Araştırma Makalesi
Research Article

Gönderim / Received: 29/05/2023
Kabul / Accepted: 26/07/2023

Hukuk Fakültesi Dergisi
Ankara Hacı Bayram Veli University
Faculty of Law Review

ISSN: 2651-4141 e-ISSN: 2667-4068
Cilt / Volume XXVII Temmuz / July 2023 Sayı / No. 3

YAPAY ZEKÂ SİSTEMLERİNİN SİBER SUÇLARLA MÜCADELEDEKİ ROLÜ: ULUSLARARASI HUKUK İNCELEMESİ

THE ROLE OF ARTIFICIAL INTELLIGENCE SYSTEMS IN THE FIGHT AGAINST CYBERCRIMES: A REVIEW OF INTERNATIONAL LAW

Erhan CAN*

ÖZET

10.34246/ahbvuhfd.1306712

Günümüzün teknolojik imkânları ve yaşanan gelişmeler, ülkelerin siber uzay alanında etkin ve kapsamlı çalışmalar yapmalarını gerekli kılmıştır. Yaşanan gelişmelerde öncelikli adımların atılmasında iki unsurun önemli olduğu söylenebilir: Yapay zekâ ve siber güvenlik. Siber riskleri ortadan kaldırma ve savunma kapsamı, çok boyutlu ve disiplinlerarası çalışmaların bir bütün halinde değerlendirilmesini gerektirmektedir. Ancak hem teknik hem güvenli/etik yapay zekâ sistemleri, hukuki prosedürlerin eşgüdümlü takibine dayanan gelişmelerle sağlanabilir. Bu araştırma genelinde incelendiği üzere yapay zekânın siber güvenlik açısından değerlendirmesi; Avrupa Birliği Siber Güvenlik Kanunu'na bakmanın önemli, uygulamaların sürüm halinde sunulmadan önce "siber güvenlidir" ibaresinin kullanılmasının etkili, denetlemelerin en fazla beş yıllık süreyle yapılmasının başarılı bir etki sunacağı yorumlanmıştır. Bu durumların yanı sıra ChatGPT örneğinde olduğu gibi yapay zekâ uygulamalarının çalışma prensibinde güvenlik algısı, teknik çalışmaların güvenlik boyutunu artırmada etkili bir faktör olabilir. Ancak genel olarak yapay zekâ sistemleri için en önemli konulardan biri olan etik faktör, kullanıcıların bilgi gizliliği gibi prensipleri için incelemelerde bulunmayı, bunu da hukuki prosedürlere uygunlukla yapmayı gerektirmektedir. Örneğin yine bazı uygulamaların ülkelerde yasaklanması,

* **Dr. Öğr. Üyesi,** Ankara Bilim Üniversitesi Hukuk Fakültesi/ANKARA, **e-posta:** erhan.can@ankarabilim.edu.tr, **ORCID:** 000-0002-2434-0187, **DOI:** 10.34246/ahbvuhfd.1306712

* İntihal / ***Plagiarism***: Bu makale intihal programında taranmış ve en az iki hakem incelemesinden geçmiştir. / *This article has been scanned via a plagiarism software and reviewed by at least two referees.*

etik ve güvenlik açıklığı sorunlarından kaynaklandığı bilinmektedir. Önemli faktörün öncelikle hukuki çerçevede olduğu söylenebilir. Siber savunma mekanizmasının oluşturulması ve siber suçlarla mücadeleye ilişkin özel yasanın geliştirilmesi, yapay zekâ çalışmalarına etkin fırsat sunabilir, siber riskleri azaltılmasında etkin bir ortam yaratabilir. Bunun yanı sıra hukuki düzenlemeler incelendiğinde, ulusal düzeyde TCK m. 245/A yasak cihaz ya da programların kullanılmasına yönelik bilişim suçları için geliştirilen bir maddedir. Bu maddenin yapay zekâ uygulamalarına ilişkin geliştirilmesi, kullanılması, ulusal düzeyde kanunlarla birlikte mevzuatın iyileştirilmesi, Avrupa Birliği Siber Güvenlik Kanunu gibi uluslararası çalışmalarda örgüt/kurum üzerinde durulması önemli görülmüştür. Bunun yanında siber risk ve saldırıların ortadan kaldırılması, şirketlerin gelişmesine, ülkenin uluslararası stratejik bir konum yakalamasına, yapay zekânın birçok alanda kullanılmasına yönelik etkin sonuçların alınabileceği bir ortam yaratabilir. Bu kapsamda yapay zekâ teknolojilerinin siber suçlarla mücadelede etkili bir unsur olabileceği, sağlık, savunma gibi birçok sektörde etkili bir araç olacağı söylenebilir. Aynı zamanda sosyal medya kullanımında etik sorunların ortadan kaldırılabileceği, siber saldırılara maruz kalmanın ortadan kaldırılabileceği bir etki yaratabilir. Uluslararası hukuk incelemesi yapıldığında, Avrupa Konseyi, NATO, Afrika Birliği gibi örgütlerin yapay zekâ çalışmalarına odaklanması, Türkiye'nin bu konuda hukuki süreçleri geliştirmesini gerektirmektedir.

Anahtar Kelimeler: *Yapay Zekâ, Siber Uzay ve Risk, Güvenlik, Uluslararası Hukuk, ChatGPT.*

ABSTRACT

Current technological opportunities and developments in the world necessitate effective and comprehensive scientific research in cyberspace from countries. Two factors are important in those developments to take priority actions: artificial intelligence and cyber security. The scope of eliminating and defending cyber risks requires the evaluation of multidimensional and interdisciplinary research as a whole. However, both technical and safe/ethical artificial intelligence systems can be provided with developments based on the coordinated follow-up of legal procedures. The evaluation of artificial intelligence in terms of cyber security interpreted as examined throughout this research; taking as a reference the European Union Cyber Security Law is important, the use of the phrase "cyber-safe" before the applications are released is effective, controlling within a maximum period of five years has a successful effect. In addition to these situations, the perception of security in the working principle of artificial intelligence applications, as in the example of ChatGPT, can be an effective factor in increasing the security capacity of technical research. However, the ethical factor, which is one of the most important issues for artificial intelligence systems in general, requires examining the principles of users such as information privacy and doing this in accordance with legal procedures. For example, some applications are banned in countries and caused by ethical and security flaw problems. The important

factor is primarily in the legal framework. The forming of a cyber defense mechanism and the development of a special law on combating cybercrime can provide an effective opportunity for artificial intelligence research and create an effective environment for reducing cyber risks. In addition, when the legal regulations are examined, TCK art. 245/A is an article developed for cybercrimes related to the use of prohibited devices or programs. The importance of organization/institution emphasized in international research such as the development and use of this article regarding artificial intelligence applications, the improvement of legislation associated with laws at the national level, and the European Union Cyber Security Law. Moreover, the elimination of cyber risks and attacks can create an environment where effective results can be obtained for the development of companies, the country's international strategic position, and the use of artificial intelligence in many areas. In this context, artificial intelligence technologies can be an effective element in the fight against cybercrime and will be an efficient tool in many sectors such as health and defense. Furthermore, artificial intelligence can create a result in which ethical problems can be eliminated through the use of social media and exposure to cyber-attacks. When international law is examined, it is necessary for organizations such as the Council of Europe, NATO, African Union to focus on artificial intelligence studies and Turkey to develop legal processes in this regard.

Keywords: *Artificial Intelligence, Cybercrime and Risk, Security, International Law, ChatGPT.*

EXTENDED ABSTRACT

Artificial intelligence algorithms and crime relationships can be examined from different perspectives. For example, artificial intelligence can be used to fight crime. In addition, artificial intelligence can also be a system that causes crime to be committed. In this research, the importance of artificial intelligence in the legal system and approach is mentioned. A relationship was established between artificial intelligence and cyber risk. The effect of artificial intelligence on information technology law gains importance where human control is insufficient. There are many uses of artificial intelligence in eliminating cyber risks. Factors such as social media security and increasing country security are linked to eliminating cyber risks. Especially cyber security can be examined in terms of government, company, and individual use security.

In this research, the importance of artificial intelligence algorithms in the fight against cybercrime is explained. International law research were examined and the use of artificial intelligence in developed countries was evaluated. A few examples of the use of artificial intelligence systems in the fight against cybercrime are given and the research of international organizations are examined. One of these organizations is NATO. The relationship between cyber risk and defense deals with NATO research in terms of cyber wars. The Tallinn Handbook, prepared in 2013 with NATO research, examines the issue of law in cyber wars. Cyberdefense includes the use of force, self-

defense, and the collective security system. Accordingly, the size of the cyber attack and the use of force in a classical war level were preferred. Another example of work in international law took place in the work of the Council of Europe. The Cyber Crime Convention signed in 2001 mentions legal cooperation that is aimed to establish international relations in cybercrime.

Another international study on the relationship between cyber security and risk is the European Union Cyber Security Law. The law consists of 58 articles and 4 main titles. The law, which examines cyber attacks and security vulnerabilities, is in accordance with the ethical mindset. In addition, the control mechanism aims to increase cyber security and reduce risks. The European Cyber Security Agency, which is the most important backbone of the law, aims to carry out research that will increase the cyber security capacity. Moreover, the use of the phrase "cyber-safe" for artificial intelligence algorithms and certificates will have an important place in getting more effective results. Accordingly, the important thing is that member states increase their work in accordance with the law. Turkey also needs to study on this issue and develop it.

The most important application developed by the European Union Cyber Security Law for artificial intelligence algorithms can be seen as certificate processes. The preferred certificate for information communication and technology products is limited to five years. In the legal context, the certificate is important in terms of providing advanced technology and high confidence. Therefore, developments and research in this aspect require the legal system to be used more conveniently in the control of digital applications and products. When the research that can be done for this purpose are examined, necessary thing is to increase the frequency of artificial intelligence controls with regulations. Regulations present that processes as well as the law can be followed more quickly. In addition, international research can be explained by the fact that artificial intelligence is not allowed to be used in cases where it is not ethical and safe. An example of this can be given for ChatGPT. The use of this application is prohibited from some countries, and restrictions are made because it is not ethical and reliable. Therefore, in order to get faster solutions in the legal system, some applications should be used to control ChatGPT and to emphasize the phrase "cyber-safe".

As a result of the research, the relationship between artificial intelligence and cyber security can be considered important in terms of international research. In the Turkish legal system, TCK art. 245/A contains some regulations regarding the use of prohibited devices or programs in controlling applications for information systems. However, research such as increasing these regulations and expanding their use for security should be increased. At the national level, cyber risk has shown that security is also important to many sectors in the country. For example, legalization processes should be accelerated in order to increase the activities of companies such as BAYKAR, ASELSAN, TUSAŞ, ROKETSAN, which stand out in the defense industry,

and to ensure the security of software and hardware services. Ensuring state security, fighting against terrorist organizations, the Ukraine Crisis and the Russia-Georgia War, which show that cyber risks can be a threat during the war, make it important to develop cyber security with artificial intelligence systems. The most important ways to be effective in the international arena are the regulations in the national legal system and increasing the possibilities of using artificial intelligence.

GİRİŞ

Yapay zekâ sistemleri, suçlarla mücadelede kullanılabilecek argüman olup günümüzde önemli yere sahiptir. Hukuk sistemi ve yaklaşımında yapay zekânın kullanımı, bilişim hukuku için siber suçlarla mücadelede gerekli kabul edilebilir. Siber güvenliğin sağlanmasında yapay zekâ teknolojisi, insan gücünün yetersiz kaldığı durumlarda, bilişim sistemleriyle çözümlemeyi işlevsel kılmaktadır. Bunun önemi, özellikle de günümüzün teknoloji çağında siber güvenlik ve yapay zekânın birbirinden ayrı düşünülemeyeceğini göstermiştir. Teknoloji çağının beraberinde bilişim korsanlarının doğmasına neden olması, buna ilişkin sonuç olarak söylenebilir. Ayrıca bilgilerin korunmasına yönelik zorluklar, güvenlik açıklığına ortam hazırlamıştır. Günümüzün en önemli sorunlarından biri olarak bu konu, hukuki açıdan insanların güvenliğini sağlamayı, bilgileri korumayı zorlaştırmıştır. Bu durum ise beraberinde; sosyal medya ortamı, yapay zekâ sistemleri, ülke güvenliğini sağlamak için uluslararası yetkinliğin sağlanması gibi çeşitli durum ve faktörleri incelemeyi gerektirmiştir. Çünkü teknoloji kullanımının yaygınlaşmasıyla birlikte, bunlara ilişkin sorunlar da artmıştır. Dolayısıyla siber güvenlik hem devlet hem şirket hem de kişisel kullanım özelinde önemli bir kriterdir.

Uluslararası boyutta yapay zekâ incelendiğinde, ilerleyen dönemlerde elektronik ölçüde savaş ortamı yaratabileceği söylenebilir. Böylece yapay zekâ yalnızca ulusal güvenlik adına sınırlandırılamayacaktır; dünya genelinde verilen dijital savaşlarda başarılı olmayı gerektirecek bir konu haline dönüşecektir. İlerleyen zamanlarda dijital, internet, elektrik, elektronik savaş veya siber uzayla karşı koymalar, ciddi tehdit haline gelebilecektir. Dünya genelinde yapılacak çalışmalar, koruyucu uygulamalardan oluşmalı ve her ülkeyi-kullanıcısını ilgilendiren küresel uygulamaları içermelidir. İnsanlığın güvenliği adına prosedür, uyulması zorunlu olan kurallarla çevrelenmelidir. Herkesin/her ülkenin kanunlarıyla eşgüdümlü olması gerekliliği gibi konular, yine dünyayı ilgilendiren bir konu olarak siber güvenliği karşımıza çıkarmıştır.

Henüz şimdiden tüm dünyayı kapsayacak siber gelecek uygulamalarının tehdit oluşturmadan uluslararası kurum ve örgütlerle bunu gerçekleştirmesi gerekli görülmektedir.

