

LEGAL AND COMPLIANCE RISKS OF NEW TECHNOLOGIES

Yeni Teknolojilerin Getirdiği Hukuki Riskler ve Uyum Riskleri

Yasemin GÜLLÜOĞLU*

Fatih ERDEMİR**

Abstract

Technology is developing parabolically. This development affects businesses' way of conduct. Both internal and external processes of enterprises are digitalized in order to increase efficiency and flexibility. Yet, digitalization creates a variety of vulnerabilities and new legal and compliance risks. Some of these risks may arise directly from the technological tools used, for example, from software. Some risks arise due to the features of these technological tools. For example, being vulnerable to cyber-attacks, and hosting artificial intelligence. Some technological risks, on the other hand, may be caused by the characteristics of technological tools as well as the lack of awareness of the employees using these tools. This study aims to


* Doçent Doktor, Ankara Sosyal Bilimler Üniversitesi, yasemin.gulluoglu@asbu.edu.tr, ORCID: 0000-0003-3134-6015.

** Avukat, Ankara Sosyal Bilimler Üniversitesi Bilişim ve Teknoloji Hukuku Yüksek Lisans Öğrencisi, av.erdemirfatih@gmail.com, ORCID: 0000-0001-7188-3339.

Makale Gönderim Tarihi/Received: 29.01.2024.

Makale Kabul Tarihi/Accepted: 29.03.2024.

Atf/Citation: Güllüoğlu, Yasemin ve Fatih Erdemir. "Legal And Compliance Risks of New Technologies." *ASBÜ Hukuk Fakültesi Dergisi* 6, no. 1 (2024): 679-705.

"Bu eser, Creative Commons Attribution-NonCommercial 4.0 International License ile lisanslanmıştır. / This work is licensed under Creative Commons Attribution-NonCommercial 4.0 International License." 

address some of the legal and compliance risks that arise with technological developments and to suggest precautions that can be taken against these risks. In this context, first of all, the digitalization of enterprises will be briefly mentioned, then examples of the risks arising with digitalization will be given, and finally, some general recommendations will be made based on the measures that can be taken against these risks.

Keywords: Digitalization, Legal and Compliance Risks, Cybersecurity, Compliance Education, GRC Systems, Internet Domain Names, Copyright, Personal Data, GDPR, Data Protection.

Öz

Teknoloji katlanarak gelişiyor. Bu gelişme işletmelerin davranış biçimlerini de etkilemektedir. Verimliliğin ve esnekliğin artırılması amacıyla işletmelerin hem iç hem de dış süreçleri dijitalleştirilmektedir. Ancak dijitalleşme çeşitli güvenlik açıklarının yanı sıra yeni yasal ve uyumluluk riskleri de yaratıyor. Bu risklerin bir kısmı doğrudan kullanılan teknolojik araçlardan, örneğin bir yazılımdan kaynaklanabilmektedir. Bu teknolojik araçların özelliklerinden dolayı bazı riskler ortaya çıkmaktadır. Örneğin siber saldırılara karşı savunmasız olmak ve yapay zekayı barındırmak. Bazı teknolojik riskler ise teknolojik araçların özelliklerinden ve bu araçları kullanan çalışanların bilinçsizliğinden kaynaklanabilmektedir. Bu çalışmanın amacı teknolojik gelişmelerle birlikte ortaya çıkan bazı hukuki risklere ve uyum risklerine değinmek ve bu risklere karşı alınabilecek önlemleri önermektir. Bu bağlamda öncelikle işletmelerin dijitalleşmesine kısaca değinilecek, ardından dijitalleşmeyle birlikte ortaya çıkan risklere örnekler verilecek ve son olarak bu risklere karşı alınabilecek önlemlere dayalı olarak bazı genel önerilerde bulunulacaktır.

Anahtar Kelimeler: Dijitalleşme, Hukuki Riskler, Uyum Riskleri, Siber Güvenlik, Uyum Eğitimi, GRC Sistemleri, İnternet Alan Adı, Telif Hakkı, Kişisel Veri, GDPR, Veri Koruması.

INTRODUCTION

Enterprises should conduct their businesses according to laws and regulations. There are various and a wide range of rules that enterprises should consider depending on their scope of activity. On the other hand, it is not reasonable to expect all the employees of a company to have adequate knowledge of the related rules and regulations. To enable the employees to be aware of and abide by the laws and regulations, companies issue compliance programs. Compliance programs do not only contain laws and regulations. They also determine internal policies and procedures.

Technology has been expanding all fields of business rapidly and this proliferation affects the way companies operate. Therefore, compliance programs also must correspond to the requirements caused by technological developments.

This study aims to discuss the main compliance risks brought by new technologies and give some suggestions to deal with those risks. Firstly, the change in the conduct of businesses that is led by technological development is mentioned. Secondly, the legal and compliance risks arising from these developments are discussed. Lastly, possible solutions to confront those risks are suggested.

I. DIGITALIZATION OF BUSINESSES

Recent technological developments led to the digitalization of businesses. Not only the means that businesses use to interact with each other and customers¹ but also its internal operations have been affected by this digitalization.² Digitalization aims to increase the flexibility, and agility of business processes through

¹ William F. Crittenden, Isabella K. Biel, and William A. Lovely, "Embracing Digitalization: Student Learning and New Technologies," *Journal of Marketing Education* 41, no. 1 (2018): 5.

² Saul J. Berman, "Digital Transformation: Opportunities to Create New Business Models," *Strategy & Leadership* 40, no. 2 (2012): 16-24.

technological transformations.³ For example, companies have websites, social media accounts, and mobile applications to interact with their customers. Companies use computer software to conduct their supply-chain operations, carry out inventory management, and keep employee's personal files as well.

Some comprehensive programs are provided to manage the widespread digitalization of business operations. For instance, the IT programs provided to automate customer-facing processes are called Customer Relations Management.⁴ The different techniques used to improve and supervise the processes of organizations are called Business Process Management. The software used to manage the day-to-day activities of a company such as accounting, procurement, and supply-chain operations is called Enterprise Resource Planning.⁵

II. RISK OF NEW TECHNOLOGIES

A. Data Protection Risks

As mentioned above, numerous software is used in businesses in the digital age. Since these software process and store excess amounts of data, managing the data properly is one of the most significant issues for businesses. For instance, it may be decided to use new software for the day-to-day work of a company. In this case, it is very critical to which personnel of the company can use the software in question, and what data is collected and processed through this software. It should be ensured that the software is not used in a way that violates data protection laws.

