ISSN: 2980-1311

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ

JOURNAL OF INFORMATION TECHNOLOGIES AND COMMUNICATION

CİLT: 1 SAYI: 1 TEMMUZ - EYLÜL 2023

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ

(BTK DERGİ)

JOURNAL OF INFORMATION TECHNOLOGIES AND COMMUNICATION

YIL: 1 SAYI: 1

TEMMUZ-EYLÜL 2023

ISSN: 2980-1311

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ (BTK DERGİ)

Hakemli Akademik Araştırma Dergisi

Bilgi Teknolojileri ve İletişim Kurumu Adına Sahibi
Ömer Abdullah KARAGÖZOĞLU

Editör
Dr. Abdulkerim GÜN

Editör Yardımcısı
Salih BOZKURT

Sorumlu Yazı İşleri Müdürü
Yakuphan GÜLEÇ

Redaksiyon
Kübra YAVUZ ÇAKIR

Yönetim ve İletişim
Bilgi Teknolojileri ve İletişim Kurumu Eskişehir Yolu Mustafa Kemal Mah.
No: 276 Posta Kodu: 06530 Çankaya/Ankara
e-posta: dergi@btk.gov.tr
web: https://dergi.btk.gov.tr

Yayın Türü:
Yaygın Süreli Yayın

ISSN
2980-1311

Grafik Tasarım
Yasemin KULA
Kevser GÜLDOĞAN

Baskı Adedi
100 Adet

Bilgi Teknolojileri ve İletişim Dergisi'nde yayımlanan yazılardaki görüşler yazarına aittir.

Bilgi Teknolojileri ve İletişim Dergisi üç (3) ayda bir yayımlanır.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ
(BTK DERGİ)

JOURNAL OF INFORMATION TECHNOLOGIES AND COMMUNICATION

YIL: 1 SAYI: 1 TEMMUZ-EYLÜL 2023

T.C. BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU HAKEMLİ AKADEMİK ARAŞTIRMA DERGİSİ

BİLİMSEL YAZIŞMA

Makaleler ile ilgili tüm soru ve yazışmalarınız için:
Tel: 0312 403 16 04
e-posta: dergi@btk.gov.tr

EDİTÖRDEN

Kıymetli Okurlar,

Bilgi Teknolojileri, Elektronik Haberleşme Sektörü ve Posta Sektörü üst başlıklarıyla ilgili bilimsel alan, disiplin veya alt disiplinlerde araştırmacıların ve akademi dünyasının araştırma ve çalışmaları doğrultusunda elde edilen bulgular ile güncel sektörel gelişmelerin bilimsel bir platformda duyurulması ve yayınlanması ile deneysel ve teorik bilgilerin paylaşılmasına, geliştirilmesine ve artırılmasına katkıda bulunarak en son bilimsel gelişmeleri bir araya getirmeyi amaçlayan Bilgi Teknolojileri ve İletişim Dergisi (BTK Dergi)'nin ilk sayısı ile okuyucularımızın karşısındayız.

Bu sayımızda ilk makalemiz, Dr. Halil İbrahim ÖZBİLGER, Birsen SARIYAR ve Ahmet ERTÜRK tarafından kaleme alınan *"Bilgi ve İletişim Güvenliği Rehberinin Uygulanması ve Denetimlerine Yönelik İyileştirme Önerileri"* dir. Bu makalede, 2022 yılında yapılan Rehber denetiminde sahada karşılaşılan zorluklar ve uygulama sonuçlarının değerlendirilmesinden yola çıkılarak, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi (BİGR)'ni uygulayacak idarelerde birincil denetim sorumlusu konumundaki iç denetçilerin, Bilgi ve İletişim Güvenliği Denetim Rehberi (BİGDR)'ni esas alarak gerçekleştirecekleri denetim faaliyetlerinde ihtiyaç duyulan iyileştirme önerileri sunulmuştur.

Doç. Dr. Canan GÖNÜLLÜ tarafından hazırlanan, *"Dijitalleşen Dünyada Dönüşen Yardım Anlayışı: Dijital Yardım Kampanyaları"* başlıklı makalede; yardım, dayanışma gibi kavramlar toplumsal bütünleşmenin aracı olarak incelenmiş ve dönüşen toplum yapısıyla birlikte yardımlaşma anlayışında meydana gelen değişimler değerlendirilmiştir.

Feridun GÜNGÖR tarafından kaleme alınan *"Gerçeklik Teknolojilerinin Uygulama Alanları ve Uygulama Zorlukları"* başlıklı makalede ilk olarak, iş dünyasında şirketler arası iş birliği ve müşteri odaklı çalışma modellerinde karşılaşılan zorluklar incelenmiştir. Girişimcilerin bu teknolojileri kullanırken karşılaştığı yasal düzenlemelerle ilgili zorlukların da ele alındığı makalede, gerçeklik teknolojisine yönelik kullanıcı kabulünü geciktiren sosyal ve teknolojik zorluklar işlenmiştir.

Bir diğer makale, Doç. Dr. Gökhan DELİCEOĞLU, Doktorant Merve ERDOĞDU ve Uzm. Psk. Gizem AYTAÇ'ın *"Bilgisayar Temelli Uygulamalar ile Sporcularda Dikkat ve Alt Bileşenlerinin Tespit Edilmesi: Bir Laboratuvar Çalışması"*dır. Makalede,

sporcuların dikkat düzeylerinin; zamanlama, planlama ve performansı sürdürme gibi beceriler üzerinde etkisinin olup olmadığı deneysel yöntemlerle incelenmiştir.

Burak YAĞCI'nın yazdığı *"Bilgi ve İletişim Teknolojilerinin Gelişmesiyle Değişen Siber Suç Tanımı ve Yaklaşımlar"* başlıklı makalede ise siber suçun tanımı üzerine ulusal ve uluslararası literatür taranarak, söz konusu alanda yer alan hukuki ve teknik boşluğun doldurulması amacıyla, Birleşmiş Milletler (BM) nezdinde halihazırda çalışmaları devam eden taslak sözleşme çalışması detaylı şekilde incelenmiştir.

Son olarak Arş. Gör. Erva KARADAĞ tarafından incelenen Ali Burak DARICILI'nın kaleme aldığı *"Siber Uzay ve Siber Güvenlik: ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi"* başlıklı kitap kritiği yer almaktadır.

Böylece bu ilk sayımızda 5 makale ve 1 kitap incelemesiyle karşınıza çıkıyoruz.