Bu araştırma kapsamında, yapay zekâ sistemlerinin siber suçlarla mücadeledeki rolü ele alınacaktır. Temelde yapılacak araştırma ise, uluslararası hukuk doğrultusunda incelenecektir. Yapay zekâ sistemlerinin siber suçlarla mücadeledeki kullanımının henüz çok yaygın olmadığı dikkate alındığında, bu sistemlerin hukuki güvenliği sağlamada önemli olduğu açıklanacaktır. Araştırma doğrultusunda bu amaçla uygulanan stratejiler dikkate alınacak olmakla birlikte siber suçlardan korunmada gerekli olan hukuki prosedürün önemine değinilecek, yapay zekânın öne çıkarılması gerekli gösterilecektir. Örneğin; insan kullanımına sunulan yapay zekâ sistemleri bilgi koruma, depolama gibi konularda etik sorun yaratabilir. Eğer mevzuatta, bu tür sistemlere yönelik yaptırım yoksa, henüz kullanım sürecinden önce birtakım tehlikeler görülebilecektir. Dolayısıyla araştırma kapsamında bu doğrultuda yapılacak çalışmalar siber suç oluşturabilecek sistemler için açıklanacaktır. Yapay zekânın koruma mücadelesindeki yeri/önemine bakılarak ChatGPT uygulamasının ya da dünya genelinde kısıtlamalara gidilen uygulamaların nedenleri örnek olarak gösterilecektir. NATO, Avrupa Birliği Siber Güvenlik Kanunu çalışmaları üzerine yapay zekâ teknolojisi ele alınacaktır. Mevzuat gerekliliğinin hem yapay zekâ hem de siber savunma için incelenmesi, geliştirilen uygulamalarda birbirinden vazgeçilemez unsurlar olarak ifade edilebilir. Ayrıca virüs programlarının geliştirilmesi gibi uygulamalar, siber risklere karşı koruyucu etki yapmaktadır. Bu durum da yapay zekânın önemiyle açıklanmaktadır. Siber alanın günümüzde artık kablosuz ağın kullanıldığı her an-ortamda risk oluşturabilecek faktörlerden oluştuğu, uygulamaların bazı denetleme mekanizmalarıyla işlerlik kazanmasının önemli olduğu ifade edilebilir. İnsanların küresel ısınma gibi konularda çalışma ve uygulamalara odaklanması gibi hukuki süreçlerle siber güvenliğin de sağlanması şarttır.

I. YAPAY ZEKÂ

Bilgisayar bilim dallarından olan yapay zekâ, modern çağın bilişim sistemlerinin temel taşlarındandır. Makinelerde gelecek dönemde insansı davranışların görülebileceği, yapay zekâ kullanımlarındaki yaygınlıkla açıklanmaktadır[1]. Bilgisayara düşünme gücünün kazandırılması, geçmiş

[1] Gyanendra Singh/Ajitanshu Mishra/Dheeraj Sagar, "An Overview of Artificial Intelligence", *SBIT Journal of Sciences and Technology*, 2(1), 2020, s. 1.

tecrübelerle makinenin öğrenmesi, karar verme ya da bilişsel süreç gerektiren işlemlerle insan davranışlarını simüle etmesi, yapay zekâ sistemleriyle birlikte sağlanmıştır. Öğrenme ve anlamada insan gibi davranan bu sistemler, günümüzde önemli bir gelişme yakalamıştır. Bunlar özellikle de eğitim, etkileşim, rehberlik gibi hizmetleri sunarak insan hayatını kolaylaştıran ve artık her an-her gün bu sistemlerden yararlanılan uygulamalardır[2]. Yapay zekânın bütün sektör gruplarını etkilediği bilindiği için, uluslararası uzlaşmanın sağlanacağı çalışmaların yapılması da önemlidir. Uluslararası alandaki çalışmaların temeli ise hukuki prosedürlere odaklanan bir araştırma sürecinin önemli olduğunu göstermektedir. Bütün sektör gruplarını etkileyebilecek potansiyel tepkiler belirlenmelidir.

Yapay zekâ, bilişsel yenilikçi bir teknoloji olup insan davranışlarının bilinen sınırlarını genişletmektedir. Düşünme, tahmin etme, öğrenme gibi insan etkileşimlerinde önemli basamak olarak birçok yönüyle insanlara yardımcı olan bir sistem görevini üstlenmektedir. Dolayısıyla günlük yaşamda vazgeçilmez olması, sistemlerin gün geçtikçe daha çok gelişme yakalamasına, uygulama hizmetleriyle birlikte sunumuna ortam hazırlamıştır. Yapay zekânın dar ya da genel anlamda farklı işlem basamaklarını gerçekleştirmesi, yapay zekânın her uygulama içinde yer aldığını, ama bunların birbirinden farklılık gösterdiğini ortaya koymaktadır. Dar anlamda; basit işlemleri yapan yapay zekâ, genel anlamda; insan davranışlarını taklit eden ve geliştirildiğinde ise çok daha kompleks işlemleri yapabilecek güce sahiptir[3]. Yapay zekânın bu özelliği, birçok ülkede güvenlik için değerlendirilmesine de kapı aralamıştır. Yapay zekânın etik boyutu, siber güvenlik için bilgiyi koruma-saklama gibi konulara bağlı incelenmiştir. Bu nedenle uluslararası hukukta yapay zekâ, yaşanan teknolojik ve dijital gelişmelerle birlikte gündemde kalmaktadır[4]. Geliştirilen uygulamalarda yapay zekâ kullanımının vazgeçilmez olması, siber güvenliğin uluslararası bir önem yakaladığını göstermektedir. Tehlikeli durumların yaşanmasını önleyecek yaptırımların aynı şekilde uluslararası çalışmalarda yapay zekâyla eşgüdümlü olması gerektiği söylenebilir.

A. Yapay Zekâ Sistemlerinin Gruplandırılması

[2] Maad M. Mijwil/Emre Sadıkoğlu/Emine Cengiz/Hasibe Candan, "Vergilendirme Sürecinin İdari İşlem Bağlamında İncelenmesi", *Veri Bilimi Dergisi*, 5(2), 2022, s. 98.

[3] Ahmet Efe, "Yapay Zekâ Odaklı Siber Risk ve Güvenlik Yönetimi", *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 5(2), 2021, s. 145.

[4] İbrahim İrdem/Sedat Çobanoğlu, "Yapay Zekânın İç Güvenlik Yönetimi Üzerine Yansımaları: Siber Güvenlik", *Kaytek Dergisi*, 2, 2021, s. 187-188.

Günümüzde farklı problemleri çözümlemek amacıyla geliştirilen yapay zekâ sistemleri, kişiselleştirilmiş kullanım imkânı sunan uygulama deneyimlerine dönüşmüştür[5]. Zaman içinde bu sistemlerdeki gelişmeyle birlikte yapay zekâ, belirli şekillerde gruplandırılmıştır. Bunlar ise dar, genel, güçlü ve zayıf yapay zekâ kavramlarıdır. Dar yapay zekâ, insanların tüm zihinsel durumlarını taklit eden, ancak gerçekte zeki olup olmadığı bilinmeyen sistem olarak tanımlanır. Genel yapay zekâ, farklı uzmanlık alanlarında, karmaşık sorunları çözümleyebilme ve kendisini bağımsız şekilde kontrol edebilen, kendi düşünce, endişe, hisleriyle hem güçlü hem de eğilimi olan yazılım çeşididir. Zayıf yapay zekâ, zeki olduğu varsayılan eylemleri yönetebileceği iddia edilen sistemlerdir. Güçlü yapay zekâ ise, makine eylemlerini gerçek anlamda zeki kabul eden hipotezi savunmaktadır[6]. Yapay zekâ teknolojilerinin, kullanım alanlarına göre geliştirilen birer sistem olduğu da söylenebilir. Yapay zekâ ister şirket özelinde isterse de günlük hayatımızda kullanılan bir sistem olsun, robotik özellikler insan görevlerinin bir kısmını yerine getirebilecek araçlara dönüşmüştür[7]. Yapay zekânın karmaşık sistemleri çözmesi, hızlı işlem yapabilmesi ve kullanıcı bilgilerine ulaşabilmesi gibi durumlar, güvenlik/etik konusunu gündeme getirmiştir. Güvenlik ve etik sorunları, küresel sorun olup siber uzayda dijital alanın tamamını etkileyecek düzeyde sonuç yaratabilecektir. Bu nedenle tehlike, uluslararası mücadeleleri gerektirmektedir. Sınır dışı problemlerin artış gösterebileceği, savaş hukukunda etkilerinin görülebileceği dikkate alınabilir. Uluslararası hukuk çalışmaları, siber suçlara neden olacak bu tür sorunları belirleme ve çözümleme temelli bir yaklaşımda olmalıdır.

1. Yapay Zekâya İlişkin İyi-Kötü Değerlendirmesi

Yapay zekâ sistemleri ve makine öğrenimi, insanların hayatlarını kolaylaştırmanın yanı sıra, güvenlik sistemi için de kullanılabilirlik kazandırmıştır. Bu gelişmeler ise güvenliğin farklı konulara ilişkin sağlanması demektir. Örneğin siber güvenlik sistemi, büyük ölçekli firma ve kuruluşlar için önemlidir. Siber saldırılardan korumak için yapay zekâ araçlarının geliştirilmesi, yasa dışı amaçlarına ulaşmak isteyen saldırıları ortadan kaldıracak sistemleri gerektirmiştir. Bu yönüyle yapay zekâ sistemlerinin

[5] Yeliz Şenkaya/Uğur Güven Adar, "Siber Savunmada Yapay Zekâ Sistemleri Üzerine İnceleme", *Akademik Bilişim*, 2014, s. 2.

[6] Aslıhan Ünal/İzzet Kılınç, "Yapay Zekâ İşletme Yönetimi İlişkisi Üzerine Bir Değerlendirme", *Yönetim Bilişim Sistemleri Dergisi*, 6(1), 2014, s. 62.

[7] Harun Pirim, "Yapay Zekâ", *Journal of Yasar University*, 1(1), 2006, s. 85-88.

önemi ve siber güvenliği sağlamada potansiyel etkisi, hukuki açıdan onu öne çıkarmaktadır[8]. Diğer yandan iç güvenlik yönetiminde ülkeler, teknoloji odaklı yeni yöntemlere ihtiyaç duydukları için yapay zekâyı devlet politikaları düzeyinde inceler[9]. Bu faktörler de yine yapay zekânın kullanım amacını iyi yönde etkilemektedir. Ancak uluslararası çalışmadaki yetersizlik, yapay zekâ kullanımında güvenlik açıklıkları yaratan kötü sonuçların doğmasına neden olmaktadır. Önleyici tedbirin hem ceza hem de idare hukukuyla geliştirilmesi, bunun için çalışmaların uluslararası yetkinlikte olması, sorunları azaltmaya yardımcı olacaktır. Bunun yanında, uluslararası düzeyde bu konudaki çalışmaların yetersizliği, idare hukukuyla birlikte azaltılabilir ya da önlenebilir. İdare hukukunun içtihadı, yapay zekâ gelişmelerinin yakalanmasında ve yaşanan sorunların hızla cevaplanmasında etkin bir girdi olabilecektir. Uluslararası çalışmalardaki yetersizliğin ve sorunların azaltılmasında bu durum önemli bir yere sahiptir.

Siber risk ve sorunlar, makine öğreniminin gelişmesiyle daha çok yaygınlaşan bir konu olmuştur. Burada özellikle de bilgilerin korunması/saklanması sorunu, bilgi çağının önemli bir problemidir. Maddi ve manevi zarar oluşturacak bilgilere erişimler, uygulama veri tabanlarında kullanılan yapay zekâ sistemleriyle yaşanabilmektedir. Bireye özgü olabileceği gibi, kurumlara özgü sorunlar, uluslararası çalışmaları incelemeyi, güvenlik için ulusal kararların alınmasını bir hedef haline getirebilir. Hukuki ve teknolojik önlemler ise, teknik çalışmalar artırılırken yapay zekâ algoritmalarında yaşanabilen sorunları azaltma üzerine etkili bir metottur[10]. Yapay zekâ sisteminin kullanım amacı, yaşanan problemleri de değiştirmektedir. İyi ya da kötü amaçlarla kullanıma bağlı olarak hukuki güvencenin geliştirilmesi önemlidir. Ayrıca Birleşmiş Milletler Genel Kurulu'nda alınan "Bilgi Teknolojilerinin Kötüye Kullanılması ile Mücadele" kararı, 2001 yılından günümüze kadar bu amaç doğrultusunda siber suçlarla mücadeleler için verilen çalışmalarda artışlara zemin hazırlamıştır. Ülkelere destek verilmesi amacıyla 2005 yılında sözleşmelerin yapılacağı ve verim alınacağı düşünülmüştür[11]. O günden günümüze kadar geçen süreçte yapay zekânın

[8] Efe, *Yapay Zekâ İşletme Yönetimi İlişkisi Üzerine Bir Değerlendirme*, s. 144.

[9] İrdem/Çobanoğlu, *Yapay Zekânın İç Güvenlik Yönetimi Üzerine Yansımaları: Siber Güvenlik*, s. 185.

[10] Şenkaya/Adar, *Siber Savunmada Yapay Zekâ Sistemleri Üzerine İnceleme*, s. 1.

[11] Bilgi Teknolojileri ve İletişim Kurumu, *Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri*, 2022, s. 18-19.

özellikle az gelişmiş ya da gelişmekte olan ülkelerde, hukuki prosedürle önemli ölçüde korunabilecek bir sistem düzeyinde olabilme potansiyeli tartışmalıdır. Yapay zekânın kötü amaçlarla kullanımının yaygınlığı ve siber güvenlik için kullanımının az olması bu konulara yönelik sorunlardır. Ayrıca riskin belirlenmesi, sorun yaratabilecek unsurlar için hukuki düzenlemelerin yapılıp kanunlaştırılmasından geçmektedir.

II. SİBER GÜVENLİK

Bilgi-iletişim teknolojilerinin gelişmesi, siber suçların tarihsel süreci olarak kabul edilir. Bilgisayarın kullanılması ve internet ortamında verilerin hızlı akışı, siber risk altına girmemize neden olmuştur. İnternetin kendisinin riskli yer haline gelmesi, teknolojilerin ve uygulamaların birleşimi olan siber güvenliğin dikkate alınmasını gerektirmiştir. İnternet gibi güvenli olmayan ağ sistemiyle dağıtılması ise, siber güvenliğin büyük bir risk taşımasına ve ulusal güvenlik için değerlendirilmesine ortam hazırlamıştır[12]. 1966 yılından sonra siber risk olgusunun büyümesi, bilgisayar ve internet kullanımının herkese açık kullanıma başlanmasıyla birlikte yaşanmıştır. Hukuki düzenleme, siber risk problemlerine bağlı ortaya çıkmıştır. Türkiye'de ilk kez 1991 yılında 765 sayılı Türk Ceza Kanunu'na, "bilgileri otomatik işleme tabi tutan sistem," ifadesinin eklenmesiyle bilişim suçları gündeme gelmiştir. Bu suçlar 5237 sayılı TCK'da ise, "Bilişim Alanında İşlenen Suçlar" kapsamında 10. Bölüm başlığı olarak TCK'da dört madde halinde verilmiştir. 2000 senesinden sonra bilişim suçlarında artışların dünya genelinde yaygınlaşması, önemli maddi kayıplara ortam hazırlamıştır. Mellisa, love Bug gibi virüsler, bu kayba neden olanlar arasında öne çıkar. Uluslararası düzeyde mücadeleler, sadece devletlerin kendi hukuki sistemlerine tabi tuttukları uygulama olmamış, ayrıca siber suçlar küresel niteliğe dönüşmüştür[13]. Siber suçları yargılama esnasında ise asıl sorun, ulusal mevzuatlara ilişkin yetersizlik olarak görülebilir. Dünya genelinde ülkelerde hukuki düzenleme hemen her yerde mevcut olmadığı için küresel düzeyde siber suçlar, uluslararası hukukta sorun oluşturmuştur. Ayrıca sosyal medya kullanımında yaşanan artışlar, siber suçların daha çok artmasına da zemin hazırlamıştır. Kişi bilgisi ve paylaşımı, internette sosyal medya kullanımıyla birlikte artmış, siber dünyada endişe oluşturan sorunları beraberinde getirmiştir. Genel olarak siber dünyada

[12] Shivani Ghundare/Akshada Patil/Rashmi Lad, "Importance of Cyber Security", *International Journal of Engineering Research & Technology*, 8(5), 2020, s. 1-2.