³ Florian Imgrund et. al., "Approaching Digitalization with Business Process Management." Multikonferenz Wirtschaftsinformatik (Lüneburg, 2018), https://www.researchgate.net/publication/323665985_Approaching_Digitalization_with_Business_Process_Management/link/5dc2fd7992851c81803321cf/download?tp=eyJlb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19.

⁴ Reiny Iriana and Francis Buttle, "Strategic, Operational, and Analytical Customer Relationship Management," *Journal of Relationship Marketing* 5, no. 4 (2006): 23.

⁵"Definition of Enterprise Resource Planning (ERP)." Oracle, n.d. Accessed December 22, 2022, <https://www.oracle.com/erp/what-is-erp/>.

Moreover, the software is mostly used with internet connections therefore open to external threats. For instance, DDOS (Distributed Denial of Service) attacks, which target a single system with multiple attack devices and are therefore difficult to prevent, are one of the serious threats.⁶ It is beyond doubt that, when choosing software for an operation, it should be noted that the security level is high. Choosing an unprotected software can lead to the leakage of both customers' and company's data that needs to be protected. Through cyber-attacks, sensitive data can be accessed, deleted, or changed. Companies should make sure that the software they use is strong against possible cyber-attacks.

Cyber-attacks are carried out in various ways. One of them is spam, which doesn't sound like a serious problem. Spam e-mails are e-mails that are sent without the user's request⁷ and are intended to serve advertisements, fraudulent or pornographic content.⁸ Sending these e-mails is against the law itself and is a violation of the recipient's right not to be disturbed.⁹

However, the damage caused by spam e-mail is not limited to this. Some of the spam e-mails sent carry misleading titles, the mail domain name and IP address are hidden, and the recipient of the mail creates the idea that the mail came from another person or institution.¹⁰ Such misleading emails often direct users to phishing sites. Phishing statement is formed by the combination of password and fishing statements. Phishing sites are encountered by opening spam e-mails that seem to be sent from known shopping sites or banks' websites. The phishing sites that are opened are arranged in a very similar way to these banks or shopping sites. On this site, it is generally requested to share the user's credit card information or other confidential information such as password, by showing an

⁶ Bülent Kent, *Türkiye'de İnternet Sitelerine Erişimin Engellenmesi* (Ankara: Adalet Yayınevi, 2019), 66-67.

⁷ Gazanfer Erbaşlar and Şükrü Dokur, *Elektronik Ticaret* (İstanbul: Nobel Akademik Yayıncılık, 2012), 229.

⁸ Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku* (Ankara: Seçkin, 2012), 114.

⁹ Habip Oğuz, *İnternet Ortamında Kişilik Haklarının İhlali ve Korunması* (Ankara: Adalet, 2012),104.

¹⁰ Oğuz, *İnternet Ortamında Kişilik Haklarının İhlali ve Korunması*, 104.

account update or other reasons.¹¹ A company employee can be directed to a phishing site that appears to be related to a software or website that he/she uses at work via spam sent to his corporate e-mail account. In this way, the username and password used by the employee in company operations may fall into the hands of malicious people. Here, the risk is limited to the data entered by the employee on the phishing site and other data that can be accessed by using this data.

However, the risks related to phishing sites are not limited to these. It has been determined that 93 percent of e-mails that direct users to phishing sites are ransomware.¹² Users who receive spam e-mails allow software to be downloaded to their electronic devices without being aware of it, when they open this e-mail or while being directed to the phishing site in the e-mail or during their activities within this site. These software, called ransomware, use an encryption method to lock the relevant electronic device or certain files on this device, and prevent access to the device or documents until the requested ransom is paid.¹³ Ransomware can target various electronic devices containing information systems. IoT devices, called the Internet of Things¹⁴, can also be subject to ransomware attacks.¹⁵ Therefore, computers, phones and various information systems can be targets of ransomware. The cyber-attack on Colonial Pipeline, one of the largest oil pipelines

¹¹ "What is Phishing," Phishing.org, accessed December 12, 2022, <https://www.phishing.org/what-is-phishing>.

¹² Maria Korolov, "93% of Phishing Emails Are Now Ransomware," CSO, Last Modified June 1, 2016, <https://www.csoonline.com/article/3077434/93-of-phishing-emails-are-now-ransomware.html>.

¹³ Kim Zetter, "What Is Ransomware? A Guide to the Global Cyberattack's Scary Method," *Wired*, Last Modified May 14, 2017, <https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/>.

¹⁴ IoT devices provide information flow with less time and effort, and automation systems can be established with these devices. Devices that gain the ability to manage and organize with IoT infrastructure have become a vital part of human life in homes, large industries and corporate sectors as smart devices. (Mamoona Humayun et. al., "Internet of Things and Ransomware: Evolution, Mitigation and Prevention," *Egyptian Informatics Journal* 22 (2021): 106, <https://www.sciencedirect.com/science/article/pii/S1110866520301304>).

¹⁵ Ben Dickson, "The IoT Ransomware Threat Is More Serious Than You Think," *TechTalks*, Last Modified August 22, 2016, <https://bdtechtalks.com/2016/08/22/the-iot-ransomware-threat-is-more-serious-than-you-think/>.

in the USA that prevented the line from operating for six days, and the cyber-attack that caused the country's stock market to be cut periodically for several days in New Zealand in 2020, show the extent of the damage that can be caused by using ransomware.¹⁶ Ransomware attacks can both cause violations of data protection laws and cause companies to violate their legal obligations arising from contracts or laws by disrupting or stopping their operations. As a result, companies suffer financial loss and loss of reputation.

