights of individuals, legal entities and groups, and the measures taken against them. Therefore, it is possible to evaluate cyber security as the security of the administration on a national basis, and as the provision of social rights on an individual basis. The effects of international law differences on cyber security practices will undoubtedly be affected by legal process differences. When looking at artificial intelligence applications, these dilemmas and differences will come to the fore if artificial intelligence gets its database from very different units of international law systems.

As a result, social evaluation of cyber security and artificial intelligence applications in international law may enable a greater social understanding of the emerging information society and the development of new social norms and values. In this regard, differences in international law may positively affect the social understanding of cyber security and the response of artificial intelligence applications in the social environment. The common point that stands out in all concepts of artificial intelligence, cyber security and digitalization is that as the transition to the information society increases, the power in the hands of the governed increases compared to the past. In this context, it is possible to say that the impact on cyber security and artificial intelligence will be positive.

4. Technological Assessment of Cyber Security and Artificial Intelligence Applications in International Law

Perhaps the weakest among the topics subject to PESTEL analysis in a legal sense is the field of technology. Technology, as a human science, has always found less space within the discipline of law than other human sciences. Although there have been special applications in some areas such as case law and case files and the storage and evaluation of evidence through judicial systems in recent years, digital technology has always been in second place in legal systems [42, 43]. However, in general, it is possible to argue that technology is relatively more advanced in techniques in detection and litigation systems and in the legal practices of law enforcement forces.

Artificial intelligence and cyber security can be described as products of technology, arising directly from the concept of technology. In fact, cyber security has given serious room for action and capability to parties who are inclined to commit technological crimes [44]. However, despite the ever-increasing types and types of cyber attacks, international cooperation between governments, especially in cyber security, manifests itself in a way that minimizes differences in international law.

The cyber security and artificial intelligence technically exist and that their foundations are related to technology necessitates that legal research, studies and practices focused on these areas also be related to technology. In recent years, in legal systems whose relationship with technology has increased in the storage and sharing of information and documents related to files and cases, cyber security has led the law to address more technology issues [45, 46]. While the areas of law that come to the fore in matters related to cyber security are criminal law and the protection of personal data, in the case of artificial intelligence, although the protection of personal data and criminal law come into play, in addition to these, the law of intellectual and artistic works, authorship, the concept of ownership or It seems that issues such as privacy and human values will also come to the fore. Differences in international law, on the other hand, may have an effect in which these differences will have less impact in terms of technology, and may lead to a transition towards a global legal system for the global public.

Technological evaluation of cyber security and artificial intelligence applications in international law indicates that differences in international law will actually lead to innovations in the field of cyber security and artificial intelligence, and will open the opportunity for positive technological developments in finding the necessary methods to detect and eliminate the differences. New algorithms and new evaluation and comparison systems may be developed in regulating legal system differences and detecting differences in practice. Similarly, new studies, programs and practices may be developed for harmony between different legal systems. Based on all these possibilities, it is possible to argue that international legal

system differences will be a driving force for technologically innovative processes.

5. Environmental Assessment for Cyber Security and Artificial Intelligence Applications in International Law

In the new public management approach, the environment is one of the primary values that are described as global public goods. In the past, every country had the full authority and right to decide on the lands within its borders. Today, the prevailing opinion is that all environmental issues are issues that concern all the people of the world, because the environment is a value that belongs to the entire global public [47, 48]. According to this approach, when international institutions and organizations make evaluations on environmental issues and when legal processes are determined and processed, it is necessary to make a global evaluation within this framework.

Although technologies such as production technologies, transportation, industry and security provide environmental results directly in the production and consumption stages, cyber security and artificial intelligence applications do not directly interact positively or negatively with the environment, at least for now. Instead, it is possible to argue that cyber security and artificial intelligence studies have indirect positive contributions to the environment by increasing the level of communication and internet technologies.

The environmental evaluation of cyber security and artificial intelligence applications in international law brings with it the question of the relationship between environment and technology. Today, the environment is considered a global public good, is taxed accordingly, and is seen as a value belonging to the entire global public in legal processes [49]. Environmental practices may also differ in different nations and legal systems. These differences may lead global public administration and international organizations to take some authoritarian options on artificial intelligence and cyber security. In this regard, it is possible to describe the effects of international law differences on cyber security and artificial intelligence as positive, positive and developmental.