[13] Abdullah Aldoori, *Uluslararası Hukukta Siber Suçla Mücadele*, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, 2020, s. 5-10.

etik sorunu ve sosyal medya uygulamaları, siber riskin önemli bir konusu haline gelmiştir[14]. Dolayısıyla siber güvenlik, bilgisayar ortamında yaşanan gelişmelerle paralel ölçüde hukuki prosedürlerin geliştirilmesine ilişkin incelenebilir. Siber güvenlik açısından ilk kriterin yasayla oluşturulması gerektiği belirtilmekle birlikte ikinci asıl önemli kriterin bu süreci sağlayacak yapay zekâ sistemleriyle olabileceği vurgulanabilir. Hukuki düzenlemelerde bu konular, siber güvenliğin belkemiğini oluşturacak bir faktör olarak önemli yer tutmaktadır.

A. Siber Risk ve Güvenlik Algısı

Siber güvenlik, ağ teknolojilerinde yaşanan gelişmeyle birlikte tehditlere karşı savunma mekanizmasını amaçlamaktadır. Hukuki-kurumsal altyapı bağlamında siber güvenlik, siber alanın korunması gereken beşinci alan olarak belirlenmiş, devlet ve uluslararası örgütlere ciddi sorumluluklar yüklemiştir. Sosyal, psikolojik ve ekonomik etkenler, siber saldırıların oluşturduğu maddi-manevi hasarları önlemeyi amaçlamıştır. Siber güvenlik bağlamında hukuki çalışma ve kaynaklara artan önem Türkiye kapsamında değerlendirildiğinde, Uluslararası Telekomünikasyon Birliği'nin 2018 yılı verileri önemlidir. Buna göre Türkiye, Avrupa ülkeleri arasında 18., dünya genelinde ise 175 ülke arasında 20. sıradadır. Siber güvenlik stratejilerine yönelik hukuki düzenlemeler, Elektronik Haberleşme Kanunu gibi parça parça düzenlemelerle işlenmiştir. Bu bağlamda ulusal düzeyde hukuksal düzenlemelerin henüz yakın tarihlerde geliştiği ve bu durumun uluslararası hukuk için de geçerli olduğu söylenebilir. Ancak temelde siber uzay, güvenlik ve dijital ortam, şirketlere yönelik incelenebilmektedir. Bu nedenle siber güvenlik kapsamında doğrudan bir kanuna ihtiyaç vardır. Bunun ise günümüzde insansız hava araçları gibi ulusal güvenlik için çalışma yapan TUSAŞ, ASELSAN, ROKETSAN, BAYKAR gibi şirketler için de önemli olduğu belirtilebilir[15]. Siber güvenlik için çalışmaların artması ve denetlenmesi konuları; yasal prosedürleri geliştirmekten geçmektedir. Ayrıca kanunlaştırma durumunun önemi vurgulanabilir. Siber güvenlik için kanunlaştırma, savunma sanayisi ile sınırlı kalmayan, enerji, haberleşme, tarım, sağlık gibi bütün sektörleri kapsayan bilgi-iletişim teknolojilerinin kullanılma zorunluluğunun olduğu her alan için önemlidir.

[14] Gönül Cengiz, "Siber Suçlar, Sosyal Medya ve Siber Etik", *İletişim Çalışmaları Dergisi*, 7(3), 2021, s. 407.

[15] Alpay Karasoy/Pelin Babaoğlu,"Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı", *Yasama Dergisi*, 44, 2021, s. 149-151.

Siber uzay, dijital alt yapı, internet, bilgisayar sistemi, yazılım, donanım ve hizmetleri kapsayan dijital alandan oluşmaktadır. Dijital ortamın güvenliği, siber güvenliğin sağlanması anlamına gelir. Bu, tek bir kullanıcının dijital ortamda güvenliği ile başlayıp şirket çalışmalarına kadar devam etmektedir[16]. Dolayısıyla büyük tehdit ve risklerin oluşmasına ortam hazırlayan faktörlerin tespiti hem şirketler hem kurumlar hem de işletmeler için güvenliği sağlamada etkili faktördür. Burada kamu ve özel sektörün bütün olarak görülmesi, önlemlerin alınması ve siber risk etkilerinin azaltılması gerekmektedir. Savunma hattı oluşturulurken tüzel kişilere düşen sorumluluklar, kullanıcıların ve kendi şirketlerinin bilgilerini korumada denetim sistemlerini artırmalarını gerektiğini gösterir[17]. İç denetim, siber güvenliği artırıcı uygulama için çalışmalar yaptığı takdirde sorunlar azaltılabilir[18]. Siber güvenlik, risklerin azaltılmasını sağlayan bir yetkinlikte olmalıdır. Denetim zorunluluğunun hukuki prosedürle desteklenmesi, bu konu için önemlidir. Diğer ifadeyle denetim zorunluluğu ve uygulamaları incelendiği takdirde, hukuki geçerlilik de sağlanabilecektir. Ayrıca devletin siber güvenlik algılarında yaşanan gecikmeler, siber risklerin artmasına neden olmaktadır. Bu konuda örnek ise devletlerin savaş sürecindeki siber alandaki çarpışmalarıyla bağlantılı verilebilir. Devletlerin birbirleriyle savaşları, stratejik açıdan siber alandaki savaşları meydana getirmiştir. Örneğin Rusya-Gürcistan Savaşı sırasında devletlerin saldırıları, aynı zamanda bir siber saldırı örneğiydi. Bir görüşe göre, Gürcistan'ın Asya'dan Avrupa'ya uzanan ulaşım hatlarının merkezi haline gelmesi, Rusya'yı kaygılandıran bir durum haline gelmiştir. Rusya bu amaçla siber saldırılar da dâhil mücadeleye adım atmış, bu mücadele için sürdürülebilir çalışma yapacağını belirtmiştir. Hibrit ortam içinde siber saldırı ve vekâlet güç uygulamalarını bulunduran gelişmeler, saldırılan savaş hukuku yerine bireylerin merkeze alındığı savaş hukukunun öne çıktığını göstermiştir. Ukrayna Krizi sürecinde de hibrit ortamın yaratıldığı ve savaş sırasında potansiyel güçlerin farklı kullanıldığı söylenebilir[19]. Siber saldırılara ilişkin örnekte görüldüğü gibi, savaşlarda siber risk faktörü de önemli bir konu haline

[16] Seval Selimoğlu/Mehtap Altunel, "Siber Güvenlik Risklerinden Korunmada Köprü ve Katalizör Olarak İç Denetim", *Denetişim*, 19, 2019, s. 5-7.

[17] Onur Yılmaz, "Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik", *Cyberpolitik Journal*, 2(4), 2019, s. 28-31.

[18] Selimoğlu/Altunel, *Siber Güvenlik Risklerinden Korunmada Köprü ve Katalizör Olarak İç Denetim*, s. 6-7.

[19] Gökhan Alptekin, "2008 Rusya-Gürcistan Savaşı ve Savaş Sonrası Büyük ve Bölgesel Güçlerin Tepki ve Politikaları", *RUSAD*, 6, 2021, s. 119.

gelmiştir. Uluslararası önlemlerin savaş hukuku çerçevesinde de ele alınması elzemdir.

Siber güvenlik, çeşitli sektör gruplarını etkilemektedir. Örneğin sağlık sektöründe siber güvenlik, zengin veri kaynaklarıyla öne çıkmıştır. Siber suçlar için çekici hale gelen bu veriler, hastanelerde siber tehdide ortam hazırlamıştır. Örneğin bireylerin sağlık ve kişisel bilgileri, tehlike altında kalmıştır. Tehlikeye giren sağlık bilgilerinin yanı sıra siber suçluların hastanelere yaptıkları fidye saldırıları da önemli bir sorundur. Sağlık sektöründe siber saldırılara ilişkin bir diğer örnek ise, her cihazın uzaktan kontrol edilebilirliğine ve sağlık verilerine ulaşılabilirliğine bağlı yaşanmıştır. Cihazların güvenliğiyle ilgili endişe, verilerin korunmasının yetersizliğiyle birlikte kötü amaçlı kullanıcılar için çekici hale gelmiştir. Bu durum hasta güvenliğini önleyici bir sorun olarak görülebilir. Sağlık bakım hizmetlerinin artırılması için güvenliğin de artırılması önemli konulardan biridir. Böylece siber güvenliğin artırılmasında sektörel bazlı uygulamaların öne çıkarılması gerekmiştir[20]. Güvenlik kavramı açısından siber risklerin azaltılmasına, toplum içinde düzenin aksamadan yürütülmesini sağlayacak, bireylerin korku duymadan kullanmasını denetleyecek uygulama yönüyle incelenebilir. Çünkü güvenlik, küresel bir öneme sahip olup devletleri tehdit eden saldırıların önüne geçmede etkilidir[21]. Ancak söz konusu uygulamalarda devletlerin teknolojik gelişmişlik düzeyleri de önemlidir. Devletlerin bu gelişmişlik düzeyleri ile siber güvenliğin sağlanması arasında önemli ilişki vardır. Örneğin siber uzay teknolojilerine sahip olamayan ülkelerin ciddi güvenlik zafiyetleriyle karşı karşıya oldukları söylenebilir[22]. Dolayısıyla siber güvenlik, ilkin toplumsal koruyucu uygulama ve çalışmaların yapılmasını önemli kılmaktadır. Siber risklerin devlet ve özelde sektörlerle bireyleri tehdit etmesi, yaptırımların hukuki ölçüde hedeflenmesini gerektirmiştir. Siber risklerden korunmak için konu bunlarla sınırlı kalmayıp teknolojik imkânların ve gelişmişliğin de önemli olduğu ifade edilebilir.

[20] Yıldız Tosun/Elif Gezginci/Sonay Göktaş, "Siber Güvenlik: Sağlık Hizmetleri Ne Kadar Güvende?", *JAREN*, 7(3), 2021, s. 157.

[21] Semih Polat, *Milli Güvenlik Açısından Siber Güvenlik*, T.C. Ankara Hacı Bayram Üniversitesi Lisansüstü Eğitim Enstitüsü Amme İdaresi Anabilim Dalı Yüksek Lisans Tezi, 2020, s. 51.

[22] Soner Çelik, "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım", *Academic Review of Humanities and Social Sciences*, 1(2), 2018, s. 111.

III. SİBER SUÇLA MÜCADELEDE YAPAY ZEKÂ: GÜVENLİK YÖNETİMİ

Günümüzde siber güvenlik, verilere saldırı gerçekleştirme operasyonlarından korumada en dikkat çekici metottur. Siber uzayla birlikte elektronik sistemler büyümektedir. Bu ise sanal bir dijital alandır ve günümüzün 'nesnelerin interneti' ortamında birbirine bağlanmış bilgisayar ve akıllı telefonlar için kurulan ara bağlantı görevini üstlenir. Böyle bir alanda siber suçlardan arındırılmış bir ortamın yaratılması sağlanmalıdır. Performans açısından siber güvenliğin çeşitli engellerle karşı karşıya olduğu bilinmektedir. Bu nedenle güvenlik konusu için farklı çalışmalar öne çıkarılır[23]. Yapay zekâ sistemlerinin siber suçlarla mücadele için kullanılmasının temeli, güvenlik algısına dayanır. Ancak burada öncelikle yapay zekânın hukuken düzenlenmesinin bir güvenlik metodu olarak tercih edilmesinin etkili olacağı söylenebilir. Yapay zekânın hukuken ele alınmasında güvenlik meselesi, etik kurallar ya da rehber ilkeler vasıtasıyla mı yoksa ulusal veya uluslararası anlamda klasik hukuk kurallarıyla mı düzenlenebileceği yönündedir. Burada iki aşamalı bir düzenlemenin zorunlu olabileceği söylenebilir. Her iki durum da yapay zekânın hukuk kuralları çerçevesinde incelenmesini gerekli göstermiştir[24]. Ayrıca hukuki sorumluluk açısından bir değerlendirme yapıldığında; yapay öğrenme ve açıklanamazlık, yapay zekâya yön veren karar ya da algoritmalarda maddi varlıkların bulunmaması, söz konusu sistemlerde veri güdümünün olması, siber saldırılara açıklık gibi faktörler hukuki sorumluluğun özel olarak değerlendirilmesini gerektirir. Bu, veri güdümlülüğünü sağlayanların da sorumlu tutulmasından kaynaklanmaktadır[25]. Özelde ise bu konu, küresel boyutta olabilecek siber suçların meydana gelmesi ve güvenliğin uluslararası hukuk çerçevesinde ele alınmasını gerektirmektedir. Çünkü siber suç, sadece ulusal saldırılarla sınırlı kalmamış, uluslararası hukuku kapsayıcı sorunları beraberinde getirmiştir. Yapay zekânın hukuksal düzenlemesinde durum, siber güvenlik için siber silahların da tercih edilebileceği ulusal güvenlik algısına kadar devam eden birçok faktörü içine almaktadır.

[23] Maad M Mijwil/Mohammed Aljanabi/ChatGPT, "Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime", *Iraqi Journal for Computer Science and Mathematics*, 4(1), 2023, s. 65.

[24] Oğuz Gökhan Yılmaz, "Yargı Uygulamasında Yapay Zekâ Kullanımı – Yapay Zekâ Hakim Cübbesini Giyebilecek mi?", *Adalet Dergisi*, 66, 2021, s. 387-388.

[25] Barış Özçelik, "Yapay Zekânın Veri Koruma, Sorumluluk ve Fikri Mülkiyet Açısından Ortaya Çıkardığı Hukuki Gereksinimler", *Adalet Dergisi*, 66, 2021, s. 100.