Artificial intelligence uses statistical learning techniques to find certain patterns in large data sets and make some predictions based on these patterns.¹⁷ Mentioned large data sets include personal and non-personal data. If the data used contains personal data, liabilities may arise under personal data protection laws. The legal risks and consequences of personal data breaches are explained in the previous title. Company data may be defined as confidential information in some laws or bilateral agreements. In both data sets, the law may provide for civil and criminal sanctions; Contracts between the parties may provide for legal sanctions.¹⁸

In all the examples mentioned above, leakage of personal data or confidential information may occur. Such situations have some legal consequences. Since the Personal Data Protection Law in force in Türkiye was prepared based on the European Union regulations, the legal interpretation in this section will be made based on GDPR and the Turkish Personal Data Protection Law (KVKK).

Personal Data is defined in Article 4 of GDPR "*Personal data are any information which are related to an identified or identifiable natural person*". Data processing is generally prohibited. However, in some exceptional cases, data processing

¹⁶ Fatih Erdemir and İrem Erdemir, "Fidye Yazılımların Türk Ceza Hukuku Kapsamında Değerlendirilmesi," in *Fintek ve Hukuk*, eds. U. Aküzüm, C. Ç. Kadioğlu Kumtepe, and Z. Ekinci, (İstanbul: Hukuk Akademisi, 2021), 148-150.

¹⁷ Corrine Cath "Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges," *Phil. Trans. R. Soc. A* 376: 20180080. <http://dx.doi.org/10.1098/rsta.2018.0080>.

¹⁸"The legal implications of Generative AI," *Deloitte*, accessed March 22, 2024. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-ai-institute-generative-ai-legal-issues.pdf>.

activities may be carried out. Personal data can only be processed in cases of legal obligations, vital interests of the data subject, public interest and legitimate interest and with the explicit consent of the data owner, as stated in Article 6 of the GDPR and Article 4 of the KVKK.

The data processor must take adequate precautions and prevent personal data from being accessed and processed except for the reasons explained above. As explained in section 2, data leakage may not have occurred with the consent of the data processor. Various cyber-attacks and malware can cause data leakage. In this case, it will be investigated whether appropriate technical and administrative measures have been taken by the data processor. If the data processor has not taken sufficient and necessary precautions, whether or not he consented to data leakage will not be legally protected.

Data processors must take appropriate technical and operational measures. According to the GDPR Article 32 and KVKK Article 12. According to GDPR, the data processor must ensure “ (i) the pseudonymisation and encryption of personal data, (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.” Also, the Turkish Personal Data Protection Authority has published a guideline regarding this. In this guideline, how technical and administrative measures can be taken are explained as examples.¹⁹

In accordance with Article 82 of the GDPR, people who suffer damage due to personal data leakage have the right to demand compensation for the damage. Again, in accordance with the same article, the data processor can be relieved of this liability if he proves that he has no fault. To prove that there is no fault, it will be checked not only whether the data processor consents to the data leak, but also

¹⁹ Bkz “Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler),” KVKK, accessed December 22, 2023, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf.

whether it has taken the administrative and technical measures described above as necessary and sufficient.

In conclusion, the use of software in violation of data protection law is a fact that every data processor may face. On the other hand, to cope with the legal consequences of this risk data processors must take adequate precautions prescribed by law in force. For example, let's take an example where data that is under the responsibility of the data processor is leaked because of malicious software or a cyber-attack. In this example, let's assume that the data processor was not aware of this leak and did not consent to it. Let's assume that the data controller in the example is an electronic money institution established within the borders of the Republic of Türkiye. In the analysis to be made here; first, it will be investigated whether the necessary precautions have been taken in accordance with the personal data protection law. Then, it should be checked whether leakage tests have been carried out in accordance with Article 12 paragraph 3 of the Communique on Information Systems of Payment And Electronic Money Institutions And Data Sharing Services Of Payment Service Providers In The Field Of Payment Services. In both cases, if it is concluded that there is no fault or deficiency on the part of the data processor, it should be checked whether the notification periods of data leakage are complied with. Articles 32 and 33 of GDPR regulate the notification of data breaches to the data owner and supervisory authority. Likewise, Turkish personal data protection law article 12 paragraph 5 also regulates this issue. Here, it is investigated whether the necessary notifications have been made within the stipulated periods, that is, within 72 hours after the data leak. If no violation is found on the part of the data processor in this regard, only then can the data processor be relieved of liability. In this example, the situation of the subject causing the data leak should also be evaluated. In a Turkish Supreme Court decision, it was stated that the main purpose of protecting personal data is to ensure the security of privacy.²⁰ It has been stated that a prison sentence will be given for this in accordance with Article 135 of the Turkish Penal Code. At the same time, it has been stated that for entering an information system and continuing to stay there, a prison sentence or a fine will be imposed within the

²⁰ Yar. HGK, E. 2014/56, K. 2015/1679, 17.6.2015, (Lexpera).

scope of Article 243 of the Turkish Penal Code. As can be seen, the legislators both stated that data processors should take some precautions and also stipulated some penalties for the individuals in the legislation in order to deter such actions.

B. Trademark And Trade Name Infringement Risks in Domain Names

The widespread use of technology in business life not only creates new legal problems but also allows us to encounter previously encountered legal problems in different ways. Trademark and trade name violations carried out through websites are one of them. Active use of the internet environment by companies to create recognition, brand value and reach customers; This has led to the spread of trademark and trade name violations through websites. Here, we would like to mention the violations made using internet domain names. Internet domain name is the address used to access a website. Domain names, which were initially used to provide easy access to a website, have over time become an identity that enables a company to be recognized commercially.²¹ Domain names are identified with the person who owns the site, and those who want to have information about the relevant person visit these domain names directly or through internet browsers. While it is not possible to protect a trade name or brand all over the world with a single action, the owned domain name can be used globally. For this reason, domain names have a high commercial value.²² Although the commercial value of domain names is high, domain names with extensions such as com, net and org can be obtained by paying very small prices, and it is not checked whether any intellectual property rights are violated during the creation of these domain names. In the acquisition of the domain name, action is taken without checking whether the rights of third parties are violated, only whether this domain name is already used or not. Domain names that are determined to be unused are allocated to the person requesting the name according to the first come, first served principle. In this way, malicious people who easily acquire domain names offer to

²¹ Mehmet Hanifi Bayram, *Avrupa Birliği ve İnternet Hukuku* (Ankara: Seçkin Yayıncılık, 2011), 41.

