ARTIFICIAL INTELLIGENCE AND THE NEW CHALLENGES FOR EU LEGISLATION[*]

Prof. Dr. Z. Seldağ GÜNEŞ PESCHKE[**]

Dr. Öğr. Üyesi Lutz PESCHKE[***]

ABSTRACT

Artificial Intelligence is one of the most debated topics of the last decade which is developed by the new technological changes. With the introduction of AI into our daily lives, discussions occurred on machine learning and the legal and ethical issues governing artificial intelligence. At that point, conflicting situations emerged regarding the use of AI technologies, especially data issues and bias. In 1995, European Data Protection Directive, EU Directive 95/46 was passed which regulated the processing of personal data within the borders of EU and provided data privacy and security standards for the individuals. The Directive was repealed on 25th May 2018 by General Data Protection Regulation (GDPR), which brings new concepts with more strict rules on the protection of personal data. Due to its legal nature, GDPR includes binding rules not only for EU countries but also for those who carry out all activities related to data processing inside EU. With the development of technology and depending on different IT techniques, data processing has changed and access to data became easier than ever. As a result of these technologies, the concepts of big data and artificial intelligence have been widely discussed and the development of new electronic devices and the implementation of more use of robots have brought some legal questions into practice. Recently, there are some new regulations that seem likely to enter EU legislation in the next years, such as Artificial Intelligence Act, Data Governance Act, Data Act, and European Health Data Space. There is uncertainty for the next years, about how new regulations will affect each other including GDPR. This paper aims to discuss artificial intelligence, including GDPR and the new legal developments in the EU legislation within the technological implementations.

Key Words: Artificial Intelligence, Data Processing, EU Legislation, GDPR, Big Data.

---

[*] DOI: 10.33432/ybuhukuk.1104344 – Geliş Tarihi: 15.04.2022 - Kabul Tarihi:19.08.2022.

[**] Ankara Yıldırım Beyazıt University, Faculty of Law, Proffessor Dr., speschke@ybu.edu.tr, ORCID: 0000-0003-3679-6525.

[***] Ihsan Dogramaci Bilkent University, COMD, Assistant Professor, lutz.peschke@bilkent.edu.tr, ORCID: 0000-0002-9513-3257.

YAPAY ZEKA VE AB MEVZUATI İÇİN YENİ ZORLUKLAR

ÖZET

Yapay zeka, son yıllarda yeni teknolojik değişimlerle birlikte gelişen teknik konulardan biridir. Yapay zekanın günlük hayatımıza girmesiyle, makina öğrenmesi ve yapay zekayı yöneten yasal ve etik konular üzerine tartışmalar yaşanmaktadır. Bu noktada, yapay zeka teknolojilerinin kullanımı ve özellikle kişisel verilerin korunmasıyla ilgili çelişkili durumlar ortaya çıkmaktadır. 1995 yılında, kişisel verilerin AB sınırları içinde işlenmesini düzenleyen ve bireyler için veri gizliliği ve güvenlik standartları sağlayan 95/46 Avrupa Veri Koruma Direktifi kabul edilmiştir. Direktif, kişisel verilerin korunmasına ilişkin daha katı kurallar ve yeni kavramlar getiren AB Genel Veri Koruma Tüzüğü (GDPR) ile 25 Mayıs 2018 tarihinde yürürlükten kaldırılmıştır. GDPR , hukuki niteliği nedeniyle sadece AB ülkeleri için değil, AB içinde veri işleme ile ilgili tüm faaliyetleri yürütenler için de bağlayıcı kurallar içermektedir. Son yıllarda, teknolojinin gelişmesi ve farklı teknolojilere bağlı olarak verilerin işlenmesi teknik olarak değişmiş ve verilere erişim hiç olmadığı kadar kolaylaşmıştır. Bu teknolojilerin bir sonucu olarak, büyük veri ve yapay zeka kavramları ortaya çıkmış, yeni elektronik cihazların geliştirilmesi ve robotların daha fazla kullanılmaya başlanması ile yapay zeka kavramı günlük hayatımıza girmiştir. Ancak, bu gelişmelerle birlikte yapay zeka kullanımı ve data işlenmesine ilişkin bazı yasal sorular da ortaya çıkmıştır. Son zamanlarda, taslak olarak hazırlanan Yapay Zeka Tüzüğü, Veri Yönetişim Tüzüğü, Veri Yasası ve Avrupa Sağlık Veri Alanı gibi önümüzdeki yıllarda AB mevzuatına girmesi muhtemel görünen, bazı yeni düzenlemeler bulunmaktadır. GDPR dahil olmak üzere, bu yeni düzenlemelerin birbirlerini nasıl etkileyeceği konusunda belirsizlikler vardır. Bu makalede, teknolojik uygulamalar çerçevesinde, Genel Veri Koruma Tüzüğü dikkate alınarak, yapay zekanın AB mevzuatında gelişimi ve önümüzdeki yıllarda AB'de yürülüğe girmesi planlanan, yeni hukuki düzenlemelere ilişkin değerlendirmelerde bulunulmuştur.

Anahtar Kelimeler: Yapay Zeka, Veri İşleme, AB Mevzuatı, Genel Veri Koruma Tüzüğü, Büyük Veri.

INTRODUCTION

Artificial Intelligence is one of the increasing topics of the last decade which is developed by the new technological changes. There are many descriptions of AI, but broadly it is defined as a computerised system exhibiting behaviour thought of as requiring intelligence[1]. AI cannot be considered a single technology, but it is declared a scientific discipline that gathers as a set of technologies. European Commission's High-Level Expert Group on Artificial Intelligence has defined it as systems which display intelligent behaviour, analyse their environment and take actions for several specific goals.

With the introduction of AI into our daily lives, discussions occurred on machine learning and the legal and ethical issues governing artificial intelligence. At that point, conflicting situations emerged regarding the use of AI technologies, especially data issues and bias. A group of techniques like knowledge representation, reasoning, planning, and optimization are used to perform the data coming from the sensors. As AI systems depend on huge amounts of data for good performance, if the data is not well balanced or inclusive enough, it may cause some unfair decisions and may be in favour of some groups against others. This situation affects the implementation of AI and can change the application of some existing rules.