Yapay zekânın kullanım alanlarından birinin siber suçlarla mücadele olması ise, birkaç örnek çalışma üzerinden incelenebilir. IBM Watson yapay zekâ sistemi, özellikle de siber saldırıları önlemek için geliştirilmiştir. Bu yapay zekâ sistemi, özel versiyon olarak bilgisayar sisteminde kötü niyet ve şüpheli işlemleri önlemede Yahoo'ya, Lloyds İngiliz sigorta şirketine ve internet servis sağlayıcısı olan TalkTalk'a siber riskleri azaltmada yardımcı olmuştur[26]. Siber güvenlikte öngörücü analitiklerin etkili uygulamaları arasında IBM Watson gibi Splunk da siber saldırıları önlemede etkilidir. Siber saldırıların hızlı bir şekilde tanımlanması ve bunlara karşı koyulması, en yeni analiz çözümlemelerinin geliştirilmesinde bu sistemleri öne çıkarmaktadır. Potansiyel avantajın kazanılmasında bu saldırıların en başta önlenmesi, olası tehditleri ilerleyen dönemler için azaltmak anlamına gelmektedir[27]. Siber güvenlikte yapay zekâyla öngörücü analitiklerin oluşturulması ve yatırımların yapılması önemlidir. Devlet ve şirket özeli için bu çalışmaların geliştirilmesinin hukuki çerçevede zorunlu tutulması, daha sistemli uygulamaların yapılmasını ve maddi kaynakların ayrılmasını kolaylaştırabilir. İnterneti korumanın zor bir iş olduğu, siber güvenliğin sadece sistematik gelişmeleri öne çıkarmayla sağlanacağı söylenebilir. Çevrimiçi kullanımlarda bireyin beklentileri; ağda güvenlik ve mahremiyeti, gizliliği koruyan bilgi işlemlerini yapabilmeyi hedefler. Bu nedenle siber saldırıların önlenmesi, tespit edilmesi ve mücadele yönteminin geliştirilmesi, günümüzde birçok konuyla bağlantılıdır. İnsanlığın geleceği açısından bu konular, yalnızca yapay zekâ uygulamalarını geliştiren şirketlerle sınırlı kalmayacak ve belirli devletlerin tekeline bırakılmayacak kadar ciddi hususlardır.

A. Ulusal Güvenlik Algısı ve Yapay Zekâ

Yapay zekânın güvenlik alanındaki kullanımı, teknolojinin yaygınlaşması ve Çin, ABD gibi bazı ülkelerde sağlık, hukuk gibi birçok alanda kendine yer edinmesiyle birlikte önemli bir boyut yakalamıştır. Kullanım için önemli gerekliliğin kanunlaştırmaktan geçtiği bilinmektedir. Bu amaçla devletler, yapay zekâya ilişkin mevzuatlara odaklanmıştır; Çin, ABD ise mevzuatları geliştiren ülkelerin başında yer almaktadır. İlk olarak 2009 yılında ABD'de bu amaçla Ulusal Robotik Girişim çalışmaları başlamış, 2016 yılında ise

[26] Gökhan Erdoğan, "Yapay Zekâ ve Hukukuna Genel Bir Bakış", *Adalet Dergisi*, 66, 2021, s. 128.

[27] Awodiji Temitope/Tosin-Amos Aderonke/Femi Ayoola/John Owoyemi, "Stop Cyber Attacks Before They Happen: Harnessing The Power of Predictive Analytics in Cybersecurity", *Journal of Multidisciplinary Engineering Science and Technology*, 10(4), 2023, s. 15863.

Amerika Robotik Yol Haritası ve insan-robot etkileşiminde arama kurtarma, sağlık hizmetleri, güvenlik alanları gibi birçok etik ve hukuki prensipler temel alınmıştır. Ulusal strateji planlarının 2018 yılında Yapay Zekâ Komitesi kurularak geliştirilmesiyle birlikte ise ülkelerde mevzuat düzenlemeleri kendine yer bulmuştur[28]. Temelde en önemli kavramlardan biri, güvenlik için kanunlaştırma çalışmaları ve uygulamalarıdır. Burada yapay zekâların denetlenmesi amacıyla siber güvenliğin sağlanması odaklı bir değerlendirme yapılabilir. TCK m. 20, yapay zekânın eylem ve işlemlerinden sorumlu olarak tüzel kişileri göstermektedir. Daha doğrusu yapay zekâ sistemlerinin şirketlerde kullanımının zorunluluk haline gelmesi, güvenlik tedbiri açısından tüzel kişinin sorumlu tutulduğunu göstermektedir. Ancak varlığın ya da kuruluşun tüzel kişi olarak değerlendirilmesi, tamamıyla yasa koyucunun takdirine bırakılmıştır. Örneğin Yeni Zelenda'daki Whanganui ile Hindistan'daki Ganj Nehri veya başka ülkelerde bazı idollere hukuki kişilik tanınmıştır. Burada kişilik, gerçek ya da tüzel kişi olmaya bağlanan hukuki bir ölçüdür. Dolayısıyla buradaki örnek, Ganj nehrinin tüzel kişiliğinde olduğu gibi, varlığın ya da kuruluşun tüzel kişi olarak tanınması, tamamıyla ilgili hukuk sisteminin gereklerine göre yasa koyucunun takdirine bırakılmıştır[29]. Dolayısıyla yapay zekâ kapsamında hukuki süreçlerin geliştirilmesi, tüzel kişi ya da gerçek kişi olmaya yönelik de bir ayrım içermektedir. Yapay zekâdan sorumlu kişilerin tüzel kişi olarak sorumlulukları artırıldığında, yapıcı çalışma ve sonuçlar alınabilecektir. Tüzel kişinin arkasındaki kişilerin sorumlulukları, yani şirketin tamamının sorumlu tutulması, yaptırımların artırılmasına yardımcı olacaktır. Burada asıl sorun yapay zekâya kişilik tanınıp tanınmamasına dayanır. Yaşanan sorunlardan yapay zekânın sorumlu olması, kişilik tanınmasına ilişkin bir durumdur. Örneğin buna ilişkin bir açıklamaya göre, 2016 yılında Sophia adlı bir robota kişilik tanıyan Suudi Arabistan, vatandaşlık hakkı tanımıştır. Dünyada vatandaşlığa sahip ilk robot olarak Sophia, Birleşmiş Milletler tarafından da unvan verilen ilk robottur. Çünkü ilk İnovasyon Şampiyonu olma özelliğine sahiptir. Bu olayla birlikte hukukçular arasında robotlar için hukuki kişilik tartışması başlamıştır[30]. Bu kişiliğin özelde cezai sorumluluk açısından yapay zekâyı tasarlayan kişilere uygulaması önemli bir sorun olmuştur. Doğrudan

[28] Gizem Yılmaz, "Yapay Zekânın Yargı Sistemlerinde Kullanılmasına İlişkin Avrupa Etik Şartı", *Marmara Avrupa Araştırmaları Dergisi*, 28(1), 2020, s. 31-32.

[29] Yılmaz, *Yargı Uygulamasında Yapay Zekâ Kullanımı – Yapay Zekâ Hakim Cübbesini Giyebilecek mi?*, s. 391.

[30] Yılmaz, *Yargı Uygulamasında Yapay Zekâ Kullanımı – Yapay Zekâ Hakim Cübbesini Giyebilecek mi?*, s. 390-391.

uygulama ve yaptırımların yetersizliği, uluslararası hukuk çerçevesinde de önemli bir problem olarak görüldüğünü, yapay zekâya kişilik tanınmasının sorunları daha da çok artırdığını göstermektedir.

Ulusal güvenlik için siber risklerin belirlenmesi ve suçların önlenmesinde kullanılacak sistem olarak yapay zekâ, mücadelede önemli bir rol üstlenebilir. Sanal alanda güvenlik faktörü olarak siber risklerin azaltılması, siber suçların işlenme şekillerini bilmekle ilişkilendirilebilir. Truva atı, bukalemun, yerine geçme, mantık bombaları, artık toplama, gizli dinleme, süper darbe, salam tekniği, bilgi aldatmacası, ağ solucanları, bilgisayar virüsleri, istem dışı alınan elektronik iletiler, web sayfası hırsızlığı ve yönlendirmeler, phishing olarak gruplandırılan siber suçlar, yapay zekâ sistemlerinin kullanılmasını amaçlayan uygulamaların her biri için güvenlik konusunu öne çıkarmaktadır[31]. Yapay zekâ sistemleriyle siber suçların önlenmesinin günümüze ilişkin mücadeledeki önemi, siber terörizmin ulusal güvenlik haline gelmesiyle de bağlantılıdır. Terörist gruplarının internetin sunduğu avantajlardan da yararlanması, günlük yaşamda hemen her konunun siber uzay içinde yer almasına neden olmuştur. Çevrimiçi platformlarda şiddetin görülmesi, devlete saldıran grupların varlığı gibi birçok unsur, siber güvenliğin daha geniş bir ölçekte ele alınmasını gerektirmiştir. Ulusal güvenlik mekanizmasına saldıran siber terörizmin etkisi, terör örgütü faaliyetlerinin internet ortamında görülmesinden dolayı risklidir. Dijital savaşların varlığıyla siber riskler, ulusal güvenlik platformu bağlamında değerlendirilir[32]. Siber terörizmin potansiyel tehdit yaratması, hükümete ve özel bilgisayar sistemlerine saldırı gerçekleştirmesi, askerî, finansal ve hizmet sektörlerine sorunlar yaratması gibi birçok faktörle bağlantılıdır. Siber mağduriyetin büyüklüğü, bilgisayar teknolojisine güvensizlik yaratmıştır[33]. Dolayısıyla siber risk hem devlete hem de şirketlere güveni sarsabilir. Mağduriyetin büyüklüğü, yapay zekânın suçlarla mücadelede kullanılması gerektiğini göstermektedir.

[31] Oğuz Turhan, *Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar)*, T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği Planlama Uzmanlığı Tezi, 2006, s. 47-58.

[32] Altun Altun, "Siber Suçların Kriminolojik Analizi", *International Journal of Social, Humanities and Administrative Sciences*, 8(48), 2022, s. 95.

[33] Gabriel Weimann, "Cyberterrorism", *United States Institute of Peace*, Special Report, 2004, s. 1.

1. İç Güvenlik Yönetiminde Yapay Zekânın Uluslararası Hukukta Yeri

Güvenliği sağlama ve mücadele zorlukları, siber alan üzerinden incelendiğinde, küresel boyutta bir etkiye sahiptir. Uluslararası çalışmalar devletlerin hepsini kapsadığı takdirde, siber risklerin azaltılmasına daha yapıcı yaklaşılabilir. 2001 yılında ise Avrupa Konseyi bünyesinde Budapeşte'de kabul edilen Siber Suç Sözleşmesi, adli yardımlaşmalara ilişkin hükümleri içerir. Uluslararası yardımlaşma mantığı ise, iş birliğinin bu yönde sağlanmasında küresel bir ölçektir. Bu durum ulusal güvenlikte etkili bir adım olarak görülmekle birlikte Türk hukuk sisteminde uygulanma durumu tartışmalıdır. Türk literatüründe 'bilişim suçu' yaygın düzeyde kullanılmış, ancak uzlaşının sağlanamadığı görülmüştür. Uluslararası alanda mutabakatın sağlanamadığı da söylenebilir[34]. Siber suçlar uluslararası hukukta iş birliğine dayanan konu olsa da temelde ulusal güvenlik için mücadeleler, rekabet gücünün önemli bir parçasıdır. Bilgi ve iletişim sistemlerinin güvenliği, yaşanabilecek güvenlik zafiyetlerini ortadan kaldıracak ve verilerin kötüye kullanımı üzerinde önleyici faaliyetleri kapsayacak konu için önemlidir. Kamu düzenine ilişkin bozulma, ulusal güvenliğin ihlal edilmesine neden olacaktır. Büyük ölçekli ekonomik zararlar da yine iç güvenliğin sağlanmasında siber suçların önlenmesini ve mücadele edilmesini gerektirir[35]. Siber güvenliğin uluslararası hukuktaki önemi ve yapılan çalışmalar incelendiğinde, ulusal güvenlik için etkisinin vazgeçilmez bir faktör olduğu görülmektedir. Bu nedenle siber suçları önlemede metot olarak yapay zekâ teknolojisi öne çıkar. Dijital alandaki suçların önlenmesi, bilgisayar ve makine öğrenimli araçlarla sağlanabilecektir.

a. Yapay Zekâ ve Siber Suçlar: Mücadelede Kullanıldığı Alanlar

Yapay zekâ, siber güvenlik için kullanımda henüz erken bir aşama olarak görülmektedir. Ancak büyük ölçekli firma ve kuruluşlar, güvenlik sistemlerini korumak amacıyla yapay zekâ sistemlerini geliştirmeye odaklanmışlardır. Siber saldırganların yetenek ve araçlarını devamlı geliştirmesi, yapay zekâ ve güvenlik algısının da artırılmasını gerektirmiştir. Buna bağlı çalışma

[34] Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 19(2), 2013, s. 1230-1231.

[35] Merve Erdem/Gürkan Özocak, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 68(1), 2019, s. 166-167.

ve uygulamalar, yapay zekâ algoritmasının geliştirilmesini siber suçlarla mücadelede etkili bir araç olarak görmüştür[36]. Siber suçlarla mücadelede yapay zekânın kritik bir rol üstlenmesi, siber istihbarattaki eksikliği sona erdirmek amaçlı bir uygulamadır. Bu konu için bir örnek, yapay zekânın siber risklere karşı korumada kullanım alanından iç güvenliği artırmaya ilişkin verilebilir. Yapay zekânın iç güvenlik yönetimine etkisi, siber suçlarla mücadele amaçlıdır. İç güvenliğin yönetiminde dengeleyici yaklaşım olarak yapay zekâ algoritmalarının geliştirilmesi hedeflenmiştir[37]. Siber güvenlik ve denetim mekanizması, iç güvenliğin yapay zekâ sistemiyle birlikte denetlenmesi anlamına da gelmektedir. Yapay zekânın kullanım alanlarından denetim, siber risklerle mücadelede etkili araçlardan biridir. Siber istihbaratın sağlanması kapsamında yapay zekâ, çözüm odaklı bir faktör olabilmektedir.