²² Ayça Zorluoğlu, "Alan Adlarında Kötü Niyet Kavramı," *Hacettepe Hukuk Fakültesi Dergisi* 2, no. 1 (2012): 82.

sell their domain names to the real owners of these names at exorbitant prices, promote their own products by using the well-known reputation of famous brands, or damage the reputation of these companies by sharing obscene content in domain names containing well-known company names.²³

When it comes to damaging the reputation of companies through internet domain names and violating their rights arising from trademarks and trade names, legal regulations and lawsuits that protect these rights may come to mind. However, filing a lawsuit in a country court for a globally accessible domain name will not be a practical solution. An important institution that should be mentioned in this context is The Internet Corporation for Assigned Names and Numbers ICANN. ICANN is an institution with a private-public partnership structure that performs the task of IP address space allocation in the international platform.²⁴ ICANN published a policy called UDRP ("Uniform Domain Name Dispute Resolution Policy") in 1999, in case of violation of the personal rights of others by using the trademark, business name, trade name or name of others with the registration of domain names, and the desire to sell the registered domain names to the name owners for high amounts, and stipulated arbitration rules for the solution of these problems. The arbitration procedure to be applied for these rules has been regulated in the document named RUDRP ("Rules for Uniform Domain Name Dispute Resolution Policy"). The UDRP is in addition to the contract for people who want to buy a domain name from ICANN. In other words, people who buy domain names²⁵ from ICANN's accredited organizations agree to comply with the provisions of the UDRP in advance.²⁶ For a dispute to be settled through arbitration, the consent of the parties must be obtained.²⁷ In this way, the consent

²³ Ezgi Öztürk, "İnternet Yoluyla Markanın Haksız Kullanımı," *Terazi Hukuk Dergisi*, no.45 (2010): 70.

²⁴ "ICANN Archives," *ICANN Archives*, accessed December 22, 2022, <https://archive.icann.org/tr/turkish.html>.

²⁵ "Information for Registrars," *ICANN*, accessed December 22, 2022, <https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en>.

²⁶ "Uniform Domain Name Dispute Resolution Policy," *ICANN*, accessed December 22, 2022, <https://www.icann.org/resources/pages/policy-2012-02-25-en>.

²⁷ Yasemin Güllüoğlu Altun and Elif Bilen, "Tahkim Sözleşmesi," *Hukuk ve Adalet Eleştirel Hukuk Dergisi* 13, no. 29 (2021): 178.

of the domain name holders regarding the arbitration procedure is obtained in advance.²⁸ RUDRP is implemented by multiple arbitration organizations approved by ICANN²⁹ and one of them is WIPO (World Intellectual Property Organization).³⁰ Instead of filing a lawsuit, the victims may initiate the relevant arbitration procedure by applying directly to the WIPO.³¹

C. Copyright Risks

Another technological risk source that may cause legal and compliance problems is artificial intelligence (AI). AI refers to a computer or computer-controlled robot that can complete a task involving a certain degree of intelligence.³² It is a technology that enables a system to learn from experience and adapt over time. That's why the use of AI provides great convenience for companies and makes their operations cost-efficient.³³ Artificial intelligence is broadly used by businesses in different sectors. However, the way AI technology works carries some risks for companies. Components of AI can be listed as data science, machine learning and deep learning and thanks to these components computer programs with AI make decisions in a human-like way³⁴ The decisions are based on a system similar to black boxes. It is almost impossible to understand why and how it is

²⁸ İrem Erdemir, "Kişilik Hakkının İnternet Ortamında İhlali" (Master diss., Hacettepe University, 2019), 71.

²⁹"List of Approved Dispute Resolution Service Providers," *ICANN*, accessed December 22, 2022, <https://www.icann.org/resources/pages/providers-6d-2012-02-25-en>.

³⁰"Domain Name Dispute Resolution," *WIPO*, accessed December 22, 2022, <https://www.wipo.int/amc/en/domains/>.

³¹"Uniform Domain-Name Dispute-Resolution Policy," *ICANN*, accessed December 22, 2022, <https://www.icann.org/resources/pages/help/dndr/udrp-en>.

³² Chethan Kumar, "Artificial Intelligence: Definition, Types, Examples, Technologies," *Medium*, Last Modified August 31, 2018, <https://chethankumargn.medium.com/artificial-intelligence-definition-types-examples-technologies-962ea75c7b9b>.

³³ Rajendra Akerkar, *Artificial Intelligence for Business* (Norway: Springer, 2019), 3.

³⁴ Wolfgang Amann, *Artificial Intelligence and its Impact on Business* (Information Age Publishing, 2020), 80.

made.³⁵ That may cause risks for organizations such as biased data, unsuitable modeling techniques and incorrect decision-making.³⁶ The risks are higher for organizations in regulated industries such as financial services.³⁷ On the other hand Artificial intelligence uses statistical learning techniques to find certain patterns in large data sets and make some predictions based on these patterns.³⁸ With this feature, artificial intelligence is likely to create some products that are subject to copyright.

The powers granted to the owner of intellectual rights are stated in the third section of the Law on Intellectual and Artistic Works No. 5846. Accordingly, the rights of the author are divided into two: material and moral rights. Moral rights are the right to present to the public, the right to determine the name, and the right to prohibit changes to the work. Their material rights are listed as the right to process, the right to reproduce, the right to disseminate, the right to represent, and the right to transmit to the public by means of signal, sound and/or image transmission. When the owner of the work learns about the violation of these rights, within the scope of Article 66 et seq. of the Law on Intellectual and Artistic Works No. 5846, it may file lawsuits to redress the violations or to seek compensation from those who caused the tender within the scope of these violations.

In web 1.0 phase, that is, when the internet first emerged, users were just consumers of content. When it came to the Web 2.0 stage, users started to produce

³⁵ Thomas Davenport and Rajeev Ronanki, "Artificial Intelligence for the Real World," *Harvard Business Review*, January-February 2018, 113.

³⁶ Nancy Albinson, et. al., "Future of Risk in the Digital Era: Transformative Change. Disruptive Risk," *Deloitte*, accessed December 22, 2023, 6 <https://www2.deloitte.com/us/en/pages/advisory/articles/risk-in-the-digital-era.html>.