Artificial intelligence is a human-designed system, that collects structured or unstructured data in the physical and digital world, reasoning the knowledge from these data and decides the best option for the given goal. The development and operation of AI must be regulated clearly by norms concerning the principles of democracy and the fundamental rights of individuals. There is a very close link between AI and data, as in the process of AI big amount of data is gathered. At this point, data protection becomes an important issue on a global level. Many regulations are put into force by the states not only at the national level, but also at the international level for the control of data.

[1] **Walters, Robert/Novak, Marco** (2021) Cyber Security, Artificial Intelligence, Data Protection & the Law, Springer, Singapore, p.41.

After the EU 95/46 Directive, in 2018, GDPR was enforced to strengthen data protection in all EU states. Non-EU countries also started bringing their data protection regulations closer to that of the GDPR which is derived from the Data Protection Directive 95/46 and also from Council of Europe Convention no 108 on data protection. Right now, there are new drafts that seem likely to enter into EU legislation in the next years, such as Artificial Intelligence Act, Data Governance Act, Data Act, and European Health Data Space. At this point, there is uncertainty about how new regulations will affect each other including GDPR. This paper aims to discuss artificial intelligence and the new legal developments in the EU legislation within the technological implementations.

I. AI IN THE CONTEXT OF DATA PROCESSING

From the beginning of the digital age, technology is developing very rapidly, however, legal rules follow these technological changes to make the necessary arrangements according to the needs. The production of new electronic devices and the implementation of more use of robots have brought some legal questions into practice[2].

With the development of technology and depending on different IT techniques, data processing has changed and access to data became easier than ever. As a result of these technologies, the concepts of big data and artificial intelligence have been widely discussed legally by jurists, legal scientists and legislators.

Recently, new drafts have been prepared in European legislation, such as Artificial Intelligence Act, ePrivacy Regulation[3], etc. in parallel with technological developments, on the one hand, to protect the individuals, on the other hand, to regulate the technology. These new regulations may have a direct

[2] **Lucchi, Nicola** (2016) The Impact of Science and Technology on the Rights of the Individuals, Law, Governance and Technology Series 26, Springer, p.4; **Edwards, Lilian** (2019c) "Data Protection and e Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling", Law, Policy and the Internet (Ed. Lilian Edwards), Hart, UK, p.120.

[3] **Specht, Louisa/Mantz, Reto** (2019) Handbuch Europisches und deutsches Dateschutzrecht, Beck, Munich, p.129.

impact on the GDPR as well as, cause mandatory changes in the existing provisions because of data processing activities.

A. THE CONCEPT OF ARTIFICIAL INTELLIGENCE

With the implementation of the internet, data has become one of the greatest powers in our lives. The manufacturing of driverless cars started after the 1950s. AI technologies were used generally in the production phase of smart cars. The big automobile companies like General Motors in 1958, and the Japanese Tsubuka Mechanical Engineering Laboratory in 1977 produced their prototypes. These activities continued with Ernst Dickmann's autonomous land vehicle and many more examples. Lately, Elon Musk introduced a fully self-driving autopilot from Tesla[4].

Although the first examples of artificial intelligence were used in smart cars, recently AI technology is applied to many other electronic devices. AI technologies support the engineering of systems that have a degree of autonomous agency. Today AI systems are frequently used at all levels of daily life, from everyday activities to professional work[5] such as in IoT[6] devices, health care, banking, and especially in smart cars.

There is not only one agreed description of AI, broadly it is defined as a computerised system exhibiting behaviour thought of as requiring intelligence[7]. AI cannot be considered a single technology, but it is declared a scientific discipline that gathers as a set of technologies. AI refers to systems that indicate intelligent behaviours and analyses their attitudes and actions to obtain specific

---

4 **McLachlan, Scott/Kyrimi, Evangelia/Dube, Kudakwashe/Fenton, Norman/Schafer, Burkhard** (2022) "The Self-Driving Car: Crossroads at the Bleeding Edge of Artificial Intelligence and Law", Cornell University, Workingpaper. <https://8303d3e493133b9b937b9684793ab2f814c189c3.vetisonline.com/abs/2202.02734>

5 <https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy>

6 **Serpanos, Dimitrios/Wolf, Marilyn** (2018) Internet of Things – IoT Systems Architectures, Algorithms, Methodologies, Springer International Publishing; **Sönmez Çakır, Fatma/Aytekin, Alper/Tüminçin, Alper Fatma** (2018) Nesnelerin İnterneti ve Giyilebilir Teknolojiler, Sosyal Araştırmalar ve Davranış Bilimleri Dergisi, C:4, S:5, s.85.

7 **Walters/Novak,** p.41.

goals[8]. The system which is based on AI can be software-based, operating in the virtual world like, search engines on the internet, fingerprint or recognition of face systems, or voice assistants. Additionally, AI can be in hardware devices, like robots, autonomous cars, drones or Internet of Things applications.

Today, Big data is increasingly growing all over the world. It is important to integrate legal and ethical norms of big data and artificial intelligence into our daily lives. At that point, a big amount of data is processed during a huge variety of digital activities. The studies in this context show that norms on Big Data and artificial intelligence should be set for the regular data flow inside the society which guides the governments, users, and companies.

B. GDPR AND DATA PROCESSING

Personal data is a fundamental human right, which was mentioned in the UN Universal Human Rights Declaration in 1948 and the European Human Rights Convention in 1950[9]. Also, the judgments or decisions given by ECrtHR, have strengthened the legal character of data protection and privacy in EU legislation[10]. Understanding privacy is a very complex challenge since it is dependent on the development of information and communication technologies. Basic principles of privacy are mentioned in the European Charter of Fundamental Rights, as well as in Article 8 of the European Convention on Human Rights[11]. According to Edwards, privacy is a cultural concept interpreted diversely in different countries assuming different connotations. People have certain expectations according to their national

---

8 **Do Carmo, Tania/Rea, Stephen/Conaway, Evan/Emery, John/Raval, Noopur** (2021) In: Law and Policy, V:43, Issue 2 (April 2021), p.176.