Bilgi Teknolojileri ve İletişim Dergimizin bu ilk sayısında yer alan makalelerin okuyucularımız için faydalı olmasını temenni eder, hepinize iyi okumalar dileriz.

Dr. Abdulkerim GÜN

Editör

İÇİNDEKİLER

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ (BTK DERGİ)
CİLT: 1 SAYI: 1 TARİH: TEMMUZ - EYLÜL 2023 ISSN: 2980-1311

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİNİN UYGULANMASI VE DENETİMLERİNE YÖNELİK İYİLEŞTİRME ÖNERİLERİ

Halil İbrahim ÖZBİLGER[1]

Birsen SARIYAR[2]

Ahmet ERTÜRK[3]

Özet

Teknolojik gelişmelerin etkisiyle giderek artan dijitalleşme, hayatı hızla değiştirmektedir. Bu dönüşüm, fırsatlarıyla beraber riskleri de getirmektedir. Bunun doğal sonucu olarak günümüzde, siber tehditlerin kurumların riskleri arasında en üst sıralarda yerini aldığı gözlemlenmektedir. Örneğin; veri sızıntısı, dağıtılmış hizmet reddi (DDoS), kimlik avı, yapılandırılmış sorgu dili (SQL) enjeksiyon, zararlı yazılım ve oltalama (Phishing), casus, reklam ve fidye yazılımları ile truva atları (Trojan), solucanlar (Worm), tuş kaydediciler, botlar olarak nitelendirilen kötü amaçlı zararlı yazılımlar (Malware), kurumların karşılaşabildiği bu tür siber tehditlerden bazılarıdır. Bu nedenle, tüm kurum ve kuruluşlarda olduğu gibi kamu idarelerinde de yürütülen iş ve işleyişin planlanması ile yeniden tasarımında gerek mevcut ve(ya) doğabilecek siber güvenlik risklerine karşı önlem alınması gerekse de bu risklerin gerçekleşmesi durumunda doğacak etkinin azaltılması amacıyla proaktif şekilde harekete geçmek, içinde bulunulan dönemde anahtar aksiyon haline gelmiştir. Bu çalışmada, öncelikle konu hakkında teorik çerçeve çizilmiş olup sonrasında 2022 yılında gerçekleştirilen Rehber denetiminde sahada karşılaşılan zorluklar ve uygulama sonuçlarının değerlendirilmesinden yola çıkarak T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi (BİGR)'ni uygulayacak idarelerde birincil denetim sorumlusu konumundaki iç denetçilerin BİGR'yi ve Bilgi ve İletişim Güvenliği Denetim Rehberi (BİGDR)'ni esas alarak gerçekleştirecekleri denetim faaliyetlerinde ihtiyaç duyulan iyileştirme önerileri sunulmuştur. Çalışma sonucunda ulaşılan ve sekiz başlıkta sayılan iyileştirilmesi gereken alanlarla ilgili getirilen çözüm önerilerinin, yapılacak denetimlerin etkililiğini ve etkinliğini artıracağı değerlendirilmektedir.

Anahtar Kelimeler: *Bilgi Güvenliği, Siber Güvenlik, Dijital Dönüşüm, İç Denetim, Bilgi ve İletişim Güvenliği Denetimi.*

Jel Kodlar: *K24, M42, M48*

[1] Dr., İç Denetçi, T.C. Ticaret Bakanlığı, hiozbilger@hotmail.com, ORCID: 0000-0002-9137-8855

[2] CIA, İç Denetçi, T.C. Ticaret Bakanlığı, bsariyar@hotmail.com, ORCID: 0000-0001-9656-1491

[3] CISA, İç Denetçi, T.C. Ticaret Bakanlığı, aerturk77@hotmail.com, ORCID: 0009-0009-2556-9360

IMPROVEMENT RECOMMENDATIONS FOR IMPLEMENTATION AND AUDITS OF THE INFORMATION AND COMMUNICATION SECURITY GUIDE

Abstract

Increasing digitalization with the effect of technological developments is rapidly changing life. This transformation brings risks along with opportunities. As a natural consequence of this, it is observed that cyber threats take their place among the top risks of institutions today. For example; data leakage, distributed denial of service (DDoS), phishing, structured query language (SQL) injection, malware and phishing (Phishing), spyware, adware and ransomware, as well as trojans (Trojans), worms (Worm), keyloggers, Malicious malware (Malware), which is described as boots, are some of these types of cyber threats that institutions may encounter. For this reason, as in all institutions and organizations, in the planning and redesign of the work and operation carried out in public administrations, it is necessary to take proactive action in order to take precautions against the existing or cyber security risks that may arise, and to reduce the impact that will arise in the event of the realization of these risks. became the key action in the period. In this study, firstly the theoretical framework was drawn on the subject, and then the based on the evaluation of the difficulties encountered in the field and the results of the implementation during the Guideline inspection carried out in 2022, The improvement needed in the audit activities to be carried out by the internal auditors, who are the primary auditors in the administrations that will implement the Information and Communication Security Guide (ICSG) published by the the Republic of Turkey Presidency Digital Transformation Office (DTO), based on the ICSG and the Information and Communication Security Audit Guide (ICSAG). recommendations are presented. In the study, it is evaluated that the solution proposals regarding the areas that need improvement listed in the eight titles will increase the effectiveness and efficiency of the audits to be made.

Keywords: *Information Security, Cyber Security, Digital Transformation Internal Audit, Information and Communication Security Audit.*

Jel Codes: *K24, M42, M48*

GİRİŞ

Günümüzde dijitalleşmenin etkisiyle iş ve işlemlerin planlanmasında, iş yapma şeklinde ve süreçlerin bilgi teknolojileri (BT) kullanımı ile yeniden tasarımında yaşanan dönüşüm; çalışma hayatında birçok kolaylık ve faydayı beraberinde getirse de kurum ve kuruluşların maruz kaldıkları risklerde de farklılaşmalara sebep olmaktadır. Bu değişim, risk haritalarında önlem alınması gereken BT ve(-ya) siber güvenlik risklerinin ilk sıralara yerleşmesi ile sonuçlanmaktadır. Bu durum yalnızca elektronik haberleşmede faaliyet gösteren kurum ve kuruluşlarda değil enerji, bankacılık vb. kritik hizmetleri sunan işletmelerde de görülmektedir. Nitekim risklerin gerçekleşmesi durumunda kurumların karşılaştıkları sonuçlar olarak tanımlanabilen kriz kavramı, geçmiş dönemlerde akla ilk gelen mali durumlarda yaşanılan çöküntü ya da bozukluklukların karşılığı iken bugün mali durumların yanında ve hatta öncesinde siber saldırılar, veri sızıntıları, iş sürekliliğinin temin edilememesi gibi bilgi güvenliğinin sağlanamamasıyla sonuçlanan BT kaynaklı krizlerin ifadesi olarak önemli konuma gelmiştir.