Siber güvenlik odaklı denetim mekanizması, makine öğrenim algoritmalarında üç ayrı kategoride değerlendirilebilir. Bunlardan ilki olan denetimli öğrenme, siber suçlarla mücadele için insanların davranış kalıplarını öğrenme odaklı yapay zekâ motorunu eğitmektedir. Yapay zekâ motoru için denetimli öğrenme, örneğin güvenlik açıklıkları gibi bir işlemi, birden çok ikili uygulama kalıplarının anlaşılması için geliştirilebilir. Denetimsiz öğrenmede yapay zekâ motoru ise, sınıflandırılmayan-gruplandırılmayan öğrenme modelleri içerisinde oluşturulabilir. Böylece hem güvenlik uzmanı hem de kötü niyetli korsanlardan korunacak sistem yapısı oluşturulabilir. Güvenlik açıklıklarının giderilmesinde yapay zekâ motorunun bu özelliğinin kullanılması ve geliştirilmesi önemlidir. Diğer yapay zekâ öğrenme motoru ise, takviyeli öğrenmedir. Daha iyi veri kalitesini sağlamak için performans iyileştirme, çevreyle etkileşim sağlayarak elde edilmektedir[38]. Diğer özelliklerde olduğu gibi bu son özellik de yapay zekânın birçok işlemi gerçekleştirebilecek güç ve potansiyele sahip olduğunu göstermektedir. Yapay zekâ sisteminin siber suçlarla mücadele için kullanımı, iç güvenliği sağlama, kamu ve özel sektörlerde veri güvenliğini artırma, hizmet sektörünü iyileştirme ve e-ticaret uygulamalarının güvenilirliğini sağlama gibi konulara ilişkin de incelenebilir. Ancak temelde sadece bu genel konularla sınırlı kalmayan, siber terörizme ortam hazırlayan dijital alan kullanıcılarını ortadan kaldırmayı amaçlayan birçok uygulama da yapay zekâ sistemlerinin mücadele

[36] Efe, "Yapay Zekâ Odaklı Siber Risk ve Güvenlik Yönetimi", s. 144.

[37] İrdem/Çobanoğlu, *Yapay Zekânın İç Güvenlik Yönetimi Üzerine Yansımaları: Siber Güvenlik*, s. 175.

[38] Efe, *Yapay Zekâ Odaklı Siber Risk ve Güvenlik Yönetimi*, s. 151-152.

için tercih edilebileceğini göstermektedir. İrdem ve Çobanoğlu hem devletin hem de özel sektörün bilgi güvenliğini korumada virüs programlarını örnek göstermişlerdir. Özellikle "hackleme" saldırılarında virüs programlarının etki potansiyeli, yapay zekâ yüklü sistemler aracılığıyla verilerin korunmasını sağlamaktadır. Bu yönde yapay zekâ teknolojileri olarak EDR, NDR, UEBA, TIP gibi uygulamaların kullanılması, bilgi güvenliği açısından etkili olabilir[39]. Başka örnek ise ulusal güvenliği sağlamak için kullanılan sistemlerden biri olan ABD'deki "ses kayıt algoritmaları" için verilebilir. Sahil güvenlik birimlerinin kullandığı algoritmalar ise yapay zekânın siber suçlarla mücadelesinde önemli bir yer tutar. Ayrıca iç güvenlik, ulaştırma gibi alanlarda yasa dışı ve tehlikeli malların kontrolü, yapay zekâ algoritmasıyla yapılabilmektedir. Bu tür çalışmaların ABD'de artış gösterdiği bilinmektedir. Sınır güvenliğinin sağlanmasında da yine ABD, yapay zekâ sistemlerini siber güvenlik için sadece dijital alanla sınırlandırmayıp sistem üzerinden kontrolü sağlamaya çalışmaktadır. Ayrıca yapay zekâ otonom araçlarının da hava, kara, deniz kuvvetlerinde kullanımı, siber güvenliğin bir parçasıdır[40]. Dolayısıyla yapay zekânın kullanım alanı oldukça çeşitli olup siber güvenlik için bir mücadele yöntemi şeklinde görülebilir.

b. Siber Suçlarla Mücadelede Geliştirilebilecek Yapay Zekâ Uygulamaları

Siber altyapı sistemleri, müdahale ve tehditlere karşı savunmasızdır. Fiziksel cihazların ve insan müdahalesinin yetersiz kaldığı sistemlerdir. Bu nedenle siber savunma sistemlerinin kullanımı esnek, uyarlanabilir ve sağlam olması gereken, akıllı gerçek zamanlı kararlar alabilen sofistike sistemleri gerektirmektedir. Yapay zekâ, siber güvenlik ve savunma sistemlerinin bu hedefler doğrultusunda kullanılabileceği sistemlerdir[41]. Yapay zekâ sistemleri, teknoloji alanını daha kolay kullanma imkânı sunmaktadır. Hızlı ve kolay işlem imkânlarının yanı sıra güvenilir olması da beklenmektedir. Siber savunma mekanizmasında bu sistemlerin analiz etme süreçleri hızlı ve etkilidir. Böylece en kısa sürede tehdit oluşturan faktörleri belirleme ve

[39] İrdem/Çobanoğlu, *Yapay Zekânın İç Güvenlik Yönetimi Üzerine Yansımaları: Siber Güvenlik*, s. 186.

[40] Daniel Hoadly/Nathan Lucas, "Artificial Intelligence and National Security", *Congressional Research Service*, Report, 2018, s. 10-13.

[41] Selma Dilek/Hüseyin Çakır/Mustafa Aydın, "Applications of Artificial Intelligence techniques to Combating Cyber Crimes: A Review", *International Journal of Artificial Intelligence & Applications*, 6(1), 2015, s. 21.

yüksek düzeyde bir koruma sağlayabilme gücüne sahiptir. Ancak böyle bir ortamda özellikle de siber uzayın bir sınırlılığı belirlenemediği için hukuki işlemlerin yapılması zorlaşmaktadır. Çünkü yargı yetkisini tespit etmek zordur[42]. Bu nedenle siber suçlarla mücadele için geliştirilebilecek yapay zekâ uygulamaları sınırlıdır. Hukuki düzenlemeler geliştirilmeden yapay zekâ sisteminin siber suçlarla mücadelede yetersiz kalacağı ifade edilebilir. Söz konusu hukuki düzenlemeler, bilişim suçlarının incelendiği maddelerden biri olan TCK m. 245 kapsamında incelenebilir[43]. Yasak cihaz ya da programların kötüye kullanılmasını önlemeyi amaçlayan TCK m. 245/A hükmü şu şekilde düzenlenmiştir:

"Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır."

Bilişim teknolojileri ve beraberindeki uygulamalar, kötüye kullanım çerçevesinde denetlenmesi gereken, ancak bu konuda yapay zekâ çalışmasının yetersiz kaldığı uygulamalardır. Yapay zekâ sistemlerinin en büyük tehlikelerinin güvenlik ve etik sorunu olması, bilişim sistemlerinin güvenliğinin test edilmesini önemli kılmaktadır. Bu kapsamda yapay zekâ testlerini her yönüyle değerlendirme amacıyla tercih edilebilecek sistemin geliştirilmesi, mevzuatlarla desteklenmesi, TCK m. 245/A hükmünün de bu mevzuata dâhil edilmesi önemli görülebilir. Dolayısıyla TCK m. 245/A'nın yapay zekâ uygulamalarında güvenilirliği sağlamada ve kontrol mekanizmasını oluşturmada etkili bir mevzuat olabileceği yorumlanabilir.

Yapay zekâ uygulamalarının siber güvenlikte uygulama alanı fazladır. Derin öğrenme, gözetimli ya da gözetimsiz öğrenme gibi çeşitlerden bahsedilebilmekle birlikte öncelikli olarak hangi alanda kullanılacaksa ona göre geliştirilmesi hedeflenmektedir. Temel amaçlardan biri güvenlik olmakla birlikte ulusal ve ulus ötesi yetkinliğin sağlanması önemlidir. Özellikle sınır

[42] Akanksha Chauhan, "Role of AI in Cyber Crime and Hampering National Security", *SSRN*, 9, 2022, s. 1.

[43] Nurşen Selen Agin, *Türk Ceza Hukuku'nda Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık Suçu (TCK m.158/1-f)*, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, 2019, s. 41.

anlayışının geniş olması, güvenliği sağlamayı zorlaştırmıştır. Yeni politika ve stratejiler, siber güvenlik alanını artırmada etkili metotlardan biridir. Örneğin siber istihbarat, terör, insan kaçakçılığı, uyuşturucu ticareti, yasa dışı göç gibi sorunlar, yapay zekâ sistemleriyle denetlenip önlenebilir. Yapay zekâ yeteneklerinin geliştirilmesi ve yönetişimin sağlanması, çok disiplinli ve paydaşlı bir alandır. Bunun için politika önerileri, teknik ve hukuki hususların geliştirilmesi gibi konular, eşgüdümlü çalışma yapmayı gerektirmektedir[44]. Bu kapsamda bir değerlendirme, uluslararası hukukta Siber Suç Sözleşmesi'nin yasak cihaz ve programların üretilmesi ya da elde bulundurulmasının sözleşmeye taraf devletlerden istenmesi yönüyle yapılabilir. Bu durum, yapay zekâ uygulamaları için de aynı şekilde taraf devletlerden bunun istenmesini zorunlu kılmaktadır. Bir görüşe göre ise, Siber Suç Sözleşmesi taraftarları, bilişim alanında işlenen suçlarla mücadele etmek için ulusal mevzuatlarını geliştirmeyi ve bazı suçlarla kanunlaştırmayı taahhüt etmektedir. Türkiye'nin 2010 yılında imzalamış olduğu bu sözleşme, 2014 yılında Sanal Ortamda İşlenen Suçlar Sözleşmesi adıyla yürürlüğe girmiştir. Bu amaçla birtakım değişikliklerin iç hukukta görüldüğü, bunun ise TCK m. 245/A olduğu dikkat çekmiştir. Bu madde, bilişim alanında suçlar bölümüne eklense de[45], söz konusu maddenin yapay zekâ uygulamaları için doğrudan kullanım odaklı olması önerilebilir. Maddenin bağımsız şekilde düzenlenmesi önemli bir gelişme olmakla birlikte siber suç ve yapay zekâ kapsamlı çalışmaların artırılması, uluslararası hukukta Siber Suç Sözleşmesi doğrultusunda bunun önemli olacağını göstermektedir. Siber saldırı ve mağduriyet çerçevesinde bu konu önemli bir yere sahiptir. Bir diğer görüşe göre, siber saldırıların önemli sonucu, siber mağduriyetleri yaşatmasıdır. Sektörel ve devlet özelinde bunun sonuçları olmakla birlikte online siber zorbalıklara maruz kalan bireylerin, siber travma yaşayabileceği, yeni mağduriyetlere maruz kalabileceği bilinmektedir. Yapay zekâ sistemleri, dinamik ve esnek yapıda olduğu için mağduriyetlerin önlenebileceği uygulama ve çalışmaların da hedeflenmesi önemlidir[46]. Siber zorbalıklarla mücadelede bu tür konular, yapay zekânın hem adalet hem de güvenlik kriterleriyle geliştirmeyi önemli gösterir. Yapay zekânın etik ilkelere

[44] Mustafa Kürşat Şahiner/Emrah Ayhan/Murat Önder, "Yeni Sınır Güvenliği Anlayışında Yapay Zekâ Yönetişimi: Fırsatlar ve Tehditler", *Uluslararası Çalışmalar Dergisi*, 5(2), 2021, s. 83.

[45] İslam Safa Kaya/Adem Çakır, "Yasak Cihaz veya Programlar Suçu", *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 38, 2020, s. 32.

[46] Görkem Derin/Erdinç Öztürk, *Yapay Zekâ Psikolojisi ve Sanal Gerçeklik Uygulamaları*, 1. Bası, Türkiye Klinikleri, 2020, s. 42-44.

bağlılığı ve siber suçlarla mücadele edecek düzeyde geliştirilmesi, hukuki prosedürle bunun bir zorunluluk olmasıyla sağlanabilir.

B. Siber Risklerle Mücadelede Bilişim Uygulamalarının Denetlenmesi

Bilişim uygulamalarının denetimi, siber riskleri önlenmede ve savunma mekanizmasını geliştirmede önemli bir faktördür. Siber risklerin önlenmesi amacıyla politikaların geliştirilmesi ve bu politikalar aracılığıyla teknolojik gelişmelerin hız kazanması söz konusudur. Dolayısıyla güvenlik için politikalar, öncelikli konular arasında yer almaktadır. Siber güvenlik için yenilikçi çalışmaların yapılması ve gerekli güvenlik politikalarının oluşturulması, siber alanda doğru bir stratejinin geliştirilmesiyle sağlanabilir. Bunun yanı sıra denetimde etkililik ve yaygınlık için uzaktan denetimin de aynı şekilde oluşturulması önemlidir[47]. Yönetim ve denetim, bilişim uygulamaları için siber güvenlik odaklı oluşturulabilir. Siber tehditleri ortadan kaldırmanın ya da siber riskleri bilgi teknoloji sistemleri üzerinden hemen tespit etmenin gerekliliği, verileri korumayla bağlantılıdır. Çünkü başarısızlık durumunda finansal kayıpların oluşması ve güven kaybının yaşanması, mağduriyet yaratabilmektedir. Atakan çalışmasında ifade edilen uzaktan denetimin yanı sıra[48], Güngör çalışmasında belirtilen iç denetim[49] de önemlidir. Siber güvenliğin bilgi ve iletişim teknolojileri açısından gerekliliği, uluslararası mekanizmanın bu konuda eksik kalması sonucuyla bağlantılı olup ülkelerin kendi hukuk ve kültür anlayışına bağlı birtakım çalışmalarla hukuksal düzenlemeye gidildiğini göstermiştir[50]. Bu durum, siber riskleri önlemede kısmi ölçüde bir koruma sağlamaktadır. Kablosuz iletişim teknolojilerinin tehlikesi ve siber saldırı, devlet kurumları açısından askerî ya da siyasi saldırı yaratabilecek durumlarla incelendiğinde, çeşitli çözüm önerileri geliştirilir[51]. Bunlardan biri, bilişim uygulamalarının denetimidir. Uygulamaların denetimi

[47] Mehmet Atakan, "Siber Güvenlik Risklerinin ve Covid-19 Salgınının Uzaktan Denetim Üzerindeki Etkileri", *Denetişim*, 22, 2021, s. 27-28.

[48] Atakan, *Siber Güvenlik Risklerinin ve Covid-19 Salgınının Uzaktan Denetim Üzerindeki Etkileri*, s. 28-29.

[49] Nevzat Güngör, *İç Denetimde Bilgi Teknolojileri ve Siber Güvenlik: Borsa İstanbul Şirketlerinde Bir İnceleme*, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı Doktora Tezi, 2021, s. 261-265.

[50] Nezir Yeşilmen, *Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik*, Orion Kitabevi, 2018, s. 85-86.