6. Legal Assessment of Cyber Security and Artificial Intelligence Applications in International Law

Although law and justice are closely related concepts, the most fundamental distinction between law and justice is that, although law is a tool for implementing justice, laws are a set of values fed by social and societal values. While legal processes proceed through laws, laws derive their origin from the social structure in which it exists, whether political or cultural and theological. From this point of view, it is possible to see the laws as a road map of legal processes arising from the reality of social life and management paradigms.

While laws are emerging, their main reason is to serve the public, and the primary reason for these services is the protection of public rights and freedoms. Rights and freedoms, on the other hand, are the rights and freedoms shaped within the social structure and human rights, or more generally, the rights that individuals are born with and possess for existential reasons. Law is a tool for their protection, and laws serve as the basic protection.

Regarding cyber security, services such as protection of individuals' personal data, privacy of private life, education and health received through digital environments can be described as universal laws that are least affected by differences in international law. However, relations between individuals and the norms and values of society are areas where there are more differences between international legal systems. In the subject and applications of artificial intelligence, data security, protection of private life and property concepts, especially intellectual and artistic works, are important and prominent concepts. In this respect, differences in international law will direct studies on cyber security and artificial intelligence, which will make it necessary to protect fundamental people and freedoms in different areas.

The legal evaluation of cyber security and artificial intelligence applications in international law may actually develop in a way that the differences between law and justice will become more evident, and therefore the public subject to these legal regulations will seek more rights and freedoms. In this regard, it may be possible to develop new security system rules and regulations and artificial intelligence applications for them, focusing especially on minimizing legal system differences in both cyber security issues and legal practices. In this regard, international legal system differences may have a positive effect on cyber security and artificial intelligence, encouraging development.

Discussion and Conclusion

Although legal regulations and norms in the international arena are close to each other in terms of individual rights and freedoms, practices in daily life may differ due to many different reasons such as the management styles of countries or regions, religious beliefs, cultural values, relations within the social structure or unity of history. In addition, new legal terms and concepts that emerge every day may be affected by these differences. At this point, many issues, from the level of internalization of the new legal developments of the differences of the legal systems in question to the integration into the social structure, find answers and are being studied in the academic field of law.

On the other hand, cyber security, which has emerged with technological advances and especially globalization, and artificial intelligence, which has come to the fore in recent years, are seen as areas where the differences between legal systems are now more discussed and new regulations are needed in the global public context. The common point of the studies carried out in recent years on this subject reveals that, unlike the heavy and cumbersome bureaucratic structure of the past, there is a need for more modern, more pargmatic and solution-oriented legal norms today.

Cyber security is a problem that countries face both nationally and its effects on an individual basis, a subject that has been addressed in more studies in recent years. As virtual environments take more place in the daily lives of individuals, the activities of some malicious individuals or organizations regarding information and data security in the cyber environment are also increasing. To combat this, only regional measures are not sufficient; solution measures must be taken in a global context. From this perspective, more effective solutions can be provided to issues related to cyber security on a plane where international legal differences will gradually converge. In addition, a transition to a joint action plan is required to prevent cyber crimes or to fulfill the penal conditions in case a crime is committed. In this

process, international legal system differences are important in taking global measures against cyber security and implementing action plans.

Artificial intelligence applications, on the other hand, constitute an area where the issue of cyber security is reduced from the national to the individual dimension. Although there are regional and country restrictions on the algorithms used as a basis in artificial intelligence applications, there is a need for more international collaborations in the development, regulation, implementation and monitoring of the results of these algorithms.

In general, according to the findings of the research, international legal differences have political and economic negative effects both on the establishment and implementation of cyber security and on the maintenance of artificial intelligence applications in daily life. On the other hand, in social, technological, environmental and legal terms, international legal differences have positive effects on the continuity of cyber security and artificial intelligence applications and have a developing and driving force. It can be stated that there is an increasing need for studies, field practices and collaborations, especially in the field of international law, and that it is necessary to support the studies to be carried out in this field.