Etkileri tam olarak ölçülemediği ve anlaşılamadığı düşünülen, sosyo-ekonomik alandaki değişimleri de beraberinde getiren dijitalleşme ile birlikte yaşanan teknolojik gelişmeler, zamanda ve mekânda esneklik sağladığı gibi diğer taraftan yeni riskleri ve saldırı arayüzlerini de ortaya çıkarmıştır.

2025 yılına kadar dünya çapında yüz milyardan fazla bağlantı olacağı; yüzde 55'inin akıllı üretim ve akıllı şehirler gibi iş dünyasında, yüzde 45'inin nesnelerin interneti (IoT) ile araçların interneti (IoV) şeklinde gerçekleşeceği tahmin edilmektedir. Bağlantıların toplamda sadece yüzde 10'unun insanlar arasında, yüzde 90'ının ise eşya\şeyler *(things)* arasında gerçekleşeceği tahmin edilmektedir (Ping, 2016).

Bilgi sistemlerindeki muhtemel güvenlik durumlarının yeterince anlaşılamaması ve(ya) sağlanamaması sonucunda kötü niyetli kişilerce güvenlik önlemlerinin bertaraf edilmesiyle bilgi sistemlerinin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sekteye uğraması, özellikle kamu güvenliği açısından 21.yy'ın petrolü olarak nitelendirilen (Schwab vd., 2011; Taffel, 2021) verilerin korunmasını, kritik önemi haiz bir durum haline getirmiştir.

Kamu idarelerinde ortaya çıkabilecek veri sızıntısı, dağıtılmış hizmet reddi (*DDoS*), kimlik avı, yapılandırılmış sorgu dili (*SQL*) enjeksiyon, zararlı yazılım ve

oltalama (*Phishing*) olarak adlandırılan, her on bir saniyede bir gerçekleştiği tahmin edilen siber saldırılar (Morgan, 2019) ile kurumların bilişim sistemlerine zarar vermek amacıyla tasarlanmış casus, reklam ve fidye yazılımları ile truva atları (*Trojan*), solucanlar (*Worm*), tuş kaydediciler, botlar olarak nitelendirilen kötü amaçlı zararlı yazılımlar (*Malware*), kurumsal imajı derinden etkileyebileceği gibi ciddi veri kaybı ve mali kayıplara da neden olacaktır (Chu ve Holt, 2012, s. 33-34). Ülkelerin maruz kaldıkları zararlı yazılım saldırıları çeşitlilik göstermektedir. 2023 yılının ilk iki ayı ile ilgili istatistiklere göre dünya genelindeki kullanıcılar ortalama en çok (yüzde 9,2) fidye virüsüne (*Ransomware*), en az ise (yüzde 0,01) şifre kırıcı (*password hacking*) virüslere maruz kalırken, Türkiye'de ise en çok (yüzde 12) trojanlere, en az ise (yüzde 0,2) arka kapı (*backdoor*) virüslere maruz kalınmıştır. Öyle ki; her bir dakikada dünya çapında ekonomik etkisi 1.141.553 ($) olan 34.740 şifre, 1.902 IoT tabanlı, 1.095 DDoS, 7 oltalama, 18.295 zararlı yazılım saldırıları gerçekleşmektedir (Özkaya, 2023). Bu durum her ne kadar ülkelerin sosyo-ekonomik durumlarıyla açıklansa da söz konusu kötü amaçlı yazılım ve saldırılara maruz kalmamak için BT risklerini azaltmak amacıyla uluslararası bilgi güvenliği standartları ve ulusal yasal düzenlemelere uygun olarak gerekli önlemlerin alınması ve sistematik şekilde bağımsız denetim birimleri tarafından denetimlerin gerçekleştirilmesi siber güvenliğin en önemli gereksinimi haline gelmiştir.

Bu çalışmada, dijital dönüşümün doğal sonucu olarak bilginin ve bilgi güvenliğinin artan öneminden bahisle BT risklerini azaltabilmek amacıyla Türkiye örneğinde kamu kurum ve kuruluşları ile önemli altyapı hizmeti sağlayan işletmelerde uygulanmak amacıyla ulusal düzeyde usul ve esasların belirlendiği T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) tarafından yayımlanan "*Bilgi ve İletişim Güvenliği Rehberi (BİGR)" ve* Rehberin uygulama süreci ile tedbirlerin etkinlik durumunun değerlendirilmesi amacıyla gerçekleştirilecek denetim faaliyetlerinde kullanılacak "*Bilgi ve İletişim Güvenliği Denetim Rehberi (BİGDR)*"nin genel içeriği hakkında bilgi verilerek denetimlerin icra edileceği idarelerin kurum içi kaynaklarından olan İç Denetçi (*Internal Auditor*) perspektifiyle süreçte iyileştirilmesine ihtiyaç duyulan alanlar akademik bakış açısıyla ele alınmıştır.

Çalışmanın amacı, Bilgi ve İletişim Güvenliği Denetimi kapsamında kamu idarelerince gerçekleştirilen denetimlerde karşılaşılan sorunları tespit etmek ve bu sorunlarla ilgili iyileştirme önerileri sunmak olarak belirlenmiştir. Bu kap-

samda çalışmanın birinci bölümünde öncelikle dijital döşümde iç denetime ilişkin çalışmalar yer almaktadır. İkinci bölümde günümüz dünyasında etki ve sonuçları açısından oldukça önemli olan dijital dönüşüm ve bilginin artan önemi ele alınmıştır. Çalışmanın üçüncü ve dördüncü bölümlerinde birbirleriyle bağlantılı olarak sırasıyla bilgi ve iletişim güvenliği ve denetimi rehberleri ile rehber denetiminde iyileştirilmesi gereken alanlar ve çözüm önerileri çalışmanın dördüncü bölümünde açıklanan araştırma yöntemi çerçevesinde farklı açılardan değerlendirilmektedir.