[51] Yuchong Li/Qinghui Liu, "A Comprehenvise Review Study od Cyber-Attack and Cyber Security: Emerging Trends and Recent Developments", *Energy Reports*, 7, 2021, s. 8176.

ve siber riskle mücadele ilişkisi, şirketlere bu konuda yaptırımların hukuki ölçüde sunulmasını gerektirir. Bir başka ifadeyle denetimin iyileştirilmesi ve bir performansın kazanılması, siber güvenlik bağlamında yapılacak çalışmaların artırılması, eğitimlerin verilmesi ve bunun zorunlu tutulmasıyla sağlanabilir. Hukuki düzenleme açısından yetersizlik, şirketlere büyük sorumlulukların düştüğünü göstermektedir. Ayrıca Efe çalışmasında da vurgulandığı gibi, risk-tehdit analizlerinin yapılması ve değerlendirilmesi önemlidir. Bunun yanı sıra ise hesap verilebilirlik modelinin tanımlanması, kontrol mekanizma çevresinin oluşturulması, siber yetenek stratejisinin yeniden geliştirilmesi gibi çalışmalar, bilişim uygulamalarını denetleyerek siber riski azaltmada elverişli olacaktır[52]. Siber risklerin azaltılmasında genel sorumlulukların şirketler özelinde açıklandığı, bunun hukuki prosedürle zorunlu çalışmalara tabi tutulmadığı durumda kişisel verilerin yeterince korunup saklanmadığı sonucu karşımıza çıkacaktır.

1. Siber Güvenliğin Hukuksal Dayanımı ve Hukuki Prosedür Zorunluluğu

Devletlerin kendi mevzuatlarını oluşturmalarının ve yaptırım mekanizmasını ortaya koymalarının avantajları, siber uzayda egemenlik konusuyla öne çıkmaktadır. Uluslararası ve iç hukuk mekanizmalarında siber güvenlik, saldırıların uluslararası toplumu yakından ilgilendiren konu olması dolayısıyla küresel çapta gerekli önlemlerin alınmasını gerektirmiştir. Hukuki düzenlemelerde ise ABD, Avustralya, Çin, Küba gibi ülkeler, mevcut kuvvet kullanma yasağını uluslararası hukuk kuralları çerçevesinde uygulamışlardır. Yine kuruluş ve örgütler uluslararası hukuk bağlamında yetkin prosedürleri oluşturmada etkilidir. Siber güvenlikle ilgilenen örgütler arasında Kuzey Atlantik Antlaşması Örgütü (NATO), Afrika Birliği, Şangay İş Birliği Örgütü, Avrupa Konseyi bulunmaktadır[53]. Öne çıkan devletlerin kuruluş ya da örgütlerle birlikte sahada yer aldığı görülmektedir. Örneğin bir görüşe göre, büyük veri ve yapay zekâ teknolojilerinin her alanda karar vermede etkili olduğu, bunlardan birinin ise askerî karar verme süreçlerinde öne çıktığı söylenebilir. Sahadaki uygulamalara entegre olması, Askerî Karar Verme Süreçleri (AKVES) uygulamasıyla uzun vakit alan konuların hızlı bir şekilde

[52] Efe, *Yapay Zekâ Odaklı Siber Risk ve Güvenlik Yönetimi*, s. 161.

[53] Erdem/Özocak, *Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü*, s. 127-133.

çözümlenebileceği bir saha çalışması başlamıştır[54]. Siber risk ve savunma konusu, siber savaşların askerî alanda önemli yere sahip olduğunu göstermiş, bu konuda NATO çalışmaları dikkat çekmiştir. Siber risklere karşı çözüm bulmak ve siber savaşlarda kuvvet kullanımının nasıl olabileceğine yönelik metot geliştirmek birçok açıdan gayret göstermenin bir sonucu olmuştur. Bunlardan biri, NATO'nun 2013 yılında hazırladığı Tallinn El Kitabı'dır. Bu el kitabı kapsamında, siber güvenliğin hukuksal boyutu tartışılmıştır. Bu tartışma, Ortak Siber Savunma Mükemmeliyet Merkezi'nin 2009'da oluşturduğu uluslararası uzmanlardan oluşan grupla birlikte yapılmıştır. El kitabında siber savunma, kuvvet kullanma, meşru müdafaa hakkı ve kolektif güvenlik sistemi işlenmiştir. Bu kılavuza göre, siber eylemlere bağlı kuvvet kullanma konusu siber saldırının büyüklüğü ve etkinliği içerisinde ele alınmıştır. Siber saldırı klasik bir faaliyetle karşılaştırılabilecek oranda ise kuvvet kullanma olarak yorumlanmıştır. Bu durumda devlet bütünlüğü, egemenliği ya/ya da hürriyetine siber saldırı gerçekleştiği kabul edilmiş, hukuku aykırı olduğu değerlendirilmiştir. Dolayısıyla siber saldırının büyüklüğünü baz alan bir kılavuz, NATO tarafından siber suçlar çerçevesinde dikkate alınmıştır[55]. Dolayısıyla örgüt ve kurumlar, yapay zekâ teknolojisini sahada stratejik düzeyde kullanmayı hedefleyen uygulamalara odaklanmakta, kılavuz yayınlamakta ve hukuksal olarak bunu gerçekleştirmeyi hedeflemektedir. Özellikle gelişmiş ülkelerde yapılan bu çalışmaların gelişmekte olan ülkelerde yetersiz kaldığı söylenebilir.

Türkiye'de kuruluş ve örgüt sayısının artırılması, hukuki düzenleme ve hukuki prosedürle birlikte daha etkili çalışmaları yapmak için önemlidir. Avrupa Birliği'nin siber güvenliği hukuk çerçevesinde incelendiğinde, Avrupa Birliği Siber Güvenlik Kanunu, teknoloji ürünlerinin kullanılmasında devletlere ufuk açıcı uygulamalardan oluşmaktadır. 58 maddeden ve 4 ana başlıktan oluşan kanun kapsamı, özellikle de siber saldırı, güvenlik açıklığına bağlı sorunları ele almaktadır. Bu kapsamda etik düşünce yapısına uygun ve siber riskleri azaltan uygulamaların tercih edilmesi ya da denetimden geçmesi konusu geliştirilmeye çalışılmaktadır. Yasanın omurgası, kanunun

[54] Ertuğrul Serkan Yalınpala/Özgür Körpe, *Sanal Görüş Sistemlerinin Askerî Karar Verme Süreçlerinde ve Kurmay Subay Eğitimlerinde Kullanımı*, *Harpte Yeni Kavramlar Operatif Sanat, Teknoloji ve Harp Hukukundaki Yansımalar*, Ed. Özgür Körpe, Milli Savunma Üniversitesi Yayınları, 2021, s. 61.

[55] Hasan Temel, *Kuvvet Kullanma Hukuku Kapsamında Siber Saldırı Kavramı*, *Harpte Yeni Kavramlar Operatif Sanat, Teknoloji ve Harp Hukukundaki Yansımalar*, Ed. Özgür Körpe, Milli Savunma Üniversitesi Yayınları, 2021, s. 133.

2. başlığında incelenen Avrupa Siber Güvenlik Ajansı'na birçok yetki ve sorumluluk yüklemiştir. Bu sorumluluklardan bazıları şunlardır[56]:

- Siber güvenlik için uzmanlık merkezi görevini üstelenen ajans, bilimsel ve teknik kalite kapsamında çalışmalar yapmaktadır.

- Ajans, üye devletlerin siber güvenlik dâhilinde geliştirdikleri politikaları ve uygulamayı hazırlamaya yardımcı olmalıdır. Ajansın kapsamlı yetkiye sahip olduğu ve onu otoriter sahibi yaptığı bir açıklamadır.

- Üye devletler, sınır dışında bir olay yaşadıkları takdirde, siber tehditlerden korunmaları için gereken eylemler sunulacaktır. Siber güvenlik kapasitesini artırabilecekleri birçok durum için eylemlerin tanımlanması sağlanabilecektir.

Avrupa Birliği Siber Güvenlik Kanunu'nun kendini güncel tutması için sertifika süreleri daha kısa süreyle şirketlere sunulmuştur. Kanunun 47. 49. ve 51. maddelerinde işlenen konular, bu amaçla kanunu önemli kılmaktadır. Madde 47, sertifikanın şemasını ve özelliklerini ele almıştır. Bu yalnızla Avrupa Birliği için geçerli değildir, bunun yanında ulusal sertifikasyonun nasıl yapılacağına da değinilir. 51. maddede, bu amaçla bilgi iletişim ve teknoloji ürünleri için beş yıl şartı aranmıştır. Sertifika süreciyle, ürün ve hizmetlerin yeni teknolojilerle güvenliğinin artırılabilmesi amaçlanmıştır. İleri teknolojinin yanı sıra ileri güvenlik olarak bu uygulamalar hukuki prosedür zorunluluğuyla incelendiğinde, hukuki ve teknik adımların birbirini kapsadığı ifade edilebilir. Bununla birlikte dijital uygulama ve ürünlerin tamamında "siber güvenlidir" onayının alınması sağlandığı takdirde, güvenilirliğin sadece bir tercih sebebi olmayıp zorunlu tutulabileceği hukuksal bir dayanım haline dönüşeceği söylenebilir[57]. Hukuki prosedür, kendini sürekli geliştirmeli ve yenilemelidir. Bunun önemi, özellikle bilişim teknolojilerini kullanan insanların güvenliğini sağlayabilmektir. Hukuki süreçler devamlı geliştirilmediği takdirde uygulamaların güvenlikli olup olmadığı sorgulanmaktadır. Süreçlerin daha hızlı olması, bilişim ve iletişim teknolojilerinde yaşanan gelişmelerin yakalanması için çalışmaların artırılması, kanunun yanı sıra yönetmelik ihtiyacının da olduğunu göstermektedir. Yönetmeliklerle uyumu daha hızlı şekilde sağlama ve yakalamada etkili olabileceği, siber saldırıların

[56] Sena Nezgitli/Recep Benzer, "Avrupa Birliği Siber Güvenlik Kanunu", *Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi*, 2(1), 2020, s. 14-16.

[57] Nezgitli/ Benzer, "Avrupa Birliği Siber Güvenlik Kanunu", s. 15-16.

önlenmesinde ve yapay zekâ teknolojilerinin kullanılarak denetlenmesinde önemli bir sonuç yaratabilecektir.

Şirketlerin kendilerine yönelik politika ve sistem geliştirdiği söylenebilir. Bu konuda bir örnek, İş Bankası için verilebilir. Dijital dönüşümle hizmet ve süreçleri geliştirmek amacıyla İş Bankası, tehditlerle mücadelede yapıcı çalışmalar geliştirmiştir. Bunu ise herhangi bir hukuki mevzuata ihtiyaç duymadan yapmıştır[58]. Yapay zekâ algoritmalarıyla bunun sağlanması ve siber güvenlik çalışmalarının artırılması, hukuki düzenleme olmadan büyük şirketlerin bu tür uygulamaları yapabileceğini göstermiştir. Bu ise kalitesiyle öne çıkan şirketlerin güvenlik için geliştirdikleri bir stratejidir. Ancak şirketlerin sadece küçük bir kısmının hukuki zorunluluk olmadan yapay zekâ algoritmalarını ve siber güvenliği artırdığı söylenebilir. Dolayısıyla siber güvenlik için yapay zekânın hukuksal dayanım zorunlu olmalıdır. Ancak yapay zekânın hukuk dünyasında nasıl olması gerektiği de tartışmalı konulardan biridir. Dülger, yapay zekâ teknolojisinin yaratabileceği mahremiyet ve gizlilik açıklıklarının dikkate alınıp hukuksal düzenlemenin yapılması gerektiğini belirtmiştir[59]. Özellikle yapay zekâ performansının gün geçtikçe artması ve ülke içerisinde kullanımına izin verilen uygulamaların etik olmasına önemli bir kriterdir. Hukuki düzenleme ve mevzuat, uygulamaların güvenlik aşamalarından geçmesine ve etik olup olmadığının kullanım için değerlendirilmesine yardımcı olacaktır. Teknolojinin insan yararına kullanımını hedefleyen çalışmaların öncelikle hukuksal zeminde desteklenmesi, bu süreci kolaylaştırabilecektir. Ayrıca küresel geleceği etkileyebilecek sorunlar için şimdiden önlemlerin alınması, tehditleri azaltmada etkili olabilecektir. Etik/güvenlik sorunu, devletlerin bu çalışmalarının uluslararası hukukta yer almasının önemli ve tüm dünyaya mesaj veren konulardan biri olacağını unutmamalıdır. Bu amaçla bilişim suçları açısından TCK m. 245/A maddesi, yapay zekâ uygulamalarını denetlemede etkili olabilecektir. Bu maddenin yapay zekâ ve siber suçlar için kullanımının yetkinliği artırılmalıdır. Kanun kapsamında bir diğer düzenleme mantığı, Avrupa Birliği Siber Güvenlik Kanunu'na göre geliştirilebilir. 2014 yılından günümüze kadar yapılan çalışmaların az olduğu, kanunların bu yönde daha etkin ve yapıcı uygulamalarla desteklenmesinin önemli olduğu kabul edilebilir. Diğer yandan kanundaki düzenlemelerin

[58] Özen Akçakanat/Ozan Özdemir/Mehmet Mazak, "İşletmelerde Siber Güvenlik Riskleri ve Bilgi Teknolojileri Denetimi: Bankaların Siber Güvenlik Uygulamalarının İncelenmesi", *Mehmet Akif Üniversitesi Uygulamalı Bilimler Dergisi*, 5(2), 2021, s. 264-265.