Limitations of the Research

The most important limitation of the research is that there are limited legal studies in the literature on artificial intelligence and cyber security and it is not possible to access quantitative data in this field. However, such studies are needed both to reveal the importance of the subject and the impact of legal differences, as well as for further research and field applications on the subject. For this reason, in the research, deficiencies in the field and literature were pointed out by making inferences based on qualitative data and qualitative methods.

Another important limitation of the research is that there are too many factors and factors of international law differences. For this reason, the research has been discussed within a very broad framework in terms of scope and limitations. More studies are needed in the literature. In this way, it may be possible to conduct studies that will reveal more specific results.

Contributions of the Research to the Field

The main contribution of the research to the field is that it has outputs for both literature and field applications in order to fill a significant gap in the literature, which is a serious deficiency in the field of international law, cyber security and artificial intelligence. The lack of sufficient studies in the field, which is actually a limitation of the research, also shows the contribution of the research to the field.

Another important contribution of the research to the field is that it addresses the subject not only in terms of literature but also in terms of field applications. In this respect, the research has been approached in a pragmatic manner and is important in terms of revealing what is missing in the studies to be carried out in cyber security and artificial intelligence applications and which areas will be more beneficial to focus on.

References

1. Perry S. Hart on social rules and the foundations of law: Liberating the internal point of view. *Fordham L. Rev*,2006:75:1171.
2. Luhmann N. Law as a social system. *Nw. UL Rev*,1988:83:136.
3. Luhmann N. Law as a social system. Oxford socio-legal studies, 2004.
4. Selznick P. Law, society, and industrial justice. Quid Pro Books, 2020, 30.
5. Vago S, Nelson A, Nelson V, Barkan SE. Law and Society: Canadian Edition. Routledge, 2017.
6. Sutton J. Law/society: Origins, interactions, and change. Pine Forge Press, 2001, 474.
7. Podgorecki A. Law and society. Taylor & Francis, 2023.
8. Nader L. (Ed.). Law in culture and society: With a new preface. Univ of California Press, 1997.
9. Vinjamuri L, Snyder J. Law and politics in transitional justice. Annual Review of Political Science,2015:18:303-327.
10. Nagin DS, Telep CW. Procedural justice and legal compliance. Annual review of law and social science,2017:13:5-28.
11. Smith D. Law, justice and the unity of value. Oxford Journal of Legal Studies,2012:32(2):383-400.
12. Kempeneer S, Pirannejad A, Wolswinkel J. Open government data from a legal perspective: an AI-driven systematic literature review. Government Information Quarterly, 2023, 101823.
13. Fernández Villaverde J. Magna Carta, the rule of law, and the limits on government. International Review of Law and Economics,2016:47:22-28.
14. von Daniels D. On monarchy. Critical review of international social and political philosophy,2018:21(4):456-477.
15. Swaine L. The battle for liberalism: Facing the challenge of theocracy. Critical Review,2007:19(4):565-575.
16. Kwon Y. A review on the national culture and its effects on the transportation safety perspectives. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation,2019:13(2):275-281.
17. Vannini P. Mobile cultures: from the sociology of transportation to the study of mobilities. Sociology compass,2010:4(2):111-121.
18. Gharaibeh A, Salahuddin MA, Hussini SJ, Khreishah A, Khalil I, Guizani M, *et al*. Smart cities: A survey on data management, security, and enabling technologies. IEEE Communications Surveys & Tutorials,2017:19(4):2456-2501.
19. Rudalevige A. The administrative presidency and bureaucratic control: Implementing a research agenda. Presidential Studies Quarterly,2009:39(1):10-24.
20. Corallo A, Lazoi M, Lezzi M, Luperto A. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers in Industry,2022:137:103614.
21. Abd Rahim NH, Hamid S, Kiah MLM, Shamshirband S, Furnell S. A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*,2015:44(4):606-622.