1. DİJİTAL DÖNÜŞÜMDE İÇ DENETİME İLİŞKİN ÇALIŞMALAR

Uluslararası meslek standartları ile etik kuralları ve metodolojisi olan İç Denetimin, AB uyum yasaları çerçevesinde, Türk kamu yönetiminde ilk defa Türkiye Cumhuriyet Merkez Bankası'nda, 2002 yılında uygulamaya geçmesinden itibaren, gerek akademinin gerekse de konunun uygulayıcısı ve uzmanları tarafından sıklıkla ele alınan konulardan biri olduğu görülmektedir.

Tarihsel kökeni her ne kadar 13. yüzyıla kadar dayandırılsa da modern anlamda 1900'lü yılların başlarında Kıta Avrupası ülkelerinde ilk olarak uygulanan iç denetim (Kızılboğa, 2013, s. 108), 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunun'da; kamu idarelerinin çalışmalarını geliştirmek ve onlara değer katmak için etkililik, ekonomiklik ve verimlilik esaslarına göre kaynakların yönetilip yönetilmediğini belirlemek ve idari kademelere rehberlik yapmak amacıyla gerçekleştirilen nesnel güvence sağlama ve danışmanlık faaliyeti şeklinde ifade edilmektedir. Klasik denetim yöntemlerini kapsamakla birlikte rehberlik fonksiyonu kapsamında ileriye dönük faaliyetlerle ilgili alınması gereken iyileştirici aksiyonları da belirleyen, dinamik bir denetim sistemi olarak nitelendirilen (Bilge ve Kiracı, 2010; Stewart ve Subramaniam, 2010, s. 334) iç denetim sistemi, çalışmanın konusu çerçevesinde literatürde farklı yönleriyle ele alınmıştır.

Appelbaum ve Nehmer (2017) tarafından gerçekleştirilen çalışmada dijital dönüşüm çağında kurumların iç ve dış denetimlerinin tasarlanması ve uygulanması için bir çerçeve ortaya konulmaktadır. Çalışma, dijital dönüşüm araçlarının kanıt toplama yetenekleri aracılığıyla bazı işlevlerde denetim sırasında denetçiler tarafından değerlendirilen belirli iddiaları desteklemek için denetimlerde nasıl yararlanılacağını göstermektedir. Dijital dönüşüm araçlarının bazı durumlarda

varlık ve değerleme iddiaları hakkında kanıt sağlayabileceklerine vurgu yapılarak, dijital dönüşüm ve güvenliğinde denetim elemanlarının önemine vurgu yapılmıştır.

Barrigon'a göre (2020), teknolojik gelişmelere ayak uydurma ihtiyacının, iç denetim mesleğinin bir gereği olduğu, dijital dönüşümde sadece karşı karşıya kalınan risklerin değil aynı zamanda bunları azaltmak için uygulanan kontrollerin de daha iyi değerlendirilmesi gerektiği, siber güvenliğin test edilmesinde iç denetçilerin veri analitiği, yapay zeka ve blockchain (blok zincir) teknolojilerindeki riskli alanlara eğilirken hangi tür eylemleri gerçekleştirmesi gerektiği tablo halinde sunulmuştur.

Lois vd.'nin (2020), dijital çağda iç denetimi etkileyen çağdaş faktörleri ve bunun uygulanması için kullanılabilecek teknikleri araştırdığı ve 105 çalışan ile gerçekleştirdiği çalışmada elde ettikleri bulgulara göre; etkin bir dijital denetim sisteminin kurulması için teknolojik gelişmelerin vazgeçilmez olduğu, siber saldırılara karşı veri koruma önlemlerinin yanı sıra çalışanların becerileri ve eğitimlerinin etkisinin önemli bulunduğu, siber güvenliğin sağlanıp sağlanmadığının test edilmesi için sanal iç denetim ekiplerinin hazırlanmasına ve oluşturulmasına özel önem verilmesi gerektiği sonucuna varılmıştır.

Gupta ise (2020), iç denetçilerin dijital dönüşüm sürecindeki önemi ve karşılaştıkları zorlukları ortaya koymuştur. Bu kapsamda iç denetçilerin siber ortamdaki muhtemel riskleri belirlemede ve değişen çevrede denetim faliyetlerinin nasıl gerçekleştirileceği değerlendirilmiştir. Bu çalışmada denetçinin teknoloji odaklı süreçlere daha fazla ilgi göstermesi gerektiği önerilmiş, denetimin dijitalleşme süreci yani BT denetimi, dijital denetim ve siber denetim için BT desteği söz konusu çalışmada; grafik halinde sunulmuştur.

Pizzi vd.'nin çalışmasında (2021), "Endüstri 4.0" ile hızlanan dijital dönüşümün çalışma hayatındaki ve iç denetim mesleğiyle ilgili dört farklı araştırma alanındaki (teknolojik yenilik, sürekli denetim, veri analitiği ve suistimal tespiti) etkisi sorgulanarak araştırma sonuçları değerlendirilmiştir.

Otia ve Bracci (2022), yaşanılan dijital dönüşümün kurumların paydaşları ile ilgili talep ve beklentilerinde ne yönde değişikliklere neden olduğunu incelemiştir. Üç yüzden fazla katılımcı ile gerçekleştirilen araştırma sonuçları tablo halinde sunulmuştur. Elde edilen bulgularda teknolojik gelişmelerin tetiklediği hesap ve-

rebilirlik ve şeffaflık için artan denetim talebinin denetimin yapılma biçiminde bir etkiye sahip olduğu tespit edilmiştir.

BİGR'nin gündeme gelmesi ve gerekli denetimlerin başlamasıyla bahse konu uygulayıcıların olduğu kadar akademinin de ilgisini çekmeye başlamış, Rehber hakkındaki ulusal literatürdeki çalışmalar da aynı ölçüde hız kazanmıştır.

Ağdeniz (2021), yaptığı çalışmada DDO tarafından çıkarılan BİGR denetiminde kamu iç denetçilerinin rolü ve yetkinliklerini sertifika ve denetim sayıları temelinde değerlendirmeye çalışarak yılda en az bir kez kamu iç denetçilerinin söz konusu Rehber kapsamında denetim yapma zorunluluğunu belirtmiş, Kamu İç Denetim Genel Raporlarının içerik analizini de yaparak iç denetimin mevcut durumunu *açıklamıştır.*

Meral ve Bülbül (2022), örneklem yöntemiyle belirlenen kamu kurumlarında farklı alanlarda görev yapan çalışanlara yönelik gerçekleştirdikleri araştırmayla kurumların sahip olduğu verilerin önem düzeyi yükseldikçe buna benzer şekilde bilgi güvenliği politikalarının da arttığını; ancak kamu kurumlarının bilgi güvenliği politikalarının etkinliği konusunda genel olarak yetersiz olduğunu ortaya koymuştur.