[59] Murat Volkan Dülger, "Yapay Zekâlı Varlıkların Hukuk Dünyasına Yansıması: Bu Varlıkların Hukuki Statüleri Nasıl Belirlenmeli", *SSRN*, 2021, s. 1.

belirli bölümler halinde geliştirilmesi, örgüt ve kurumların oluşturulması, sivil toplum çalışmalarının toplumu siber suçlardan koruyacak faaliyetlere odaklanması ve insan haklarının hukuksal zeminde aranması/artırılması gerekebilir. Kanun düzenlemesi, en küçük faktörden en büyük soruna göre gruplandırılmalıdır. Örneğin NATO'nun hazırladığı kılavuz, askerî alanda ve savaşta, siber saldırılara karşı savunmada, kuvvet kullanmada ne tür bir metot benimseneceğini ele almaktadır. Bunun gibi örneklerin artırılması ve savunma sanayi özellikli uygulamaların hukuksal zeminle korunması önemlidir. Ayrıca Avrupa Birliği Siber Güvenlik Kanunu'nun bilişim suçları için kurduğu Avrupa Siber Güvenlik Ajansı gibi özel ajansların kurulması, sürecin daha hızlı şekilde takip edilmesi ve denetlenmesinde önemli yere sahiptir. Uluslararası hukukta, örgüt ve kurum çalışmalarına bakılarak yapılan düzenlemeler, yapay zekânın öncelikle sektör bazında ele alınarak sürecin takibe alındığı ve bir sonuç beklendiği uygulamalardan oluşabilir. Bununla birlikte doğrudan insan güvenliğini hedefleyen çalışma oranlarının artırılması ve hukuksal olarak korumanın geliştirilmesi, buna ilişkin bir diğer önemdir.

b. Yapay Zekâ Sistemine Yaklaşım ve Hukuki Güvenlik (ChatGPT Örneği)

Ülkelerde yapay zekâyla ilgili kanunlar, öncelikle sistemin özerk bir tüzel kişilik, ayrı bir hukuk ve kontrolüne yönelik ele alınmasını gerektirir. Buna göre hukuki düzenlemenin ayrı yapılması, hukuki yönüyle güvenilir sistemlerin kullanılması için önemlidir[60]. Yapay zekâya ilişkin hukuki düzenlemeler, siber güvenlik alanında kullanım için de gereklidir. Hukuki düzenlemelerin yapılması için bir örnek ise, sosyal medya uygulamaları için verilebilir. Sosyal medyanın kontrol altına alınması, öne çıkan gelişmiş ülke çalışmalarına bakılması etkili bir faktör olabilir. Burada gizlilik sözleşmesiyle başlayan ve müşteri üzerinde olumsuz etki yaratan sonuçların önlenmesi, hukuki düzenlemelerle hedeflenebilir[61]. Hukuk kapsamında düzenleme içeriği, dijital suçlara ve suçlarda etik konusuna bakılarak incelenmelidir. Siber uzay endişesi, çevrim içi suçların incelenmesinde etik, güvenlik, saldırı, kimliklerin taklit edilmesi, gönderilerin izinsiz kullanılması gibi birçok konuya yönelik

[60] A. Atabekov/Oleg Aleksandrovich Yastrebov, "Legal Status of Artificial Intelligence Across Countries: Legislation on the Move", *European Research Studies Journal*, 21(4), 2018, s. 773.

[61] Taylan Gülaslan, "Sosyal Medya Güncel Tartışmalar: Sosyal Medyanın Kontrolü & Sosyal Medya Hizmet ve Gizlilik Sözleşmeleri & Yerli ve Milli Sosyal Medya", *Uluslararası Yönetim Akademisi Dergisi*, 4(1), 2021, s. 1-3.

incelenebilir. Bu konular, dijital denetim, gözetleme, koruma gibi faktörlere ilişkin hukuksal düzenlemelerin yapılmasını önemli kılmaktadır. Siber etik kurallarının yetersiz olduğu kabul edilmekle birlikte, siber suçlara ilişkin yeni hukuki düzenlemelerin yapılması da önemli bir yere sahiptir. Etik dışı sorunların hukuksal düzeyde yaptırımlarının yanı sıra, ticari konulara, telif haklarına, kişilik haklarına saldırıya göre de yorumlanması gerekmektedir[62]. Bu çerçevede sosyal medya ve dolayısıyla uygulamaların kontrolü, siber güvenliği artırılmış ortamlar olarak hukuki güvenliğin de önemli olduğunu göstermektedir.

Yapay zekâ uygulamaları hem bireylerin kişisel kullanımları için hem de işletmelerin iş potansiyelini artırmaları için kullanılan sistemlerdir. Örneğin Türk şirketlerinde yapay zekânın önemi, envanterin optimize edilmesi amacıyla kullanılan sistemleri incelemek için geliştirilen bir çalışmayla açıklanabilir. Ekonomik verimin alınmasında yapay zekâ sisteminin stok riskini ve güvenliğini yönetmede etkili bir faktör olduğu, bu sistemleri kullananların yüksek düzeyde verim aldıkları belirlenmiştir[63]. Bu örnekler çoğaltılabilmekle birlikte işgücü potansiyeli için yapay zekânın önemi, işletmelerin ne tür sistemleri tercih ettiklerini düşündürmektedir. Temel amaçlardan birinin güvenlik olması, siber güvenlik olmadan yapay zekâ sistemlerinin kullanım potansiyelinin etkili olamayacağını belirtmektedir. Özellikle de insansı robot davranışları, siber güvenlik ve etik konularını gündeme getirmektedir. Eğer hukuki düzenlemeler yetersiz ise bu tür sistemlere duyulan güven de azalmaktadır. Özellikle bazı ülkelerde, bireysel kullanımlarda bu tür uygulamaların etik sorun yaratabileceğine değinilmiş ve kullanılması yasaklanmıştır. Bu kapsamda bir örnek, son zamanlarda öne çıkan sürümüyle ChatGPT kapsamında incelenebilir. Dijital Dönüşüm Ofisi çalışmasına göre, ChatGPT'nin kullanımının yasaklanması, kullanım alanları içinde ele alınmıştır. Okul ve üniversitelerde bu uygulamanın yasaklanma düşüncesi, öğretmenler üzerinde yapılan çalışmaya göre, ev ödevlerini yapmak ve kopya çekmek amaçlı kullanıldığı için öngörülmüştür. Ocak 2023 tarihinde uygulamayı ilk yasaklayan okul, New York Devlet Okulları olmuştur. New York City eğitim departmanının sözcüsü Jenna Lyle, ChatGPT için güvenirliğin olmadığı konusuna yönelik eleştiri ve yorum geliştirmiş,

[62] Cengiz, "Siber Suçlar, Sosyal Medya ve Siber Etik", s. 407-417.

[63] Mohamed Mostafa, *Artificial Intelligence Applications in Supply Chain Management and Analysis in Turkey*, T.C. İstanbul Sabahattin Zaim Üniversitesi Lisansüstü Eğitim Enstitüsü İşletme Anabilim Dalı Yüksek Lisans Tezi, 2020, s. 91-92.

öğrenciler için bunun uygun olmadığını öne sürmüştür. Yasaklar bu amaç doğrultusunda başlamış ve birçok bölgeyi de etkilemiştir. Longview Okul Bölgesi, Seattle Devlet Okulları, Kelso Okul Bölgesi, Baltimore Devlet Okulları da uygulamayı yasaklamıştır. Bu yasaklar, birçok bölge okullarıyla devam etmiştir[64]. ChatGPT, şu anda en gelişmiş yapay zekâ sistemine sahip olarak insanların kolay şekilde eriştikleri ve birçok işte kullandıkları uygulamadır. Yasaklamada temel faktörlerden diğerinin ise, etik faktör ve güvenlik olabileceği söylenebilir. Sektörlerin tamamında kullanım kolaylığı sunan bu sistemlerin güvenlik açısından ne kadar kullanılabilir veya etik olduğu üzerine tartışmalar yapılmış, bazı ülkelerde doğrudan yasaklamaya gidilmiştir. Normalde; ChatGPT'nin güvenlik ve uçtan uça şifrelemede etkili olduğu ve siber saldırılara karşı korumada önemli bir fark yarattığı düşünülebilir. Dijital Dönüşüm Ofisi, güvenli oturum açma, yetkilendirme, bilgileri koruma, hizmetlere erişim gibi konularda bireye kişiselleştirilmiş bir ChatGPT sunulduğunu belirtir. Özellikle kimlik doğrulamanın kötü niyetli chatbotlar için olası tehlikeleri azalttığı bilinmektedir. Diğer yandan uçtan uça şifreleme ve kendi kendini imha eden mesajlar, gizlilik-güvenlik açıklığını önlemektedir[65]. Uygulamanın siber saldırılara karşı savunma mekanizması, birçok yapay zekâ sisteminin bu sistem örneğinde olduğu gibi, yapay zekânın siber suçlarla mücadelede kullanılabileceğini de göstermiştir. Benzer uygulamaların verilerin korunması için geliştirileceği unutulmamakla birlikte dünyada hangi kısıtlamalara tabi tutularak uygulamanın kullanılabileceği tartışmalıdır. Özellikle de ChatGPT için etik sorunlar, insan odaklı yaklaşımda bilgilerin ne oranda internet ortamından intihal yapılıp kullanıldığını ya da bilgilerin doğruluğunun neler olup olmadığını tartışılır düzeye getirmiştir. Doğal olarak uygulamanın öncelikle kısıtlama ya da sınırlama özelinde incelenip hukuki prosedürle denetlenmesi ve daha sonrasında kullanımına izin verilmesi gerekir.

Yapay zekâ sisteminin siber güvenlik için etkili mekanizmaya sahip olduğu bilinmekle birlikte uygulama özelliklerinin denetimden geçmesi önemlidir. Yapay zekânın etik boyutu ve denetlenmesi şirketlerde hem yapay zekânın kontrol edilmesini hem de bütünleşik yapay zekâ mantığıyla bu teknolojinin kendisinin denetlenmesini ifade eder. Bu şekilde iç denetim

[64] Dijital Dönüşüm Ofisi, *Chatbot Uygulamaları ve ChatGPT Örneği*, Türkiye Cumhuriyeti Cumhurbaşkanlığı, 2023, s. 42-44.

[65] Dijital Dönüşüm Ofisi, *Chatbot Uygulamaları ve ChatGPT Örneği*, s. 33-34.

ve iç kontrol mekanizmaları arasında ilişkisel bir mantık kurulabilecektir[66]. Şirketlerin etik sorunu ve bu açıdan denetlemelerin gerekliliği, yapay zekânın kullanım amacına göre değişmektedir. Etik problemi çok yönlü olduğu için yapay zekânın öncelikle sektörel olarak değerlendirilmesi gereken problemleri vardır. Örneğin bir görüşe göre biyoetik sorun, cerrahi olarak kullanılacak robot sistemlerinin güvenliğinin tam ve yetkin olmasını gerektirmektedir[67]. Etik sorunların ve yasakların getirildiği robotlar arasında insansı robotlar vardır. Bu robotlar, ChatGPT gibi birçok bilginin hızlı bir şekilde sunumunda etkili olan, ancak şüpheli olarak kabul edilen bilgilerin söz konusu varlığından şüphe duyulmasına yöneliktir. Bununla birlikte sosyal medyada insanların güvenliğini önleyen siber saldırılar vardır. Söz konusu sorunların ortadan kaldırılması, teknik çalışmaların artırılmasını ve bu amaçla yapay zekânın geliştirilmesini önemli kılmıştır. Yapay zekânın şirketlerde muhasebe, insan kaynakları gibi birçok alanda kullanılması yönünde etkisi, siber güvenliğin her ne olursa olsun önemli faktör olduğunu göstermektedir. Bunun için siber risk ve saldırılardan korunmanın yolu, hukuksal olarak ceza kanunundaki yaptırımın uygulanarak uluslararası düzeyde geçerlilik sağlanarak oluşturulması önemlidir.

Etik sorunların yaşanmasını önlemede yapay zekâ teknolojisine şüpheyle yaklaşılması ve siber mekanizmayla bu teknolojinin denetlenmesi, iç/dış kontrollerin yapıldığı uygulamaları gerektirmektedir. Bu durum bazı ülkelerde yapay zekâ uygulamalarının doğrudan kullanımına izin verilerek bazılarında doğrudan yasaklanarak bazılarında ise kısıtlamalarla yapılmaktadır. Genel güvenlik sürecinden geçmesinin elzem olduğundan bahsedilebilir. Dolayısıyla asıl sorun, uygulamanın güvenlik-etik konularıyla yapılan değerlendirmedeki yetersizlikten kaynaklıdır. Hukuksal açıdan çalışmalar, yapay zekânın yargı organlarında da kullanılabileceğine ilişkin değerlendirmeyi öne çıkarmaktadır. Bu kapsamda geliştirilen bir görüşe göre, her türlü hukuk metninin yapay zekâ sistem ve uygulamalarının temel parçası olabilecek şekilde düzenlemelere tabi tutulması önemli bir olay olarak yorumlanabilir. Hukuki uyuşmazlıkların giderilmesinde yapay zekâ teknolojisinin hukuk davalarında kullanılması değerlendirilmekle birlikte yapay zekânın hemen her açıdan yaşanabilecek

[66] Belde Duru Özcan/Mustafa Doğan, "Yapay Zekâ Denetim ve Kontrolü İçin Bütünleşik Yapay Zekâ Mantıksal Çerçevesi", *Üçüncü Sektör Sosyal Ekonomi Dergisi*, 57(4), 2022, s. 3160.

[67] Gülay Halidi, "Yapay Zekâ Etiği Tartışmaları İçin Bazı Tarihsel-Kavramsal Önbilgiler", *Türkiye Biyoetik Dergisi*, 9(4), 2022, s. 159.

sorunlara göre de denetlenmesi yine önemli bir unsur olabilir[68]. Bunun yanında ceza kanununa ve kapsamına göre, esaslı yaptırımlar uluslararası düzenlemeler çerçevesinde de ele alınmalı, idare hukukunun etkisinin de bu yönde önemli bir sonuç yaratacağı düşünülmelidir. Teknolojinin hızlı gelişmesi, kanun düzenlemesine ek olarak mevzuatın ve idare hukukunun karar almadaki etkinliği, hızlı çözüm önerisi bağlamında etkili olabilecektir. Bunun yanında yapay zekânın kanun kapsamında da irdelenmesi önemli bir yere sahiptir. Örneğin TCK m. 245/A, bu konuda esaslı yaptırımların yapay zekâ teknolojisi için yeterli olmadığını göstermektedir. Bunun yanı sıra uluslararası ölçekte Avrupa Birliği Siber Suçlar Kanunu'nun ulusal hukuk düzenlemesinde yetersiz kaldığı, bunun ise sertifika süresi, içeriği, denetimi gibi birçok konuyla birlikte geliştirilmesi gerektiği belirtilebilir. Yapay zekâ sistemleri, siber suçlarla mücadelede bu uygulama örneklerinde görüldüğü gibi etkilidir, ancak hukuki güvenlik açısından inceleme kriterleri yetersizdir. Diğer yandan yapay zekânın insan zekâsının ürünü olduğu ve onu yönetmenin hem etik hem de hukuki prosedürle yönetilebileceği unutulmamalıdır.

SONUÇ

Yapay zekânın geliştirilmesinin desteklenmesi, güvenliliği ve etik algısı konusu, hukuki prosedürlerin oluşturulmasını gerektirmektedir. Teknolojinin gelişmesi, kullanım olanaklarının daha güvenilir kılınması için hukuksal dayanım elzem görülmelidir. Burada temel amacın neler olabileceği, yapay zekânın hukuk içerisinde nasıl yer alacağı gibi konular üzerinde durulması, öncelikle güvenlik ve etik kapsamlı inceleme yapmayı gerektirmektedir. Siber güvenlik konusu açısından ise bu husus, siber riskleri azaltma, saldırıları önleme ve savunma mekanizmalarını oluşturmada, yapay zekâ sistemlerinin geliştirilme ve sürüme koyulmada belirli kriterlere bağlı tutulmasını gerektirmektedir. Her şeyden önce ise ulusal güvenlik ve siber uzayda uluslararası yetkinlik, rekabet edebilecek bir potansiyel yaratmada yapay zekânın da geliştirilebilmesinin önemli olduğunu göstermektedir.