9 **Güneş Peschke, Seldağ/Sayan, Ömer Fatih** (2021) "A Comparative Study of Privacy Policies and Data Protection During the COVID-19 Pandemic Within Different Countries", CORONALOGY: Multidisciplinary Academic Analysis in Perspective of Covid-19 (Eds Sefer DARICI, Ayşe Meriç YAZICI), De Greuter – Sciendo.

10 **Güneş Peschke, Seldağ** (2014) The Protection of Personality Rights From Roman Law Till Today, Ankara, Yetkin.

11 **Edwards, Lilian** (2019a) "Privacy and Data Protection1: What is Privacy? Human Right, National Law, Global Problem", Law, Policy and the Internet (Ed. Lilian Edwards), Hart, UK, p.52.

origin[12]. For that reason, it is not surprising that privacy laws differ from country to country by cultural differences[13].

Over the years, many national and international regulations were enforced in this regard. EU has regulated data protection Directive 95/46/EC in 1995 on the protection of individuals concerning the processing of personal data and on the free movement of such data to unify the data protection in Europe[14]. 95/46/EC was an important component of EU privacy and human rights law which was applied to national provisions of all member states concerning fundamental rights and freedoms of natural persons.

95/46/EC was replaced with the Regulation (EU) 2016/679 which is known as the General Data Protection Regulation (GDPR) by the European Parliament in 2016. Today, GDPR is the main regulation of the EU on the protection of personal data which was enforced in all Member States and has become a law that is directly applicable in all EU member states after 25 May 2018 without requiring implementation through national laws.

GDPR is not only a regulation which strengthens the rules of the 95/46 EU Directive but also introduces new ones. Most of the principles of GDPR date back to the former data protection directive 95/46 EC and sometimes to the Council of Europe Convention 108 (1981).

Therefore, there are differences between a directive and a regulation in the hierarchy of laws. Regulation is applied across all EU member countries once it is initiated without the need for the country by country to implement them. GDPR is a body of law, extraterritorial which the EU imposes its privacy

---

12 **Edwards**, p.71.

13 **Greenleaf, Graham** (2012) "Korea's New Act: Asia's Toughest Data Privacy Law", 117 Privacy Laws & Business International Report, pp.1-6.

14 **Güneş Peschke, Seldağ/Peschke, Lutz** (2013) "Protection Of The Mediatized Privacy In The Social Media: Aspects Of The Legal Situation In Turkey And Germany", Gazi Üniversitesi Hukuk Fakültesi Dergisi C:17, S:2, s.873.

norms on the wider world. The operators outside of Europe should also comply with the Regulation[15].

GDPR rules are applied to all relevant organizations regardless of size and this regulation protects all relevant individuals. Processing of personal data of the individuals in EU even the data controller or data processor who is not in the EU should also be subject to GDPR, as their behaviors are in the EU.

GDPR regulates data processing activities under several principles, related to data management and data processing from obtaining user consent to handling data breach situations[16]. Data protection activities based on lawfulness under Article 6 of GDPR are implemented transparently and securely which protects the dignity and the autonomy of the individuals, ensuring that fair and lawful processing can take place. There are several cases of the infringement of privacy according to ECHR Article 8 which includes data processing activities[17].

The consent of the individual and the legitimate interest are kept in balance under a good legal reason for the data processing activities. In this data flow, the shared private data should be kept confidential[18]. In GDPR it is mentioned that data can be processed only under some conditions[19]. These principles can be summarized as fair processing; purpose specification; the need for a legitimate basis, such as consent of a person, the right of access; the right to have data rectified; and independent supervision[20].

---

15 **Edwards, Lilian** (2019a) "Privacy and Data Protection1: What is Privacy? Human Right, National Law, Global Problem" Law, Policy and the Internet (Ed. Lilian Edwards), Hart, UK, p.65.

16 **Arat, Tugay/Aslan, M. Mert** (2021) "Sosyal Medyada Veri Güvenliği ve Kişisel Mahremiyet Sorunu", Akdeniz Üniversitesi İletisim Fakültesi Dergisi, S:35, p.390.

17 Gaughran v. The United Kingdom *(Application No.45245/15),* 3/06/2020; Breyer v. Germany *(Application No. 50001/12)* 07.09.2020; Case Of Szabó And Vissy v. Hungary *(Application No. 37138/14)* 06.06.2016.

18 **Arat/Aslan,** p.390.

19 **O'Doherty, Michael** (2020) Internet Law, Bloomsbury Professional, Croydon, p.202.

20 **Fuster, Gloria González**, (2014) The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer, Brussels, p.4.

EU Data Protection regime is binding sometimes for other non-EU legal systems and implement laws similar in broad ways to data protection. Data cannot be exported from EU countries which have not been certified as "adequate" according to EU rules that aim to protect the personal data of EU citizens[21].

GDPR requests reasonable data protection measures from organizations for the protection of the personal data of persons. Processing of data, their conditions, the provisions on data destruction and related issues with data are also subject to strict conditions under GDPR and hard sanctions are applied to those who do not comply with the provisions of the regulation[22]. For instance, Peschke et al. (2022) described relevant circumstances and requirements in the context of COVID-19 tracking applications (CTA) during the pandemic[23]. Accordingly, decentralized and anonymized data storage in combination with voluntary usage is the prerequisite for compliance.

To sustain the functioning of data protection, European Data Protection Board (EDPB) is established as an independent body according to GDPR. The Board has representatives from the national data protection authorities and the European Data Protection Supervisor (EDPS). EDPB is founded to ensure the implementation of GDPR by providing legal guidance, advice and compliance with the promotion of cooperation within the national authorities.

In the strategic plan for 2021-2023, EDPB underlines three key issues for the application of data protection rules in the member states and beyond EU borders. For advancing harmonisation and facilitating compliance, EDPB aims to give guidance on key notions on the scope of data subjects' rights and develop tools which help to implement data protection into practice[24]. EDPB monitors

---

21 **Edwards, Lilian** (2019b) "Data Protection: Ener the General Data Protection", Law, Policy and the Internet (Ed. Lilian Edwards), Hart, UK, p.78.

22 **Simitis, Spiross/ Hornung, Gerrit/ Döchmann, Indra Spieker genannt (2019)** Datenschutzrecht, Baden Baden Nomos Kommentar, Nomos, p.29.