22. Nemytina MV, Podmarev AA, Sorokina EA, Chechelnitskiy IV. Review of the international scientific conference «The Law and the Society: evolution in interaction»(28-29 th March, 2014). RUDN Journal of Law,2014:2:414-427.
23. Raustiala K, Slaughter AM. International law, international relations and compliance. International Relations and Compliance. Princeton Law & Public Affairs Paper, 2002, 02-2.
24. Blackie D, M Turner D. Disability in the Industrial Revolution: Physical impairment in British coalmining, 2018, 1780–1880 (p. 241). Manchester University Press.
25. Albritton Jonsson F. The industrial revolution in the Anthropocene. The Journal of Modern History,2012:84(3):679-696.
26. Ogata S, Cels J. Human security-Protecting and empowering the people. Global Governance,2003:9:273.
27. Soceanu A, Vasylenko M, Gradinaru A. Improving cybersecurity skills using network security virtual labs. In Proceedings of the International MultiConference of Engineers and Computer Scientists, 2017, 2.
28. Chadha R, Bowen T, Chiang CYJ, Gottlieb YM, Poylisher A, Sapello A, *et al*. Cybervan: A cyber security virtual assured network testbed. In MILCOM 2016-2016 IEEE Military Communications Conference. IEEE, 2016, 1125-1130.
29. Mačák K. Is the international law of cyber security in crisis?. In 2016 8th international conference on cyber conflict (CyCon). IEEE, 2016, 127-139.
30. Shackelford SJ, Russell S, Kuehn A. Unpacking the international law on cybersecurity due diligence: Lessons from the public and private sectors. *Chi. J. Int'l L.*,2016:17:1.
31. Stevens T. Cyber security and the politics of time. Cambridge University Press, 2016.
32. Cavelty MD. Cyber-security and threat politics: US efforts to secure the information age. Routledge, 2007.
33. Beck T, Demirgüç Kunt A, Levine R. Law, politics, and finance. Available at SSRN 269118, 2001.
34. Reus Smit C. (Ed.). The politics of international law. Cambridge University Press, 2004, 96.
35. Bozeman B, Johnson J. The political economy of public values: A case for the public sphere and progressive opportunity. The American review of public administration,2015:45(1):61-85.
36. Horn MJ. The political economy of public administration: Institutional choice in the public sector. Cambridge University Press, 1995.
37. Spremić M, Šimunic A. Cyber security challenges in digital economy. In Proceedings of the World Congress on Engineering. Hong Kong, China: International Association of Engineers,2018:1:341-346.
38. Venkatachary SK, Prasad J, Samikannu R. Economic impacts of cyber security in energy sector: A review. International Journal of Energy Economics and Policy,2017:7(5):250.
39. Brooks CW. Law, politics and society in early modern England. Cambridge University Press, 2009.
40. Buzan B. From international system to international society: structural realism and regime theory meet the English school. International organization,1993:47(3):327-352.
41. Musolf GR. Social structure, human agency, and social policy. International journal of sociology and social policy,2003:23(6/7):1-12.
42. Brenner S. Law in an era of smart technology. Oxford University Press, 2007.
43. Zittrain J. Law and technology The end of the generative internet. Communications of the ACM,2009:52(1):18-20.
44. Ponkin IV, Redkina AI. Artificial intelligence from the point of view of law. RUDN Journal of Law,2018:22(1):91-109.
45. Watney MM. Artificial intelligence and its' legal risk to cybersecurity. In European conference on cyber warfare and security. Academic Conferences International Limited, 2020, 398-405.
46. Shamiulla AM. Role of artificial intelligence in cyber security. International Journal of Innovative Technology and Exploring Engineering,2019:9(1):4628-4630.
47. Morrisette PM. Conservation easements and the public good: preserving the environment on private lands. Nat. Resources J,2001:41:373.
48. Sagoff M. Aggregation and deliberation in valuing environmental public goods:: A look beyond contingent pricing. Ecological economics,1998:24(2-3):213-230.
49. Tavas B, Tekiner Mave, Yılmaz K. *AB Uyum Sürecinde Sınır Güvenliği ve Yönetim Stratejisi.* Sage Yayıncılık Reklam Mat.San. ve Tic.LTD.ŞTİ, 2016.