Özen ve Gürel (2022), fiziksel varlıkların programlama dilleri yoluyla yansımalarının oluşturulması şeklinde ifade edilebilen "*Dijital İkiz Yöntemi*"ne açıklık getirerek bu yöntemin modern kamu denetimlerinde yararlanılmasını ve denetim kalitesine katkısını ortaya koymuştur.

Karagöz (2022), BİGR'nin uygulanması yöntemini ve uygulamayla ilgili oluşturulması gereken denetim mekanizmalarını belirterek, denetimde bağlı kalınması gereken etik ilkelere vurgu yapmıştır.

Çalışma konusu hakkında yapılan başka bir akademik çalışma da Tulgar vd. (2022) tarafından yapılmıştır. Çalışmayla uluslararası bilgi güvenliği standartları izah edilerek, Rehber uygulama süreçlerindeki her bir adım ile ilgili açıklamalarda bulunulmuş ve Rehber'deki temel başlıklardan birisi olan Nesnelerin İnterneti (IoT) Güvenliği ile ilgili örnek bir uygulama örneği ortaya konulmuştur.

Arslan ve Özbilger (2022), ulusal mevzuat altyapısı ve düzenlemelerine göre kamu yönetimindeki bilgi işlem birimlerinin iç denetiminde örnek bir kontrol modeli açıklamıştır.

Selimoğlu ve Saldı (2022) tarafından yapılan çalışmada, Bilgi ve İletişim Güvenliği Rehberi ve Rehber denetimini doğrudan ele almasa da esas olarak siber güvenlikle ilgili olaylarda blok zincir teknolojisinden nasıl yararlanılacağı ve iç denetçilerin bu teknolojiye uyum sağlamaları için ne yapmaları gerektiği hakkında bir takım öneriler ortaya konulmuştur.

Çalışma konusuna ilişkin ulusal ve uluslararası literatürde daha önce yapılan akademik çalışmaların değerlendirilmesi sonucunda, dijitalleşmenin ve bilgi güvenliğinin sağlanması ve denetlenmesindeki önemin fark edilmesiyle uluslararası literatürdeki çalışmaların özellikle son yıllarda önemli ölçüde arttığı ve konunun yoğun olarak işlendiği; ancak Türkiye'deki literatürün sınırlı olduğu anlaşılmaktadır. Konunun güncel olması ve literatür çalışmalarının sınırlı olması nedenleriyle bu çalışmayla BİGR ve denetimi hakkında literatürde uygulamaya yönelik önemli bir açığın giderilmesine katkıda bulunulacağı ve yapılacak yeni teknik çalışmalar için yol göstermesi hedeflenmiştir.

2. DİJİTAL DÖNÜŞÜM VE BİLGİNİN ARTAN ÖNEMİ

Günlük hayatı kolaylaştıran, yapılacak işler için harcanması gereken zamanı önemli ölçüde azaltan, iş modellerini değiştirmek için teknolojiden faydalanılması süreci olarak nitelendirilen (Otia ve Bracci, 2022, s. 255) dijitalleşme ile birlikte, yeni riskler ve saldırı arayüzleri ortaya çıkmıştır. Örneğin günümüzde bir bankayı soymak için fiziksel olarak bankada bulunma gereksinimi ortadan kalkmış, internet üzerinden online olarak bankaların bilişim sistemlerine uzaktan erişip hedeflenen kötücül/zararlı işlemler yapılabilmektedir (Özkaya, 2018, s. 114). Bankacılık sektöründe dijitalleşmenin etkisiyle karşımıza çıkan risklerdeki değişikliğin yanısıra pandemi sürecinin de etkisiyle ivmelenen dijital dönüşüm ile birlikte uzaktan çalışma kamu kurumlarının dahi olağan işleyişi haline gelmiş, diğer taraftan büyük veri ve yapay zeka uygulamaları gibi yeni teknolojilerin kullanımı da artmıştır. Dijital dönüşüm ile birlikte eksponansiyel olarak artan hacimdeki bilgiye erişim kolaylaşırken, bilginin diğer iki unsuru olan gizlilik ve bütünlüğünün korunması giderek güçleşmeye başladığından, günümüzün en değerli madeni olarak nitelenebilecek bilginin güvenliği, dijital çağın en önemli gereksinim olgusu olarak literatüre girmiştir.

Bilginin depolanması ve korunması mevcut durumdaki en büyük zorluklar-

dan biri haline gelmiştir. Dijital dönüşüm ile ilgili olarak iş yaşamında sıklıkla karşılaşılan, bilgi güvenliği disiplininde oldukça önemli bir rol oynayan, çeşitli disiplinler aracılığıyla ifade edilen ve gelinen noktada ulusal güvenlik ile yakinen ilişkilendirilen siber güvenlik; elektronik ortamda gerçekleştirilen işlemler esnasında varlıkların, kullanıcıların bilgi güvenliği farkındalık eksikliğinden kaynaklanan kusurlardan, kötü niyetli kişilerin veya organizasyonların illegal eylemlerinden kaynaklanan saldırılar sonucunda zarar görmesinin önüne geçmek amacıyla alınan önlemler/tedbirler olarak tanımlanabilmektedir (Kavitha ve Preetha, 2019, s. 4).

Günümüzde kurumlar, her türlü bilgi varlıklarına siber ortamda bulunan güvenlik risklerine karşı önlem almayı ve bu durumun sürdürülmesini amaçlamaktadır. Gelişmiş güvenlik teknolojisi kullanımlarının artması sonucu, olası teknik siber saldırıların gerçekleşmesine ilişkin risk azalabilmektedir (Aloul, 2012, s. 181). Siber güvenlik risklerinin azaltılması ihtiyacı, ülkelerin uluslararası standartlar ve iyi uygulamalardan faydalanarak bilgi güvenliği alanında uygun yasal mevzuat hazırlanmasını ve uygulanması gereken tedbirlerin belirlenmesini tetiklemiştir (Sağıroğlu ve Şenol, 2018). Bu gelişmeler, dijital dönüşümü yalnızca yeni teknolojileri devreye almak olarak algılamaktan ziyade bu dönüşümün, kurumsal yeniden yapılanma modeli olarak, yeni yönetim ve denetim yapısının tasarlaması şeklinde düşünülmesi ihtiyacını zorunlu kılmıştır.