23 **Peschke, Lutz/ Güneş Peschke, Seldağ/ Gümüş Ağca, Yasemin/ Seyfafjehi, Seyedehshahezad/ Dündar, Irmak/ Aydoğdu, Yasin** (2022) "Reward Mechanisms In COVID-19 Tracking Apps And Its Impact On The Voluntary Participation Of The Public In Sustainable Innovation Processes", Türkiye İletişim Araştırmaları Dergisi, S:39, s.54-72.

24 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_strategy2021-2023_en.pdf>

the new technologies by the fundamental rights, human dignity and liberty. For that reason, EDPB aims to work more often with the policymakers to set high EU and global standards for international data transfers between the EU and third countries. In this context, the cooperation between national supervisory authorities is strengthened and coordination between them is promoted.

European Data Protection Supervisor (EDPS) is another independent authority which is based on the regulation 2018/1725 (EU) that monitors the applications of data protection rules within the EU institutions and investigates complaints on related topics. With these institutions, the EU aims to provide better implementation on the protection of personal data Europe-wide.

Fairness, legitimacy and transparency are the key principles of data processing which is mentioned in GDPR. In this sense, big data challenge purpose limitation since the key intent is to reuse personal data for unseen purposes[25]. Edwards considers big data as the twin sister of machine learning by algorithmic systems which involve statically patterns in Big Data in the form of training datasets, building models out of those patterns and using new data inputs to classify them[26].

II. THE CONCEPT OF ARTIFICIAL INTELLIGENCE AND ITS DEVELOPMENT IN LAW

A. AI AND THE LEGAL TERMINOLOGY OF EU LEGISLATION

Lee Loevinger who was a supreme court judge from Minnesota first mentioned the relation of law inspired by computational methods in 1949[27]. After that time so many discussions appeared on AI and Law, as a result of developments of new computational methods and techniques for legal reasoning and argumentation. Kevin Ashley and Edwina Rissland pointed out

[25] **Mayer-Schönberger, Viktor/Cukier, Kenneth** (2013) Big Data: A Revolution that will Transform How We Live, Work, and Think, London, John Murray, p.15.

[26] **Edwards, Lilian/Veale, Michael** (2017) "Slave to the Algorithm? Why a "Right to an Explanation" Is Probably not The Remedy You Are Looking For", 16 Duke Law&Technology Review 18, pp.24-27.

[27] **Loevinger Lee** (1949) "Jurimetrics: The Next Step Forward" Minnesota Law Review (1796), V:44, N:4.

case-based and rule-based legal reasoning with cases and hypotheticals by using elementary logic and relevant differences and similarities of cases[28]. It is clear that to develop intelligent legal information systems, there is a need for information models, algorithms and a language for legal terminology.

In the research of McCarty on Law and AI, he underlined the need for a special language which represents contents, actions and events[29]. In Europe, EU legislation produces its legal terminology which generates intra-linguistic issues.

Today, AI is not only shaping the contours of the law, but also the legal practice. The usage of legal terminology in AI is discussed to operate intelligent legal information systems as a model using computational techniques to inform practitioners and citizens about legal issues[30]. Semantic Web is the extension of the World Wide Web (Web 3.0) which aims to make the internet data machine-readable, and is used as an infrastructure to AI as a precondition to developing AI applications in the legal process for the Law domains, taking into consideration "law on the books" and "law in action".

Mc Carty discussed if it is reasonable to build a computational theory of legal arguments and the need for a language which can represent concepts, states, events, and actions based on legal reasoning and legal argumentation[31]. Later on, some other scholars also conversed about the combination of data systems, algorithms, and the adoption of knowledge in "case-based" and "rule-based" systems[32].

---

[28] **Rissland, Edwina/ Ashley, Kevin** (1987) "A case-based system for trade secrets law", In: Proceedings of the First International Conference on Artifcial Intelligence and Law, pp.60–66 ACM Press.

[29] **McCarty, L. Thorne** (1990) "Artificial Intelligence and law: How to Get There From Here" Ratio Juris, V:3, Issue 2, p.194.

[30] **McCarty, L. Thorne** (1984) Intelligent legal information systems: problems and prospects In: Campbell C (ed) Data processing and the Law Sweet and Maxwell, London, pp.125–151.

[31] **McCarty** (1990), p.190.

[32] **Ashley, Kevin** (2011) the case-based reasoning approach ontologies for analogical legal argument. In: Sartor G, Casanovas P, Biasiotti M, Fernández-Barrera M (eds) Approaches to legal: ontologies law governance and technology series. Springer, Dordrecht; **Ashley, Kevin** (1991) Reasoning with cases and hypotheticals in hypo Int J Man Mach Stud 753–796;

The importance of terminology or legal borrowing which means the relocation of legal terms from one legal system into another or from one language into another exceptionally put in use in comparative law[33]. In the intersection of AI and law, the main question is focused on if a unique legal terminology is a solution to express the meanings of legal institutions in a better way in each country.

As the EU is made up of 27 states, the EU market is nearly 500 million people which is the third largest world population after China and India. EU legislation is based on multilingualism. In 27 states, 24 different languages are spoken. Multilingualism brings a process of translation over the EU legislation and autonomous interpretation throughout the Member States. So, in the formation of new regulations, it can be a solution to use the same legal terminologies in different languages to keep the same meanings of the institutions.

B. THE USE OF AI IN LEGAL TECH

Big data and Artificial Intelligence (AI) are permeated not only in our social lives, but also their usage is increasing in legal practice and processes. As a terminology, "Legal Tech" is used for any algorithm–based technology in legal issues which consists of all information technology in the legal field and related to data. Today, AI in the legal process goes from machine learning to machine

Walton, Douglas (2006) Fundamentals Of Critical Argumentation, Cambridge Cambridge University Press,Cambridge; **Savelka, Jaromir/Westermann, Hannes/ Benyekhlef, Karim/ Alexander, S. Charlotte/ Grant, Jayla/Amariles, David/Hamdani, Rajaa/Meeùs, Sebastien/Troussel, Aurore/ Araszkiewicz, Michal/Ashley, Kevin/Ashley, Alexandra/Branting, Karl/Falduti, Mattia/Grabmair, Matthias/Harašta, Jakub/Novotná, Tereza/Tippett, Elizabeth/Johnson, Shiwanni** (2021) "Lex Rosetta: Transfer Of Predictive Models Across Languages, Jurisdictions, And Legal Domains" In: ACM (Ed.) Proceedings Of The Eighteenth International Conference On Artifcial Intelligence And Law, pp.129–138.