³⁷ Davenport and Ronanki, "Artificial Intelligence for the Real World," 113.

³⁸ Corienne Cath "2018 Governing Artificial."

content.³⁹ According to the Berne Convention⁴⁰, the copyright of a work containing creative content begins to be valid from the moment it is created.⁴¹

In case of copyright infringement in some jurisdictions, the person whose rights are violated; may request the cessation of the violation, compensation for the damages suffered as a result of the violation, or the return of the infringing materials.⁴² Under Turkish law, the copyright owner's legal rights against infringement are set out in Articles 66 to 70 of the Law on Intellectual and Artistic Works No. 5846. In accordance with these provisions, the copyright owner may request the elimination of the situation causing the violation (including the destruction or transfer of unauthorized copies), the prevention of a possible violation, and compensation for the damage suffered due to the violation. In addition, the rightful owner may request interim measures before or after filing a lawsuit in accordance with the Turkish Code of Civil Procedure. Article 77 of the Law on Intellectual and Artistic Works, which is another important regulation, stipulates that the provisions of Article 57 of the Customs Law No. 4458 will be applied during the import or export of copies that require sanctions in case of possible infringement of rights. This article has been prepared to ensure

³⁹ Dimov Daniel, "Legal issues of new and emerging Technologies." *infosecinstitute.com* accessed March 23, 2024 <https://www.infosecinstitute.com/resources/management-compliance-auditing/legal-issues-of-new-and-emerging-technologies/>

⁴⁰ Türkiye first acceded to the 1948 amended text of the Convention on January 1, 1952, and then became a party to the latest version of the Berne Convention with Law No. 4117 dated 07.07.1995 on the "Approval of the Ratification of our Accession to the Paris Text Amending the Berne Convention for the Protection of Literary and Artistic Works and Amended in 1979" (OG: 12/07/1995 dated and numbered 22341) ("Edebiyat ve Sanat Eserlerinin Korunmasına İlişkin Bern Sözleşmesi," *T.C. Kültür ve Turizm Bakanlığı* accessed March 23, 2024. <https://telifhaklari.ktb.gov.tr/TR-332363/edebiyat-ve-sanat-eserlerinin-korunmasına-iliskin-bern-sozlesmesi.html>).

⁴¹ Bkz. "Berne Convention for the Protection of Literary and Artistic Works" *Wipo.int*, accessed December 22, 2023, <https://www.wipo.int/wipolex/en/text/283698>.

⁴² Daniel, "Legal issues."

compliance with the provisions of the TRIPS Agreement⁴³ regarding confiscation at customs (Articles 51 to 60).⁴⁴

As mentioned above, there are several civil remedies against copyright infringements. Since the trials take a long time, it is recommended to reach an agreement with the person who caused the violation.⁴⁵ However, it may be possible to say that making these demands from the court will result in full compensation and satisfaction of the tendered party. Before the technological age, it might have been possible for these demands to be a means of satisfaction. However, we believe that the above-mentioned decisions to be made by the court will no longer satisfy the person who has been violated, as information can spread very quickly, it is impossible to determine who has reached the information that has been disseminated, and the return of the disseminated materials does not have a meaningful result.

Here, within the scope of the subject of our article, legal risks can be listed as follows; illegal use of content, illegal dissemination of content, and recording/reproduction of illegally published content by others.⁴⁶

Due to the nature of the internet, information thus the violation can spread very quickly. Therefore, in cases where the infringement takes place on the Internet, above mentioned civil remedies are not sufficient and satisfactory for the person whose copyright has been violated. For this reason, it can be said that because of the developing technologies regulations and legal systems cannot provide adequate legal protection in terms of copyright protection. Considering that legal remedies are not sufficient, copyright holders should take measures in parallel with technological developments in order to protect their rights. On the other hand, legislators should ensure that the laws currently in force are updated in the light of technological developments.

⁴³ World Trade Organisation, *World Trade Organisation on Trade-Related Aspects of Intellectual Property Rights*, (Switzerland, WTO, 1995), https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.

⁴⁴ Fırat Öztan, *Fikir ve Sanat Eserleri Hukuku* (Ankara:Turhan Kitabevi, 2008), 695.

⁴⁵ Daniel, "Legal issues."

⁴⁶ Daniel, "Legal issues."

III. Suggestions to Cope with the Risks

A. Training Programs Should Be Created Within the Scope of Compliance With The Legislation

It is vital that a good compliance program is in place and that employees are adequately and periodically trained. In fact, in some sector-specific legal regulations, personnel training is also regulated and made mandatory for companies operating in the sector. To give an example from some of the Turkish laws and regulations in force, it is stated that within the scope of Article 4, paragraph 6 of Communiqué on Information Systems of Payment And Electronic Money Institutions And Data Sharing Services Of Payment Service Providers, awareness should be raised about the duties and responsibilities assigned to the personnel working in information systems management. Achieving this awareness is only possible through training to be given at regular intervals and exams to measure the impact of these trainings. In yet another example; Article 19 of the regulation on banks' information systems and electronic banking services, titled "Increasing information security awareness", stipulates the creation and implementation of training programs to increase information security awareness.

Within the scope of compliance with the legislation, training programs must be included in the compliance program. A well-prepared compliance program is indispensable for companies to comply with legal obligations. However, a good compliance program alone is not enough. With the development of new technologies, governments issue new regulations to reduce the legal problems created by these technologies. These regulations should be followed, and necessary changes should be made in the compliance program. On the other hand, even if there are no legislative changes, new technologies used by the company may also require changing the compliance program or adding new sections to the program. In this respect, the program should be reviewed periodically.

Having a good compliance program for the company and constantly reviewing and updating this program is not enough to eliminate all risks. Laws are abstract. Although compliance programs contain procedural details, they cannot contain casuistic rules that include all possibilities and situations. At this point, the human impact on the subject is important. Companies should provide compliance training to their employees. This training should not only be about

processes and legal regulations. The ethical dimension of education is at least as important as the legal regulations and the operational processes of the company. Because company employees are alone with their own conscience in every matter that is not specifically regulated in the compliance program. For this reason, compliance training to be given to company employees should include high ethical principles, and these principles should be adopted by all layers of the company, especially by managers. However, in this way, employees can report the situation to their supervisors because of their conscience about an issue that has not yet been regulated in the compliance program, and possible legal risks can be eliminated in this way.