Ülkeleri dijital dönüşüme yönlendiren ve e-Devlet uygulamalarının artmasının ana nedenlerinin başında, vatandaşların bulundukları lokasyonları değiştirmeden hizmetlere ulaşmalarına imkân sağlaması ve dezavantajlı grupların kamu hizmetlerinden faydalanmaları konusunda önemli faydalar içermesi yer almaktadır. Ayrıca sosyoekonomik yapıya etki eden COVID-19 gibi krizler de özel sektör kuruluşlarında olduğu kadar devletleri de hizmet sunumunda dijital dönüşüme zorlamıştır. Diğer taraftan internet ara bağlantılarının çoğalması genellikle kamu kurumları ve vatandaşlar için en tehlikeli bir savaş uçağından, tanktan, toptan daha tehlikeli, yıkıcı ve ciddi sonuçlar doğuran siber saldırı olaylarında da önemli bir artışa yol açmıştır. Öyle ki, OECD'nin "21. yy'da Ortaya Çıkan Sistematik Riskler (Emerging Systemic Risks in the 21st Century)" başlıklı yayımladığı rapora göre; siber riskler doğal afetler, bulaşıcı hastalıklar, gıda güvenliğiyle birlikte geleceğin en yüksek riskli alanları arasında sayılmıştır (OECD, 2003).

Dijitalleşmenin getirdiği avantajlardan faydalanabilmek adına 2000'li yılların başında e-Devlet dönüşümünü hızlı bir şekilde hayata geçiren Estonya, vatandaşlarına sunduğu hizmetlerinin büyük bir kısmını online platformlara taşımıştır. İlk başta oldukça güzel ve beklenildiği gibi hizmet veren bu sistem, gerekli siber güvenlik önlemlerinin alınmaması sonucunda bilişim altyapısına yapılan hizmet dışı bırakma (DoS) saldırılarıyla hizmet veremez hale gelmiştir (Bıçakçı, 2013, s. 29). E-devlet uygulamalarına yapılan bu saldırı ile Estonya'da kamuya sunulan hizmetlere erişilememiş, hizmetlerin büyük kısmının online platformlara taşınması nedeniyle de kamu hizmetleri durma noktasına gelmiştir. Estonya özelinde yaşanan bu e-dönüşüm sürecinden elde edilen deneyimlerle tüm dünyada dijital dönüşüme yönelik yapılan çalışmalar sonucunda gerekli stratejik yol haritaları belirlenmiştir (Darıcılı, 2014, s. 7). Aynı dönemde, "*Endüstri 4.0*" ve son gelinen nokta da dijitalleşmenin en üst seviyede olduğu "*Süper Akıllı Toplum*" ya da başka bir deyişle "*Toplum 5.0*" kavramları ile birlikte görünülürlüğü ve bilinirliği artan, etkileşim içindeki bireyleri ve kurumları etkileyen, entegre bir oluşum olan (Potii, 2018) siber güvenlikle ilgili ulusal yazılım ve bilişim altyapı yatırımlara öncelik veren Estonya bugün gelinen noktada Global Siber Güvenlik Endeksi (The *Global Cybersecurity Index*-ITU)'ne göre, dünyada birinci Amerika Birleşik Devleti, ikinci İngiltere ve Suudi Arabistan'dan sonra üçüncü, Avrupa'da ise ikinci sırada yer almaktadır (ITU, 2021).

Kurumların dijital altyapıya daha fazla bağımlı olması onları siber suçlara karşı daha savunmasız hale getirmiştir (Verma ve Charu, 2022). Bu nedenle, siber uzay ülkelerin fiziksel sınırları kadar korunmaya muhtaç bir alana evrilmiştir. Bu konuda İran, Çin, ABD gibi bir çok ülke tarafından gayriresmi bilgisayar korsanı (*hacker*) ekipleri oluşturulmaktadır. Bu ekipler hem kendi siber sınırlarını korumayı hem de düşman olarak belirledikleri ülkelere siber zarar verme, gizli bilgileri çalma gibi faaliyetler göstermektedir. Bu konuda Kuzey Kore'deki Lazarus (APT38) olarak adlandırılan hacker grubunun gerçekleştirdiği faaliyetler, konu hakkında örnek olarak gösterilebilmektedir (Page, 2012).

Yakın geçmişte farklı ülkelerde bilgisayar korsanlarının gerçekleştirdiği çok sayıda siber saldırı yaşanmıştır. Son yıllarda, görülen belki de en büyük, en karmaşık ve de en şiddetli olduğu düşünülen siber saldırılardan yüze yakın ülkedeki kamu ve özel kuruluşlardaki Microsoft Windows kullanıcılarını hedef alan WannaCry virüs olayı (Savita ve Patil, 2017, s. 1939), ABD'deki en büyük finansal ku-

rumlardan biri olan Capital One'da 2019 yılında yaşanan, yüz milyondan fazla kişiyi etkileyen veri ihlali (Nelson vd., 2020), yaklaşık yüz elli milyon kişinin sağlık ve sosyal güvenlik ile ilgili kişisel verilerinin ifşa edildiği Equifax veri ihlali (Lambet, 2017, s. 33) ve 87 milyon Facebook kullanıcısının kişisel bilgilerinin ABD'deki seçim kampanyalarında izinsiz şekilde kullanıldığı "Facebook-Cambridge Analytica Scandal" olarak da bilinen veri skandalı olayında kullanıcıların kişisel facebook sayfalarında yer alan bilgiler izinli ve/veya izinsiz elde edilerek ilgili kişilerin profillerini çıkarmada ve konum bilgilerini elde etmede kullanılmış, bu bilgilerden faydalanılarak belirli bir kişinin siyasi olaylar karşısında verecekleri tepkileri değiştirmek amacıyla ne tür reklamların kullanılabileceğini öneren profiller oluşturmada kullanılması amacıyla üçüncü kişilere satılmıştır (BBC, 2018).