[33] **Fuster,** p.9.

lawing[34]. Recently, AI has started to be used in legal practice[35] generally for illumination of contracts, generation of good contracts, conducting legal research, recommendations for judicial decisions about sentencing or bail, and warning attorneys against legal errors mostly by law companies, public or private institutions, and state organizations[36].

AI can make decisions rapidly in domains involving millions of variables such as searching for the most relevant answer to a query or assessing an appropriate sentence for a crime[37]. Moreover, decision-making[38] or consulting applications are being used in law, such as Lexis Answers or Lexis Answer Card where legal questions are asked and answered with the best legal solutions[39].

Many German Federal States have started testing softwares named Precobs (Pre Crime Observation System) and SKALA (System zur Kriminalitätsanalyse und Lageantizipation) that analyses certain criminal cases to estimate the person's likelihood to return to crime[40]. However, AI is not yet ready to replace human judgment in the legal profession, although there are pilot implementations in China which are recommended by the Chinese State Courts[41].

---

34 **Buchholtz, Gabriella** (2020) "Artificial Intelligence and Legal Tech: Challenges to the Rule of Law", Regulating Artificial Intelligence (Eds. Thomas Wischmeyer/ Timo Rademacher) Switzerland, Springer, pp.177.

35 **Çekin, Mesut Serdar** (2021) Yapay Zeka Teknolojilerinin Hukuki İşlem Teorisine Etkileri, 1.Baskı, İstanbul, On İki Levha Yayıncılık, s.30-31.

36 **Erdoğan, Gökhan** (2021) "Yapay Zekâ Ve Hukukuna Genel Bir Bakiş", Adalet Dergisi, S:66 s.130; **Buocz, Thomas Julius** (2018) "Artificial Intelligence in Court Legitimacy Problems of AI Assistance in the Judiciary", Retskraft – Copenhagen Journal of Legal Studies, V:2, N:1, p.46; **Zeytin, Zafer/Gençay, Eray** (2019) "Hukuk ve Yapay Zekâ: E-kişi, Mali Sorumluluk ve Bir Hukuk Uygulaması", Türk Alman Üniversitesi Hukuk Fakültesi Dergisi, C:1, S:1, s.42.

37 **Edwards** (2019c), p.141.

38 **Ulenaers, Jasper** (2020) "The Impact of Articial Intellgence on the Right to a Fair Trial: Towards a Robot Judge?", Asian Journal of Law and Economics, V:11 No:2, pp.1.

39 **Sümer, S. Yağmur** (2021) "Ceza Yargılamasının Geleceği: Robot Hakim" Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C:23, S:2, s.1545; **Walters, Robert/Novak, Marco**, p.44.

40 **Buchholtz**, p.180.

41 <https://law.asia/ai-in-courts-paves-way-for-efficiency-consistency-in-china> (s.e.t. 15.06.2021)

In litigations, the judge must decide according to his/her conscientious opinion. Because of the judge's discretion as a human being and the application of equity principles, it seems difficult to use AI in the decision-making processes in the courts, but advisory decisions can be taken.

III. ENTRY OF AI IN EU LEGISLATION AND FORTHCOMING REGULATIONS

A. AI IN EU LEGISLATION

Considering the future developments, in the 1980s the International Association of AI and Law (IAAIL) was founded to support and develop AI regulations at the international level. Since then, the EU has been dealing with the new regulations on AI, data protection, and privacy concerning fundamental rights and human rights principles. It is considered as there is a direct link between new technologies, social change and law.

Without internet access, there is no content, application or service. Lessig's "Code and Other Laws of Cyberspace" [42] is one of the most significant books on Internet regulation since it is published in 1999. According to Lessig, code can be taken as an empowering regulatory tool, but it can be misused according to the circumstances[43]. Currently, in parallel with the technological developments, legal drafts such as Artificial Intelligence Act, Data Governance Act, Data Act, European Health Data Space, etc. are prepared by EU institutions, on different technical subjects to regulate the new technologies.

The studies in this context show that norms on Big Data and artificial intelligence should be set for regular data flow concerning GDPR and related regulations inside the society which guide the governments and users. However, according to Kesa and Kerimkae, GDPR suffers in terms of efficacy in artificial intelligence-based technologies and full compliance of data controllers and processors who use such technologies is unlikely to be achieved in regards to the right to information, the general principle of transparency and

[42] **Lessig, Lawrence** (1999) Code: And Other Laws of Cyberspace, New York, Basic Books.

[43] **Guadamuz**, p.15.

the right to erasure[44]. In AI using technologies, big amounts of data are kept about the habits and lifestyles of individuals which sometimes causes a breach of privacy. In social media channels, users determine their content and share millions of data[45]. While in 2016 the data generated for an average person was 600 megabytes, in 2020 it became around 1.5 Gigabytes. In the application of AI technologies, it can be difficult to fulfil transparency, because of the complexity of processing millions of data which creates risks for some of the fundamental rights and provisions of GDPR[46].

As it is mentioned by the European Group on "Ethics of Security and Surveillance Technologies", in our daily life, the actual and potential impact of ICT technologies and the usage of artificial intelligence is rapidly growing. This situation shows us that a balance must be kept between socio-economic stakeholders who are promoting innovation and privacy and cyber security regulations[47].

As a part of the European Strategy, a High Level of Expert Group (AIHLEG) working on Artificial Intelligence has been established by European Commission in 2018. The committee has prepared two tasks on artificial intelligence "AI Ethics Guidelines and Policy and Investment Recommendations" and "Trustworthy AI" which offer ethical guidance for AI practitioners.

In 2019 European Commission reported "Ethics Guidelines For Trustworthy AI" to support AI solutions for humanity and the environment which indicate the matters of responsibility, transparency, and data protection as the main parts of trustworthy AI[48].

---

44 **Kesa, Aleksandr/Kerikmae, Tanel** (2020) "Artificial Intelligence and the GDPR Inevitablenemeses?", Taltech Journal of European Studies, V:10, Issue 3, pp.70.