It has been mentioned above that cyber-attacks are one of the major risks for companies. The measures that can be taken against cyber-attacks are both social and technical. First of all, company employees should be made aware of possible attack methods, especially employees should be warned about spam e-mails and phishing sites. Spam e-mails sent by the companies' own IT teams in order to attract the attention of the employees to the subject and to detect possible vulnerabilities can be given as an example of such warnings. In addition, there are some technical precautions to be taken against cyber-attacks especially virus-containing applications. The first of these is backing up important data. By backing up critical data on a separate device and offline, this data will be accessible even in the event of a ransomware attack. Using anti-malware programs is another technical measure. However, the protection of these software is not endless. For this reason, protection programs should be checked frequently, and system gaps should be closed with appropriate patches. These programs should be used with the automatic updating feature active. In addition to all these, when it is noticed that a system used by the company is infected by malicious software, the whole

system should be shut down to prevent further spread of the virus, and thus the process should be overcome with the least possible damage.⁴⁷

In summary, compliance should become a company policy and ethics through qualified and periodic training to be given to employees.

B. Alternative Dispute Resolution Methods

Before the Internet existed, there was no legal dispute regarding the domain name. As legal disputes regarding domain names increased, new dispute resolution methods were created. In violations of domain names, alternative dispute resolution methods should be tried instead of traditional litigation methods, as they are faster and more effective.

ICANN is an institution with a private-public partnership structure that performs the task of IP address space allocation in the international platform.⁴⁸ ICANN published a policy called UDRP ("Uniform Domain Name Dispute Resolution Policy") in 1999, in case of violation of the personal rights of others by using the trademark, business name, trade name or name of others with the registration of domain names, and the desire to sell the registered domain names to the name owners for high amounts, and stipulated arbitration rules for the solution of these problems. The arbitration procedure to be applied for these rules has been regulated in the document named RUDRP ("Rules for Uniform Domain Name Dispute Resolution Policy"). The UDRP is in addition to the contract for people who want to buy a domain name from ICANN. In other words, people who

⁴⁷ Kim Zetter, "4 Ways to Protect Against the Very Real Threat of Ransomware," *Wired*, Last Modified May 13, 2016, <https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/>, "Ransomware Attacks," American Bankers Association, accessed December 22, 2022, https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/ransomware-tips?__cf_chl_jschl_tk__=8906558d85d556715462d48e2f547994675c6c0e-1625131683-0-AU8_rrFAgVV3VQxGEIAmIvGzWbAQgEzLxl4SheaYBX4J3l4xcOMvzXp9LNFH2iIXWn2NQA7_2RkT6f.

⁴⁸ "ICANN Archives," *ICANN Archives*, accessed December 22, 2022, <https://archive.icann.org/tr/turkish.html>.

buy domain names⁴⁹ from ICANN's accredited organizations agree to comply with the provisions of the UDRP in advance.⁵⁰ For a dispute to be settled through arbitration, the consent of the parties must be obtained.⁵¹ In this way, the consent of the domain name holders regarding the arbitration procedure is obtained in advance.⁵² RUDRP is implemented by multiple arbitration organizations approved by ICANN⁵³ and one of them is WIPO (World Intellectual Property Organization).⁵⁴ Instead of filing a lawsuit, the victims may initiate the relevant arbitration procedure by applying directly to the WIPO.⁵⁵

In areas other than domain name disputes, alternative dispute resolution can be based on negotiation and, if appropriate under the relevant law, on alternative dispute resolution with the assistance of neutral and professional third parties, such as mediation. In this way, it is possible to obtain faster and more practical solutions. In addition, some legal systems, such as Turkish Law, may have provisions on mediation as a condition of litigation. This issue should be taken into consideration. This issue should be taken into consideration Otherwise, when it is decided to file a lawsuit, the relevant legal processes may be prolonged.

⁴⁹"Information for Registrars," ICANN, accessed December 22, 2022, <https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en>.

⁵⁰"Uniform Domain Name Dispute Resolution Policy," ICANN, accessed December 22, 2022, <https://www.icann.org/resources/pages/policy-2012-02-25-en>.

⁵¹ Güllüoğlu Altun, and Bilen, "Tahkim Sözleşmesi," 178.

⁵² Erdemir, "*Kişilik Hakkının İnternet Ortamında İhlali*," 71.

⁵³"List of Approved Dispute Resolution Service Providers," ICANN, accessed December 22, 2022, <https://www.icann.org/resources/pages/providers-6d-2012-02-25-en>.

⁵⁴"Domain Name Dispute Resolution," WIPO, accessed December 22, 2022, <https://www.wipo.int/amc/en/domains/>.

⁵⁵"Uniform Domain-Name Dispute-Resolution Policy," ICANN, accessed December 22, 2022, <https://www.icann.org/resources/pages/help/dndr/udrp-en>.

C. Creating an Environment Where Personnel with the Necessary Competencies Work as a Team for the Elimination of Legal and Compliance Risks

To reduce legal and compliance risks, it is very important for companies' legal teams and technical teams to work in cooperation. While determining which technological tools, including software, should be used by companies, only getting support from technical personnel will be insufficient to prevent possible risks. Support from the legal team is also required when deciding on this issue. However, in this case, the legal team should also be informed about how a technological tool that is planned to be used works, what kind of data it uses, if any, and what kind of products it produces. In this way, it can be determined whether the technological tool to be used is usable or under what conditions, legal and compliance risks will be at a minimum level. In addition, when a legal risk arises in the future as a result of the use of these technological tools, the support of the legal team, which understands the operation of these technological tools, even at the most basic level, will be much more qualified.

In this context, having technical personnel in the legal teams of companies or employing lawyers with basic technical knowledge and background will add value to the companies' management of legal and compliance risks.