Ülkeler yukarıda birkaç örneği verilen veri ihlallerinin bir daha yaşanmaması için sadece bilgi güvenliği önlemleri almamakta ayrıca vatandaşlarının kullandıkları uygulamalar üzerinden verilerinin izinli veya izinsiz olarak başka ülkelerin istihbarat teşkilatları tarafından kullanılmalarını önlemek amacıyla da çeşitli düzenlemeler yapmaktadır. Bunun son örneği, ABD'nin Pekin merkezli ByteDance Ltd. tarafından geliştirilen Tik-Tok uygulamasındaki kişisel verilerin, Çin hükümetinin kullanımı amacıyla toplandığı gerekçesi ve ulusal güvenlik endişeleri nedeniyle merkezi hükümet çalışanlarının kuruma ait cihazlarına TikTok indirmesini yasaklayan tasarıyı kabul etmesidir (Shepardson, 2023). Yine benzer şekilde vatandaşlarının veri güvenliğini sağlamak amacıyla Çin menşeili bilgi ve iletişim güvenliği cihazları üreten Huawei firmasının ürünlerinin ABD ve Kanada hükümetleri tarafından ithaline ve satışına yasak getirilmesi (Bartz ve Alper, 2022), bu kapsamda yapılmış başka bir düzenleme olarak görülmektedir.

"Her Tehdit Olası Riskleri Belirlemekle Başlar" anlayışı doğrultusunda BT alanındaki risklerin ve olası etkilerinin detaylı bir çalışmayla belirlenmesi ve buna uygun tedbirlerin uygulamaya konulması gerektiği dersinden hareketle siber güvenlik risklerine yönelik aksiyonların alınması için bilimsel temelli yaklaşımların geliştirilmeye başlandığı görülmektedir. Dünyada bu konuda çalışan ulusal ve uluslararası kuruluşlardan bazıları aşağıda sıralanmıştır.

- Kanada için siber güvenlik konusunda uzman tavsiyesi, rehberlik, hizmet ve destek sağlayan Kanada Siber Güvenlik Merkezi (*The Canadian Centre for Cyber Security - CCCS*)

- Avrupa Birliği bünyesinde siber güvenlik alanında BT ürünlerinin, hizmetlerinin ve süreçlerinin güvenilirliğini artıran üye devletler ve kurumlarıyla işbirliği yapan Avrupa Birliği Siber Güvenlik Ajansı (*The European Union Agency for Cybersecurity - ENISA*)
- Amerika Birleşik Devletleri'nde siber güvenlik konusunda Siber Güvenlik ve Altyapı Güvenliği Ajansı (*Cybersecurity and Infrastructure Security Agency - CISA*)
- NATO bünyesinde kurulan NATO İletişim ve Bilgi Ajansı (*NATO Communications and Information Agency - NCIA*) buna yönelik çalışan dünya çapındaki örnekler olarak karşımıza çıkmaktadır.

Genel olarak bu organizasyonlar tarafından BT ve siber güvenlik alanında rehber, denetim programları, iyi uygulama örnekleri, araçlar, kontrol listeleri hazırlanmıştır. Örneğin Kanada Siber Güvenlik Merkezi'nin hazırladığı *Siber Güvenlik Denetim Programı*[1], AB üye ülkelerin bilgi güvenliğinden sorumlu *Avrupa Ağ ve Bilgi Güvenliği Ajansı*'nın hazırladığı araçların[2], ABD Savunma Bakanlığı tarafından hazırlanan *teknik uygulama klavuzları*[3]nın çeşitli kurum ve kuruluşların kullanımına sunulduğu görülmektedir.

Siber güvenlik ekosistemi hakkında son yıllarda birçok ülke örneklerinde olduğu gibi Türkiye'de de gerek mevzuat altyapının düzenlenmesi gerekse de teorik ve uygulama çerçevesinde önemli adımlar atılmıştır (Sağıroğlu ve Şenol, 2018). Bu konudaki ilk önemli ve somut adım, 2003 yılından itibaren *e-D*önüşüm Türkiye Projesi kapsamında gerçekleşmiş, iki kısa vadeli eylem planı hazırlanmıştır. İhtiyaç duyulan altyapının oluşturulması amacıyla Devlet Planlama Teşkilatı (mülga) tarafından hazırlanan *Uzun Vadeli Gelişmenin Temel Amaçları ve Stratejisi (2001-2023)*'yle Türkiye'de bilgi toplumu ile ilgili hedeflenen dönüşüme ulaşılması planlanmıştır. (DPT, 2000: 21) Kalkınma Planlarında da göze çarpan bu dönüşüm vizyonu ile DPT tarafından *Bilgi Toplumu Stratejisi (2006-2010)* ve Kalkınma Bakanlığı (mülga) tarafından *2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı* ve *Ulusal Siber Güvenlik Stratejisi ve Eylem Planları* hazırlanmıştır.

Yapılan çalışmalar, sadece mevzuat ve düzenlemelerin hazırlanmasıyla kalmamış gerekli kurumsal organizasyonel oluşumların kurulmasını da sağ-

1 Siber güvenlik denetim programı için bkz: https://www.cyber.gc.ca/en/government-institutions
2 Hazırlanan denetim araçları için bkz: https://www.enisa.europa.eu/tools
3 Teknik uygulama klavuzları için bkz: https://public.cyber.mil/stigs

lamıştır. 2000'li yılların başından itibaren Türkiye'de siber güvenlik hakkında çalışmalar yapmak ve bu kapsamda ihtiyaç duyulan eğitim ve insan kaynağı ihtiyacını karşılamak amacıyla *KamuNet Teknik Kurulu*, 2002 yılında yeniden organizasyonu ve göreve başlamasından itibaren ilgili kamu kurumları siber suçlarla mücadeleye ilişkin bilgi toplumuyla ilgili hedef, politika ve stratejiler çerçevesinde, *Siber Güvenlik Enstitüsü (SGE)*, Türk Silahlı Kuvvetleri (TSK) Siber Savunma Merkezi Başkanlığı, siber güvenlik alanında dünya genelinde yapılan kurumsal yapılar örnek alınarak, *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı* uyarınca Bilgi Teknolojileri ve İletişim Kurumu bünyesinde *Ulusal Siber Olaylara Müdahale Merkezi (USOM)* ve müstakil bir bilgi işlem alt yapısına sahip kurumlarda yer alan *Siber Olaylara Müdahale Ekipleri (SOME)* kurulmuştur. Tüm bunların kurulması organizasyonel gelişmelerdendir.