45 **Kent, Bülent** (2020) "Alman Hukukunda Sosyal Ağların Düzenlenmesi ve Alman Sosyal Ağ Kanunu", Bilişim Hukuku Dergisi, C:2, S:1, s.5.

46 **Kesa/ Kerikmae**, p.75.

47 **Lipton, Jacqueline** (2015) ReThinking Cyber Law A New Vision for Internet Law, UK, Edward Elgar, p.3.

48 The European Commission Ethic Guidelines for Trustworthy AI [2018]

Ethical standards for AI are discussed at the European level by the European Parliament, as a proposal for a Regulation on ethical principles not only to build trust at all levels of involved stakeholders and society, but also to support the development, deployment and use of artificial intelligence, robotics and related technologies in EU in a manner that is compliant with ethical principles[49]. The proposal consists of a coordination role at the Union level, as well as supports the European Commission. According to the proposal, a "Supervisory Authority" is formed in every EU Member State to cooperate and coordinate the legislation process and to monitor the application of the "Regulation" by binding guidelines. The proposal aims to prepare an annex which establishes an exhaustive and cumulative list of high-risk sectors and high-risk uses and purposes[50].

European Commission published the "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts on 21 April 2021. This proposal can be considered the first attempt of the Union, as a regulatory work, in the field of artificial intelligence[51]. When the regulation comes into force, it will closely affect companies, enterprises, customers and governments. Likewise, the General Data Protection Regulation (EU) 2016/679, Artificial Intelligence Act which will be entered into force in 2025, is expected to be a pioneer in setting global standards[52].

B. FORTHCOMING REGULATIONS IN EU LEGISLATION

Since 2010, many national policies and strategies are prepared for artificial intelligence and related technologies concerning human rights,

[49] <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html#title1>

[50] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html#title1>

[51] European Commission COM (2021) 206 final, 2021/0106 (COD) Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Act [2021]

[52] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>

democracy and the rule of law. In 2015, European Commission has made legal arrangements for the Internet of Things (IoT)[53] which is defined as a global, invisible, networking environment built through smart sensors, cameras, software, and databases, in a world-spanning information fabric which was put into action for the digitalization of society and an environment where objects and individuals are interconnected via communication networks for the benefit of citizens[54]. IoT is considered as a data processing activity according to article 2 of GDPR[55]. However, there are still uncertainties[56].

In 2016, the Commission published a staff working document called "Advancing the IoT in Europe" on the digitalization of society and businesses to create a single market for IoT. The proposal for Data Act is published on 23rd February 2022. Among the other rules, the Act consists of rules on improved access and portability for IoT devices for sharing with a third party of the user's choice. IoT systems also process personal data which may be automatically shared from machine to machine with no transparency to the user[57]. For that reason, the legal needs of IoT, AI and related technologies are getting higher and higher each day.

Consequently, Data Governance Act was published as a draft in 2020, and at the same period, European Commission published a "White Paper of Artificial Intelligence" for ethical, and legal concerns about AI that need to be regulated[58]. European Commission brought a proposal "Artificial Intelligence Act" on the 21st of April 2021 which is the first attempt to regulate artificial

---

53 **Daş, Resul/Gündüz, M. Zekeriya** (2018) "Nesnelerin İnterneti: Gelişimi, Bileşenleri ve Uygulama Alanları", Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, C:24, S:2, s.334; **Gülşen, İzzet** (2019) Nesnelerin İnterneti: Vaatleri ve Faydaları, Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi (ASEAD), C:6, S:8, s.108.

54 **Edwards** (2019c), p.133;148.

55 Opinion 8/2014 on the on Recent Developments on the Internet of Things, p.4.

56 **Wachter, Sandra** (2018) The GDPR and the Internet of Things: A Three-Step Transparency Model, Law, Innovation and Technology, V:10, N:2.

57 **Hildebrandt, Mireille/Koops, Bert-Jaap** (2010) "The Challanges of Ambient Law and Legal Protection in the Profiling Era", Modern Law Review, V:73, No:3, p.428.

58 Commission European (2020) On artificial intelligence - a european approach to excellence and trust Tech rep, European Commission.

intelligence systems in Europe. The act aims to create a legal basis for processing developing and testing innovative AI systems for the public, including health issues, such as disease prevention, control and treatment.

As health data is considered sensitive data in GDPR, the processing of health data is subject to strict rules. Especially after the pandemic period, new drafts on health data have been prepared. Regarding the processing of health data, European Health Data Space (EHDS) is another upcoming Act that the proposal has come in February 2022. The draft creates a common space in the area of health and allows improved access to own electronic health data and sharing it with other health professionals[59]. EHDS promotes the exchange of patients' data safely and in a secure way, even they travel abroad, and citizens have control over their health data. The Act supports not only digital health services, but also clarifies the security of artificial intelligence in health issues. The regulation upholds data protection rules. EHDS encourages the use of health data in research and policy-making. Currently, Medical Devices Regulation creates guidelines on Cybersecurity for medical devices which consists of rules for the processing of health data.

Forthcoming regulations on AI and related topics in EU legislation may generate new challenges for the existing ethical and legal framework of GDPR[60]. Especially in the ICT technologies which collect huge amounts of personal data, the balance between the use of data and the principles of fundamental rights should be kept in balance. It is important to ensure the compliance of these drafts with each other. With these new regulations which are proposed for a trusted and cyber-secure Europe, EU aims to achieve a high common level of cybersecurity all across EU in collaboration with the society.

[59] <https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-82020-european-health-data-space_en> s.e.t.15.06.2022

[60] **Bozkurt Yüksel, A. Ebru** (2022) "Avrupa Komisyonu'nun Yapay Zekâ Tüzük Teklifi'ne Genel Bir Bakiş". Türkiye Adalet Akademisi Dergisi, S:51, s.19-46.

CONCLUSION

In parallel with the technological developments, especially starting from the 1950s and accelerating after 2000, the legal rules have been renewed and changed according to the new implementations. The widespread use of smartphones has facilitated easy access to information, and as a result, the problem of data security has emerged. Directive 95/46, which started being implemented in the EU in 1995, was abolished with the entry into force of GDPR in 2018, and a new era has been entered into the EU legislation with the General Data Protection Regulation.