The risks that may arise as a result of the use of AI technologies have been mentioned above. In order to eliminate these risks, it would be appropriate for the technical team to first determine which technology performs which functions and which of these functions the company needs. The legal team may also be consulted after identifying appropriate AI technologies that respond to the need. Especially in the regulated sectors, the decisions made through algorithms should be transparent, reliable, fair and compatible with ethical values.⁵⁶

Technological tools are not only sources of risk. By using these tools, the company's legal and compliance risk management can be made very strong. For this, first of all, the data produced and used in the operational processes of the company must be digitized. However, each department should not carry out this

⁵⁶ Amann, *Artificial Intelligence and its Impact on Business*, 33; Albinson, et. al., "Future of Risk," 7.

digitalization independently of each other. In this context, the use of Enterprise Resource Planning (ERP) systems offers great convenience to companies. ERP system is a software that organizations use to manage their day-to-day operations. ERP enables the data flow between different business processes and therefore prevents data duplication and provides data integrity.⁵⁷ Following the establishment of an effective ERP system, a GRC system should be established. GRC software can be used while installing this system.

GRC stands for Governance Risk and Compliance, and it refers to the idea that in an organization these three notions should be considered together in a holistic view.⁵⁸ The technologies developed in order to enable organizations to support this holistic view are called GRC Systems. These systems are generally developed and sold by private third-party vendors.⁵⁹ The scope of the GRC Systems differ from each other. Moreover, the laws and regulations that an organization should abide by vary according to the different factors such as sectoral and territorial areas of business. Therefore, the legal and technical teams of an organization should analyze the GRC System of the organization together and identify the fields that are not covered by the systems if there are any.

⁵⁷"Definition of Enterprise Resource Planning (ERP)," *Oracle*, accessed December 22, 2022, <https://www.oracle.com/erp/what-is-erp/>.

⁵⁸ Melih Erdoğan and Ahmet Onay, "Yönetişim-Risk-Uygunluk (YRU) Yaklaşımı ve İç Denetim Fonksiyonu İlişkisi: İç Denetim Sorumluluklarının YRU Yaklaşımına Etkisi Üzerine Yapısal Eşitlik Modeli Araştırması," *TİDE Academia Research* 2 (2019): 149.

⁵⁹ Kenneth A. Bamberger, "Technologies of Compliance: Risk and Regulation in a Digital Age," *Texas Law Review* 88 (2010): 689.

CONCLUSION

The transformative effect of technology manifests itself significantly in business life. Both the relations of the enterprises with their customers and their operational processes are affected by this transformation and are being digitized to a great extent.

This change and transformation bring with it some legal and compliance problems. Some of these problems can be listed as follows; Violation of data protection laws due to the software used, violation of data protection laws in case the software and systems are open to cyber-attacks, leaking of the company's trade secrets, causing legal liability of the company by preventing company operations, harming transparency and accountability due to artificial intelligence, damaging reputation, trademark and trade name infringement risks through domain names and copyright risks.

Specific and Technical practices can be developed to deal with such legal and compliance risks. However, these ways of coping can be grouped under some headings. First of all, it should be noted that although the source of these risks is technology, the main solution point is human. The training of company employees on compliance from the top manager to the lowest level personnel and the ethical-based training of this training will ensure that many risks are eliminated. In addition, it is very important for employees to be aware of the risks of cyber-attacks and to know the steps to be followed in possible attacks. In addition, combating legal and compliance risks that arise as a result of technological developments may require the use of newly developed legal opportunities, sometimes leaving the traditional legal perspective, and thus obtaining practical results. Alternative solutions that allow this should be known. Finally, it would be beneficial for the legal and technical units of the organizations to work together, to benefit from the utilities of technology while coping with the legal and compliance risks caused by technology, but to overcome the possible disadvantages of these utilities a joint study by the legal team and the technical team should be maintained.

Hakem Deęerlendirmesi: ift kr hakem.

Finansal Destek: Yazar bu alıřma iin finansal destek alıp almadıęını belirtmemiřtir.

ıkar atıřması: Yazar, bu alıřmada ıkar atıřması olmadıęını bildirmiřtir.

Etik Kurul Onayı: Yazar, bu alıřma iin etik kurul onayı gerekip gerekmedięini belirtmemiřtir.

Peer Review: Double peer-reviewed.

Financial Support: The author has not declared whether this work has received any financial support.

Conflict of Interest: The author has declared that there is no conflict of interest in this research.

Ethics Committee Approval: The author has not declared whether ethical committee approval is required for this research.

REFERENCES

- Akerkar, Rajendra. *Artificial Intelligence for Business*. Norway: Springer, 2019.
- Albinson, Nancy, Cherian Thomas, Michael Rohrig, and Yang Chu. "Future of Risk in the Digital Era: Transformative Change. Disruptive Risk." *Deloitte*. December 22, 2023. <https://www2.deloitte.com/us/en/pages/advisory/articles/risk-in-the-digital-era.html>.
- Amann, Wolfgang. *Artificial Intelligence and its Impact on Business*. Information Age Publishing, 2020.
- American Bankers Association. "Ransomware Attacks." Accessed December 22, 2022. https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/ransomware-tips?_cf_chl_jschl_tk__=8906558d85d556715462d48e2f547994675c6c0e-1625131683-0-AU8_rrFAgVV3VQxGEIAmIvGzWbAQgEzLxl4SheaYBX4J3l4xcOMvzXp9LNFH2iIXWn2NQA7_2RkT6f.
- Bamberger, Kenneth A. "Technologies of Compliance: Risk and Regulation in a Digital Age." *Texas Law Review* 88 (2010): 669-739.
- Bayram, Mehmet Hanifi. *Avrupa Birliği ve İnternet Hukuku*. Ankara: Seçkin Yayıncılık, 2011.
- Berman, Stuart J. "Digital Transformation: Opportunities to Create New Business Models." *Strategy & Leadership* 40, no. 2 (2012): 16-24.
- Cath Corrine. "Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges." *Phil. Trans. R. Soc. A* 376: 20180080. <http://dx.doi.org/10.1098/rsta.2018.0080>.
- Daniel Dimov. "Legal Issues of New and Emerging Technologies." *infosecinstitute.com* accessed March 23, 2024 <https://www.infosecinstitute.com/resources/management-compliance-auditing/legal-issues-of-new-and-emerging-technologies/>.
- Davenport, Thomas and Rajeev Ronanki. "Artificial Intelligence for the Real World." *Harvard Business Review*, January-February 2018, 108-116.