Hukuki prosedürlerde özellikle de Avrupa Birliği Siber Güvenlik Kanunu'nun incelenmesi, geliştirilen yapay zekâ uygulamalarında güvenlik sorunlarının nasıl çözümlendiği üzerine teknik çalışmaların yapılması (ChatGPT örneği) gibi kriterler, mevzuatta eksikliklerin olmasını önleyecek

[68] Ömer Faruk Ebibli, *Hukuk Açısından Yapay Zekânın İncelenmesi*, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Yapı Sosyal Değişme Anabilim Dalı Yüksek Lisans Tezi, 2022, s. 1-3.

gelişmeleri öne çıkarır. Bunun yanı sıra uluslararası kuruluş çalışmalarında virüs programlarının öne çıktığı, bu sistemlerin Türkiye'de sektörel gelişmeleri hızlandırmak ve işletmelerin büyümesini sağlamak için tercih edilebilecek bir gelişme olduğu söylenebilir.

Araştırma kapsamında siber uzayın bütün sektörler üzerinde etki yarattığı, ancak siber savunmanın siber terörizmden korunma amaçlı ulusal bir güvenlik sorunu haline gelmesinin daha önemli olduğu, konunun ciddi ele alınması gerektiği görülmüştür. Sadece kullanıcıya sunulan uygulamaların siber güvenlik mücadelesiyle sınırlı kalmadığı, ülke güvenliğini de etkileyen insansız araçların yapay zekâ sistemlerinde etkin güvenlik kapsamıyla oluşturulduğu söylenebilir. Dolayısıyla araştırma kapsamında bu konuların önemli olduğu kabul edilmekle birlikte öncelikle siber güvenlik için hukuki düzenlemelere değinilmesi, uluslararası hukuk incelemesinin de bu konuda önemli yere sahip olunduğunun bilinmesi gerekmektedir. Bunun dünya genelinde bir tehdit olduğunun bilinmesi, gelişmiş ülkelerin bu konuda öne çıkan devletler olacağı, bunun da ilerleyen dönemlerde siber uzayda arka planda kalacak devletlerin çoğunlukta olacağı söylenebilir.

Dünyayı etkileyen bir tehdit olarak yapay zekâ ve siber güvenlik, hukuki düzenleme ve cezai yaptırımların temelinin yeterince oluşturulamaması halinde dünyanın sonunu getirebilecek bir sorun olarak görülebilir. Yeni küresel tehditlerden biri olabilecek bu konu, araştırma kapsamında yapay zekâ uygulama örneklerinin belirli ülkelerde yasaklanmasına ya da sınırlandırılmasına ilişkin değerlendirilen, hukuki önlemlerin teknolojinin gelişmesine katkı sunacak bir durum şeklinde görülmesinin önemli olduğunu göstermektedir. Bunun yanı sıra yapay zekâ ve siber güvenlik, ulusal güvenliğin en etkili unsurlarıdır. Siber uzayda savaşların bu konular içinde yaşanabileceği, dünyada bu konuda yapılan çalışmaların ve örgüt/kuruluş faaliyetlerinin de aynı şekilde sınırlı devletlerle kalabileceği belirtilebilir.

Devletlerin rekabet edebilecek teknoloji yetkinliği için öncelikle yapay zekâ çalışmalarına ve siber güvenliğe odaklanmaları gerektiği tüm dünya genelinde önemli bir meseledir. İnsanların topluca bir tepki gösteremediği dünyada, yapay zekânın olası bir tehdit yaratabileceği ve insanlık için risk oluşturabileceği söylenebilir. Ayrıca zamanla bu riskin artacağı düşünülmektedir. Bu çerçevede çözümleyici nitelikte çalışmaların yapılması ve konunun üzerinde ciddiyetle durulması, en önemli hukuk ve insanlık meselelerinden biri olarak görülebilir. Kanaatimce; cezai yaptırımların zorunlu olması ve yapay zekâ sistemlerinde aranan temel kriterlerden

birinin siber suçlarla mücadele üzerine olması, sorunların daha hızlı şekilde çözümlenmesinde etkili olacaktır. Risklerin azaltılması, tehlikenin sonlandırılması, güvenliğin sağlanması ve ciddi savunma mekanizmalarının oluşturulması için dünya genelinde çalışmalar, kanun, mevzuatlar, teknik, idare hukuku gibi konularda öncelikle bu tür unsurlar baz alınarak yapılabilir.

KAYNAKÇA

Agin, N S, *Türk Ceza Hukuku'nda Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık Suçu (TCK m.158/1-f)*, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, 2019.

Akçakanat Ö/Özdemir O/Mazak M, "İşletmelerde Siber Güvenlik Riskleri ve Bilgi Teknolojileri Denetimi: Bankaların Siber Güvenlik Uygulamalarının İncelenmesi", *Mehmet Akif Üniversitesi Uygulamalı Bilimler Dergisi*, 5(2), 2021, s. 246-270.

Aldoori A., *Uluslararası Hukukta Siber Suçla Mücadele*, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, 2020.

Alptekin G., "2008 Rusya-Gürcistan Savaşı ve Savaş Sonrası Büyük ve Bölgesel Güçlerin Tepki ve Politikaları", *RUSAD*, 6, 2021, s. 110-130.

Altun A, "Siber Suçların Kriminolojik Analizi", *International Journal of Social, Humanities and Administrative Sciences*, 8(48), 2022, s. 91-99.

Atabekov A/Yastrebov O, "Legal Status of Artificial Intelligence Across Countries: Legislation on the Move", *European Research Studies Journal*, XXI(4), 2018, s. 773-782.

Atakan M, "Siber Güvenlik Risklerinin ve Covid-19 Salgınının Uzaktan Denetim Üzerindeki Etkileri", *Denetişim*, 22, 2021, s. 27-39.

Bilgi Teknolojileri ve İletişim Kurumu, *Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri*, 2022.

Cengiz G, "Siber Suçlar, Sosyal Medya ve Siber Etik", *İletişim Çalışmaları Dergisi*, 7(3), 2021, s. 407-424.

Chauhan A, "Role of AI in Cyber Crime and Hampering National Security", *SSRN*, 9, 2022.

Çelik S, "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım", *Academic Review of Humanities and Social Sciences*, 1(2), 2018, s. 110-119.

Derin G/Öztürk E, *Yapay Zekâ Psikolojisi ve Sanal Gerçeklik Uygulamaları*, 1. Bası, Türkiye Klinikleri, 2020.

Dijital Dönüşüm Ofisi, *Chatbot Uygulamaları ve ChatGPT Örneği*, Türkiye Cumhuriyeti Cumhurbaşkanlığı, 2023.

Dilek S/Çakır H/Aydın M, "Applications of Artificial Intelligence techniques to Combating Cyber Crimes: A Review", *International Journal of Artificial Intelligence & Applications*, 6(1), 2015, s. 21-39.

Dülger M V, "Yapay Zekâlı Varlıkların Hukuk Dünyasına Yansıması: Bu Varlıkların Hukuki Statüleri Nasıl Belirlenmeli", *SSRN*, 2021, s. 1-9.

Ebibli Ö F, *Hukuk Açısından Yapay Zekânın İncelenmesi*, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Yapı Sosyal Değişme Anabilim Dalı Yüksek Lisans Tezi, 2022.

Efe A, "Yapay Zekâ Odaklı Siber Risk ve Güvenlik Yönetimi", *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 5(2), 2021, s. 144-165.

Erdem M/Özocak G, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 68(1), 2019, s. 127-212.

Erdoğan G, "Yapay Zekâ ve Hukukuna Genel Bir Bakış", *Adalet Dergisi*, 66, 2021, s. 117-192.

Ghundare S/Patil A/Lad R, "Importance of Cyber Security", *International Journal of Engineering Research & Technology*, 8(5), 2020, s. 1-3.

Gülaslan T, "Sosyal Medya Güncel Tartışmalar: Sosyal Medyanın Kontrolü & Sosyal Medya Hizmet ve Gizlilik Sözleşmeleri & Yerli ve Milli Sosyal Medya", *Uluslararası Yönetim Akademisi Dergisi*, 4(1), 2021, s. 1-21.

Güngör N, *İç Denetimde Bilgi Teknolojileri ve Siber Güvenlik: Borsa İstanbul Şirketlerinde Bir İnceleme*, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı Doktora Tezi, 2021.

Halidi G, "Yapay Zekâ Etiği Tartışmaları İçin Bazı Tarihsel-Kavramsal Önbilgiler", *Türkiye Biyoetik Dergisi*, 9(4), 2022, s. 155-163.

Hoadly D/Lucas N, "Artificial Intelligence and National Security", *Congressional Research Service*, Report, 2018, s. 1-38.

İrdem İ/Çobanoğlu S, "Yapay Zekânın İç Güvenlik Yönetimi Üzerine Yansımaları: Siber Güvenlik", *Kaytek Dergisi*, 2, 2021, s. 175-202.

Karasoy A/Babaoğlu P, "Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı", *Yasama Dergisi*, 44, 2021, s. 123-155.

Kaya İ S/Çakır A, "Yasak Cihaz veya Programlar Suçu", *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 38, 2020, s. 32-55.

Li Y/Liu Q, "A Comprehenvise Review Study od Cyber-Attack and Cyber Security: Emerging Trends and Recent Developments", *Energy Reports*, 7, 2021, s. 8176-8186.

Mijwil M M/ Aljanabi M/ChatGPT, "Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime", *Iraqi Journal for Computer Science and Mathematics*, 4(1), 2023, s. 65-70.

Mijwil M M/Sadıkoğlu E/Cengiz E/Candan H, "Vergilendirme Sürecinin İdari İşlem Bağlamında İncelenmesi", *Veri Bilimi Dergisi*, 5(2), 2022, s. 97-105.

Mostafa M, *Artificial Intelligence Applications in Supply Chain Management and Analysis in Turkey*, T.C. İstanbul Sabahattin Zaim Üniversitesi Lisansüstü Eğitim Enstitüsü İşletme Anabilim Dalı Yüksek Lisans Tezi, 2020.

Nezgitli S/Benzer R, "Avrupa Birliği Siber Güvenlik Kanunu", *Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi*, 2(1), 2020, s. 10-17.

Önok M, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 19(2), 2013, s. 1229-1270.

Özcan B D/ Doğan M, "Yapay Zekâ Denetim ve Kontrolü İçin Bütünleşik Yapay Zekâ Mantıksal Çerçevesi", *Üçüncü Sektör Sosyal Ekonomi Dergisi*, 57(4), 2022, s. 3160-3175.

Özçelik B, "Yapay Zekânın Veri Koruma, Sorumluluk ve Fikri Mülkiyet

Açısından Ortaya Çıkardığı Hukuki Gereksinimler", *Adalet Dergisi*, 66, 2021, s. 87-116.

Pirim H, "Yapay Zekâ", *Journal of Yasar University*, 1(1), 2006, s. 81-93.

Polat S, *Milli Güvenlik Açısından Siber Güvenlik*, T.C. Ankara Hacı Bayram Üniversitesi Lisansüstü Eğitim Enstitüsü Amme İdaresi Anabilim Dalı Yüksek Lisans Tezi, 2020.

Selimoğlu S/Altunel M, "Siber Güvenlik Risklerinden Korunmada Köprü ve Katalizör Olarak İç Denetim", *Denetişim*, 19, 2019, s. 5-16.

Singh G/Mishra A/Sagar D, "An Overview of Artificial Intelligence", *SBIT Journal of Sciences and Technology*, 2(1), 2020, s. 1-4.

Şahiner M K/Ayhan E/Önder M, "Yeni Sınır Güvenliği Anlayışında Yapay Zekâ Yönetişimi: Fırsatlar ve Tehditler", *Uluslararası Çalışmalar Dergisi*, 5(2), 2021, s. 83-95.

Şenkaya Y/Adar U G, "Siber Savunmada Yapay Zekâ Sistemleri Üzerine İnceleme", *Akademik Bilişim*, 2014, s. 1-7.

Temel H, *Kuvvet Kullanma Hukuku Kapsamında Siber Saldırı Kavramı, Harpte Yeni Kavramlar Operatif Sanat, Teknoloji ve Harp Hukukundaki Yansımalar*, Ed. Özgür Körpe, Milli Savunma Üniversitesi Yayınları, 2021, s. 122-159.

Temitope A/Aderonke T/Ayoola F/ Owoyemi J, "Stop Cyber Attacks Before They Happen: Harnessing The Power of Predictive Analytics in Cybersecurity", *Journal of Multidisciplinary Engineering Science and Technology*, 10(4), 2023, s. 15863-15874.

Tosun Y/Gezginci E/Göktaş S, "Siber Güvenlik: Sağlık Hizmetleri Ne Kadar Güvende?", *JAREN*, 7(3), 2021, s. 157-161.

Turhan O, *Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar)*, T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği Planlama Uzmanlığı Tezi, 2006.

Ünal A/Kılınç İ, "Yapay Zekâ İşletme Yönetimi İlişkisi Üzerine Bir Değerlendirme", *Yönetim Bilişim Sistemleri Dergisi*, 6(1), 2014, s. 51-78.

Weimann G, "Cyberterrorism", *United States Institute of Peace*, Special Report, 2004, s. 1-12.

Yalınpala E S/Körpe Ö, *Sanal Görüş Sistemlerinin Askerî Karar Verme Süreçlerinde ve Kurmay Subay Eğitimlerinde Kullanımı*, *Harpte Yeni Kavramlar Operatif Sanat, Teknoloji ve Harp Hukukundaki Yansımalar*, Ed. Özgür Körpe, Milli Savunma Üniversitesi Yayınları, 2021, s. 61-88.

Yeşilmen N, *Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik*, Orion Kitabevi, 2018.

Yılmaz G, "Yapay Zekânın Yargı Sistemlerinde Kullanılmasına İlişkin Avrupa Etik Şartı", *Marmara Avrupa Araştırmaları Dergisi*, 28(1), 2020, s. 27-55.

Yılmaz O, "Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik", *Cyberpolitik Journal*, 2(4), 2019, s. 22-43.

Yılmaz O G, "Yargı Uygulamasında Yapay Zekâ Kullanımı – Yapay Zekâ Hakim Cübbesini Giyebilecek mi?", *Adalet Dergisi*, 66, 2021, s. 379-415.