Today, artificial intelligence and its associated technology are growing at an incredible speed. In the face of these developments, the existing legal regulations are not sufficient. For this reason, the EU has prepared and discussed several drafts which will be put into effect in the next 5 years.

With the entry into force of the new regulations that are still in draft forms, such as the Artificial Intelligence Act, Data Governance Act, Data Act, and European Health Data Space, many rules regarding the processing and sharing of data can be changed. Of course, this situation may cause some new challenges in GDPR in the next years which is not clear yet. The fact that the new regulations are compatible with each other and follow the GDPR provisions, can eliminate this uncertainty in the coming years. Out of the EU, there are many countries which have different legal systems with different regulations. Consequently, a global data and privacy program can be a solution to ensure uniformity in the globalizing world.

ACKNOWLEDGEMENT

This paper is based on research that is executed within the scope of the project "PandeVITA – Pandemic Virus Trace Application for the Effective Knowledge Transfer Between Science and Society Inside the Quadruple Helix Collaboration" The project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 101006316.

BIBLIOGRAPHY

Arat, Tugay/Aslan, M. Mert (2021) "Sosyal Medyada Veri Güvenliği ve Kişisel Mahremiyet Sorunu" Akdeniz Üniversitesi İletişim Fakültesi Dergisi, S:35, s.387-401.

Ashley, Kevin (2011) The Case-Based Reasoning Approach Ontologies For Analogical Legal Argument. In: Sartor G, Casanovas P, Biasiotti M, Fernández-Barrera M (eds) Approaches to legal: ontologies law governance and technology series. Springer, Dordrecht.

Ashley, Kevin (1991) Reasoning With Cases And Hypotheticals In Hypo Int J Man Mach Stud pp.753–796.

Bozkurt Yüksel, A. Ebru (2022) "Avrupa Komisyonu'nun Yapay Zekâ Tüzük Teklifi'ne Genel Bir Bakiş". Türkiye Adalet Akademisi Dergisi, S:51, s.19-46.

Buchholtz, Gabriella (2020) "Artificial Intelligence and Legal Tech: Challenges to the Rule of Law", Regulating Artificial Intelligence (Eds. Thomas Wischmeyer/ Timo Rademacher) Switzerland, Springer, pp.175-198.

Buocz, T. Julius (2018) "Artificial Intelligence in Court Legitimacy Problems of AI Assistance in the Judiciary", Retskraft – Copenhagen Journal of Legal Studies, V:2, N:1.

Çekin, M. Serdar (2021) Yapay Zeka Teknolojilerinin Hukuki İşlem Teorisine Etkileri, 1.Baskı, İstanbul, On İki Levha Yayıncılık.

Daş, Resul/Gündüz, M. Zekeriya (2018) "Nesnelerin İnterneti: Gelişimi, Bileşenleri ve Uygulama Alanları", Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, C:24, S:2, s.327-335.

Do Carmo, Tania/Rea, Stephen/Conaway, Evan/Emery, John/Raval, Noopur (2021) "The Law in Computation: What Machine Learning, Artificial Intelligence, and Big Data Mean for Law and Society Scholarship", Law and Policy, V:43, Issue 2, pp.170-199.

Edwards, Lilian (2019a) "Privacy and Data Protection1: What is Privacy? Human Right, National Law, Global Problem" Law, Policy and the Internet (Ed. Edwards, Lilian), Hart, UK, pp.52-75.

Edwards, Lilian (2019b) "Data Protection: Enter the General Data Protection", Law, Policy and the Internet (Ed. Edwards, Lilian), Hart, UK, pp.77- 117.

Edwards, Lilian (2019c) "Data Protection and e Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling", Law, Policy and the Internet (Ed. Edwards, Lilian), Hart, UK, pp.119- 164.

Edwards, Lilian/Veale, Michael (2017) "Slave to the Algorithm? Why a "Right to an Explanation" Is Probably not The Remedy You Are Looking For", 16 Duke Law&Technology Review 18, pp.24-27.

Erdoğan, Gökhan (2021) "Yapay Zekâ Ve Hukukuna Genel Bir Bakiş", Adalet Dergisi, S:66 s.117-192.

Francesconi, Enrico (2022) "The Winter, The Summer And The Summer Dream Of Artificial Intelligence In Law.", *Artif Intell Law*, 30, pp.147–161 < https://doi.org/10.1007/s10506-022-09309-8>.

Fuster, G. González (2014) The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer, Brussels.

Gao, Jianxi/Li, Daqing/Havlin, Shlomo (2014), "From a Single Network to a Network of Networks", National Science Review, V:1, Issue 3, pp.346-356.

Greenleaf, Graham (2012) "Korea's New Act: Asia's Toughest Data Privacy Law", 117 Privacy Laws &Business International Report, pp.1-6.

Guadamuz, Andres (2019) "Internet Regulation", Law, Policy and the Internet (Ed. Lilian Edwards), Hart, UK, pp.3-20.

Gülşen, İzzet (2019) Nesnelerin İnterneti: Vaatleri ve Faydaları, Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi (ASEAD), V:6, N:8, pp.108.

Güneş Peschke, Seldağ/ Peschke, Lutz (2013) "Protection Of The Mediatized Privacy In The Social Media: Aspects Of The Legal Situation In Turkey And Germany", Gazi Üniversitesi Hukuk Fakültesi Dergisi" C:17, S:2, s.857-884.

Güneş Peschke, Seldağ (2014) The Protection of Personality Rights From Roman Law Till Today, Ankara, Yetkin.

Güneş Peschke, Seldağ/Sayan, Ömer Fatih (2021) "A Comparative Study of Privacy Policies and Data Protection During the COVID-19 Pandemic Within Different Countries", CORONALOGY: Multidisciplinary Academic Analysis in Perspective of Covid-19 (Eds Sefer DARICI, Ayşe Meriç YAZICI), De Greuter – Sciendo.

Hildebrandt, Mireille/Koops, Bert-Jaap (2010) "The Challanges of Ambient Law and Legal Protection in the Profiling Era", Modern Law Review, V:73, No:3, p.428-460.

Kent, Bülent (2020) "Alman Hukukunda Sosyal Ağların Düzenlenmesi ve Alman Sosyal Ağ Kanunu", Bilişim Hukuku Dergisi, C:2, S:1, s.1-46.