- Deloitte. "The legal implications of Generative AI." Accessed March 22, 2024. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-ai-institute-generative-ai-legal-issues.pdf>.
- Dickson, Ben. "The IoT Ransomware Threat Is More Serious Than You Think." *TechTalks*. August 22, 2016. <https://bdtechtalks.com/2016/08/22/the-iot-ransomware-threat-is-more-serious-than-you-think/>.
- Dülger, Murat Volkan. *Bilişim Suçları ve İnternet İletişim Hukuku*. Ankara: Seçkin, 2012.
- Erbaşlar, Gazanfer and Şükrü Dokur. *Elektronik Ticaret*. İstanbul: Nobel Akademik Yayıncılık, 2012.
- Erdemir, Fatih, and İrem, Erdemir. "Fidye Yazılımların Türk Ceza Hukuku Kapsamında Değerlendirilmesi." In *Fintek ve Hukuk*, edited by Ural Aküzüm, Cemre Çiçe Kadioğlu Kumtepe and Zeynep Ekinci, 138-180. İstanbul: Hukuk Akademisi, 2021.
- Erdemir, İrem. "Kişilik Hakkının İnternet Ortamında İhlali." Master diss., Hacettepe University, 2019.
- Erdoğan, Melih and Ahmet Onay. "Yönetişim-Risk-Uygunluk (YRU) Yaklaşımı ve İç Denetim Fonksiyonu İlişkisi: İç Denetim Sorumluluklarının YRU Yaklaşımına Etkisi Üzerine Yapısal Eşitlik Modeli Araştırması." *TİDE Academia Research 2* (2019): 149-198.
- Güllüoğlu Altun, Yasemin, and Elif Bilen. "Tahkim Sözleşmesi." *Hukuk ve Adalet Eleştirel Hukuk Dergisi* 13, no. 29 (2021): 173-226.
- Humayun, Mamoona, NZ Jhanjhi, Ahmet Alsayat, Vasaki Ponnusamy. "Internet of Things and Ransomware: Evolution, Mitigation and Prevention." *Egyptian Informatics Journal* 22 (2021): 105-17. <https://www.sciencedirect.com/science/article/pii/S1110866520301304>.
- ICANN Archives. "ICANN Archives." Accessed December 22, 2022. <https://archive.icann.org/tr/turkish.html>.
- ICANN. "Information for Registrars." Accessed December 22, 2022. <https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en>.
- ICANN. "List of Approved Dispute Resolution Service Providers." Accessed December 22, 2022. <https://www.icann.org/resources/pages/providers-6d-2012-02-25-en>.

- ICANN. "Uniform Domain Name Dispute Resolution Policy." Accessed December 22, 2022. <https://www.icann.org/resources/pages/policy-2012-02-25-en>.
- ICANN. "Uniform Domain-Name Dispute-Resolution Policy." Accessed December 22, 2022. <https://www.icann.org/resources/pages/help/dndr/udrp-en>.
- Imgrund, Florian, Marcus Fischer, Axel Winkelmann, and Christian Janiesch. "Approaching Digitalization with Business Process Management." Conference: Multikonferenz Wirtschaftsinformatik. Lüneburg, 2018.
- Iriana, Reiny and Francis Buttle. "Strategic, Operational, and Analytical Customer Relationship Management." *Journal of Relationship Marketing* 5, no. 4(2006): 23-42.
- Kent, Bülent. *Türkiye’de İnternet Sitelerine Erişimin Engellenmesi*. Ankara: Adalet Yayınevi, 2019.
- Korolov, Maria. "93% of Phishing Emails Are Now Ransomware." *CSO*. June 1, 2016. <https://www.csoonline.com/article/3077434/93-of-phishing-emails-are-now-ransomware.html>.
- Kumar, Chethan. "Artificial Intelligence: Definition, Types, Examples, Technologies." *Medium*. August 31, 2018. <https://chethankumargn.medium.com/artificial-intelligence-definition-types-examples-technologies-962ea75c7b9b>.
- Oğuz, Habip. *İnternet Ortamında Kişilik Haklarının İhlali ve Korunması* (Ankara: Adalet, 2012).
- Oracle. "Definition of Enterprise Resource Planning (ERP)." Accessed December 22, 2022. <https://www.oracle.com/erp/what-is-erp/>.
- Öztan Fırat. *Fikir ve Sanat Eserleri Hukuku*. Ankara:Turhan Kitabevi, 2008.
- Öztürk, Ezgi. "İnternet Yoluyla Markanın Haksız Kullanımı." *Terazi Hukuk Dergisi* no:45 (2010): 69-79.
- Phishing.org. "What is Phishing." accessed December 12, 2022. <https://www.phishing.org/what-is-phishing>.
- T.C. Kültür ve Turizm Bakanlığı. "Edebiyat Ve Sanat Eserlerinin Korunmasına İlişkin Bern Sözleşmesi." Accessed March 23, 2024.

<https://telifhaklari.ktb.gov.tr/TR-332363/edebiyat-ve-sanat-eserlerinin-korunmasina-iliskin-bern-sozlesmesi.html>.

William F. Crittenden, Isabella K. Biel, William A. Lovely. "Embracing Digitalization: Student Learning and New Technologies." *Journal of Marketing Education* 41, no. I (2018): 5-14.

WIPO. "Domain Name Dispute Resolution." Accessed December 22, 2022. <https://www.wipo.int/amc/en/domains/>.

Zetter, Kim. "4 Ways to Protect Against the Very Real Threat of Ransomware." *Wired*. May 13, 2016. <https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/>.

Zetter, Kim. "What Is Ransomware? A Guide to the Global Cyberattack's Scary Method." *Wired*. May 14, 2017. <https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/>.

Zorluođlu, Ayça "Alan Adlarında Kötü Niyet Kavramı." *Hacettepe Hukuk Fakültesi Dergisi* 2, no. 1 (2012): 67-84.