Kesa, Aleksandr/Kerikmae, Tanel (2020) "Artificial Intelligence and the GDPR Inevitablenemeses?", Taltech Journal of European Studies, V:10, Issue 3, pp.67-90.

Lessig, Lawrence (1999) Code: And Other Laws of Cyberspace, New York, Basic Books.

Lipton, Jacqueline (2015) ReThinking Cyber Law A New Vision for Internet Law, UK, Edward Elgar.

Loevinger Lee (1949) "Jurimetrics: The Next Step Forward", Minnesota Law Review (1796), V:44, N:4, p.455.

Lucchi, Nicola (2016) The Impact of Science and Technology on the Rights of the Individuals, Law, Governance and Technology Series 26, Springer, p. 4.

Mayer-Schönberger, Viktor/Cukier, Kenneth (2013) Big Data: A Revolution that will Transform How We Live, Work, and Think, London, John Murray.

McCarty, L. Thorne (1984) Intelligent Legal Information Systems: Problems And Prospects In: Campbell C (Ed), Data processing and the Law Sweet and Maxwell, London, pp.125–151.

McCarty, L. Thorne (1990) "Artifcial Intelligence And Law: How To Get There From Here", Ratio Juris, V:3, Issue 2, pp.189–200.

McLachlan, Scott/Kyrimi, Evangelia/Dube, Kudakwashe/Fenton, Norman/Schafer, Burkhard (2022) "The Self-Driving Car: Crossroads at the Bleeding Edge of Artificial Intelligence and Law", Cornell University, Workingpaper, <https://8303d3e493133b9b937b9684793ab2f814c189c3.vetisonline.com/abs/2202.02734>.

O'Doherty, Michael (2020) Internet Law, Bloomsbury Professional, Croydon.

Palmirani, Monica/Martoni, Michele/Rossi, Arianna/Bartolini, Cesare/Robaldo, Livio (2018) PrOnto: Privacy Ontology for Legal Reasoning.ğ In: Kő, A., Francesconi, E. (eds) Electronic Government and the Information Systems Perspective. EGOVIS 2018. Lecture Notes in Computer Science, V:11032. Springer, Cham.

Peschke, Lutz/Güneş Peschke, Seldağ/Gümüş Ağca, Yasemin/Seyfafjehi, Seyedehshahezad/Dündar, Irmak/Aydoğdu, Yasin (2022) "Reward Mechanisms In COVID-19 Tracking Apps And Its Impact On The Voluntary Participation Of The Public In Sustainable Innovation Processes", Türkiye İletişim Araştırmaları Dergisi, S:39, s.54-72.

Purtova, Nadezhda (2018) "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law", Law, Innovation and Technology, V:10, Issue 1, pp.40-81.

Rissland Edwina/ Ashley Kevin (1987) "A Case-Based System For Trade Secrets Law", In: Proceedings Of The First International Conference On Artificial Intelligence And Law, pp.60-66 ACM Press.

Savelka, Jaromir/Westermann, Hannes/ Benyekhlef, Karim/ Alexander, S. Charlotte/ Grant, Jayla/Amariles, David/Hamdani, Rajaa/Meeùs, Sebastien/Troussel, Aurore/ Araszkiewicz, Michal/Ashley, Kevin/Ashley, Alexandra/Branting, Karl/Falduti, Mattia/Grabmair, Matthias/Harašta, Jakub/Novotná, Tereza/Tippett, Elizabeth/Johnson, Shiwanni (2021) "Lex Rosetta: Transfer Of Predictive Models Across Languages, Jurisdictions, And Legal Domains" In: ACM (Ed.) Proceedings Of The Eighteenth International Conference On Artifcial Intelligence And Law, pp.129–138.

Serpanos, Dimitrios/Wolf, Marilyn (2018) Internet of Things – IoT Systems Architectures, Algorithms, Methodologies, Springer International Publishing.

Simitis, Spiross/Hornung, Gerrit/Döchmann, Indra Spieker genannt (2019) Datenschutzrecht, Baden Baden **Nomos Kommentar, Nomos Storm, Marijn/ van der Wolk, Alex**. In: RAIL: The Journal of Robotics, Artificial Intelligence & Law, V:4, Issue 6 (November-December 2021), pp.451-458.

Singil, Nesrin (2022) "Yapay Zekâ ve İnsan Hakları", Public and Private International Law Bulletin , C:42, S:1, s.121-158.

Sönmez Çakır, Fatma/Aytekin, Alper/Tüminçin, Alper Fatma (2018) Nesnelerin İnterneti ve Giyilebilir Teknolojiler, Sosyal Araştırmalar ve Davranış Bilimleri Dergisi, C:4, S:5, s.84-95.

Specht, Louisa/Mantz, Reto (2019) Handbuch Europisches und deutsches Dateschutzrecht, Beck, Munich.

Sümer, S. Yağmur (2021) "Ceza Yargılamasının Geleceği: Robot Hakim" Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C:23, S:2, s.1543-1591.

Ulenaers, Jasper (2020) "The Impact of Articial Intellgence on the Right to a Fair Trial: Towards a Robot Judge?", Asian Journal of Law and Economics, V:11 No:2, pp.1.

Valery, Stepenko/Lyudmila, Dreval/Sergei, Chernov/Viktor, Shestak (2022) "EU Personal Data Protection Standards and Regulatory Framework", Journal of Applied Security Research, Vol.17 Issue 2, p.190-207.

Wachter, Sandra (2018) **"**The GDPR and the Internet of Things: A Three-Step Transparency Model", Law, Innovation and Technology, V:10, N:2.

Walters, Robert/Novak, Marco (2021) Cyber Security, Artificial Intelligence, Data Protection & the Law, Springer, Singapore.

Walton, Douglas (2006) Fundamentals Of Critical Argumentation, Cambridge Cambridge University Press.

Zeytin, Zafer/Gençay, Eray (2019) "Hukuk ve Yapay Zekâ: E-kişi, Mali Sorumluluk ve Bir Hukuk Uygulaması", Türk Alman Üniversitesi Hukuk Fakültesi Dergisi, C:1, S:1, s.39-70.