Yaşanan teknolojik gelişmeler, yapılan kamusal reformlar çerçevesinde farklı kamu kurumlarınca geçmiş dönemlerde Başbakanlık, Kalkınma Bakanlığı ile Ulaştırma ve Altyapı Bakanlığı ve ilgili diğer kamu kurum ve kuruluşlarınca ayrı ayrı sürdürülen siber güvenlik, dijital dönüşüm (e-Devlet) vb. çalışmalarının tek çatı altında yürütülmesi amacıyla, 24 Ekim 2019 tarihli ve 30928 sayılı Resmi Gazete'de yayımlanan 48 sayılı Cumhurbaşkanlığı Kararnamesi kapsamında, T.C. Cumhurbaşkanlığı DDO kurulmuştur. Ofisin ulusal siber güvenliğin temin edilmesi amacıyla hazırladığı ve kamu kurum, kuruluş ile kritik altyapı[4] özelliğinde hizmet sağlayan işletmelerde uygulanması zorunlu olan, ilgili tarafların görüşleri alınarak oluşturulan 27 Temmuz 2020 tarihinde yayımlanan "*Bilgi ve İletişim Güvenliği Rehberi*" ve 10 Ekim 2021 tarihinde yayımlanan "*Bilgi ve İletişim Güvenliği Denetim Rehberi*" Türkiye'de siber güvenlik hakkında atılan önemli adımlar olmuştur.

DDO'nun kurulmasının, siber güvenlik alanında yapılacak çalışmaların üst düzeyde tek elden koordineyi sağlamasının yanı sıra bilgi ve siber güvenlik hakkında atılacak adımların kuvvetli şekilde en üst düzeyde desteklendiğinin göstergesi olarak da kıymetli olduğu değerlendirilmektedir. E-Devlet dönüşümü kapsamında yapılan çalışmalarda Estonya'nın yaşadığı saldırılardan dersler çıkarılmış, kamu kurum ve kuruluşlarının birbirleri ile yapacakları

4 Kritik altyapılar; enerji üretim ve dağıtım, su ve kanalizasyon sistemleri, telekomünikasyon altyapısı ile sağlık, finansal, güvenlik ve ulaştırma servisleri (Ak, 2019, s. 42).

bağlantılarda/veri transferinde internete açık olmayan kapalı bir ağ sistemi üzerinden haberleşmelerini zorunlu tutan, ilk olarak 2000'li yılların başlarında başlatılan "*KamuNet Projesi*[5]"nin hayata geçirilmesini sağlamıştır. Öte yandan kamu kurum ve kuruluşlarının KamuNet'i kullanmalarının teşvik edilmesi ve hangi düzeyde/oranda KamuNet'i kullandıklarının belirlenmesi amacıyla BİGR tedbir maddeleri içerisinde bu durumun ölçülebilmesi amacına yönelik düzenlemelere yer verilmesinin sürece katkı sağlayacağı değerlendirilmektedir.

DDO tarafından daha önce Türkiye'de bu konuda yürütülen strateji ve eylem planı çalışmalarının devamı niteliğindeki dijitalleşme yol haritasını belirlemek amacıyla Dijital Devlet Stratejisinin hazırlık çalışmaları kapsamında *OECD* ile ortak çalışma halinde çeşitli faaliyetler yürütülmektedir (DDO, 2023). Ayrıca 20 Ağustos 2021 tarihinde DDO ile Sanayi ve Teknoloji Bakanlığı işbirliği sonucunda yayımlanan *Ulusal Yapay Zeka Stratejisi (2021-2025)* doğrultusunda Kamu Bulut Bilişim Stratejisi'nin hazırlık faaliyetleri sürdürülmektedir. Bu çalışmalar kapsamında DDO tarafından *Kamu Bulut Bilişim Stratejileri Ülke İncelemeleri Raporu* ve *Mevcut Durum Analiz Raporları* tamamlanmış ve kamuoyu ile paylaşılmıştır.

Türkiye'de dijitalleşme yönünde son dönemde atılan adımlar ve gerçekleştirilen çalışmaların bir sonucu olarak *On İkinci Kalkınma Planı (2024-2028)* Özel İhtisas Komisyonları *ve Çalışma Grupları El Kitabı*'nda "*Bilgi ve İletişim Teknoloji*"leri ayrı bir özel ihtisas komisyonu kurulmuş ve dijitalleşme ile ilgili olduğu değerlendirilen "*e-Devlet Hizmetlerinin Geliştirilmesi*", "*Dijitalleşme ve Vergileme*", "*Dijital Gelişmelerin Sosyoekonomik Etkileri*" adlarında üç ayrı çalışma grubu oluşturulmuştur. 2023 Yılı Cumhurbaşkanlığı Yıllık Programı'nda "*Dijital Türkiye*" vizyonu ve "*Milli Teknoloji Hamlesi*"ne yönelik hedeflerin belirlenmesi de dijitalleşmenin ülke içerisinde dikkate alındığını ve bu konuda çeşitli önlemlerin belirlendiğini gösteren diğer düzenlemelerdendir.

ITU'ya göre dünyada on birinci, Avrupa'da altıncı sırada yer alan Türkiye'nin geldiği noktayı geliştirip en üst sıraları hedeflemesi gerekmektedir. Bu amaçla, Estonya örneğinde olduğu gibi yerli, milli ve hatta global siber yazılımlarla ilgili AR-GE çalışmalarının desteklenmesinin yanında ulusal mevzuat ve denetim

5 KamuNet Projesi için bkz: https://cbddo.gov.tr/projeler/kamu-net/

süreçleri ile ilgili altyapıların da hazır olması gereklidir. Bu süreçte devlet, özel sektör ve sivil toplum kuruluşlarıyla beraber uygun yapının oluşturulması önemlidir.

3. BİLGİ VE İLETİŞİM GÜVENLİĞİ VE DENETİMİ REHBERLERİ

2019/12 sayılı "*Bilgi ve İletişim Güvenliği Tedbirleri*" konulu Cumhurbaşkanlığı Genelgesi ile bilgi ve iletişim güvenliğine ilişkin temel prensipler ve yol haritası belirlenmiştir. Bahse konu Genelge ve Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ile uyumlu biçimde kamu kurum ve kuruluşları ile kritik altyapı hizmeti sağlayan kurumların uyması zorunlu kılınan, bilgi ve iletişim güvenliğinin sağlanması amacıyla DDO koordinesinde bilişim alanında tüm dünyada geçerli standartlar, iyi uygulamalar, rehberler incelenerek hazırlananan "*Bilgi ve İletişim Güvenliği Rehberi*", 27 Temmuz 2020 tarihinde yayımlanarak yürürlüğe girmiştir.

Bilişim alanında belirlenen tüm tedbirlerin nihai hedefi bilgi güvenliğinin sağlanmasıdır. Bilgi güvenliğinden bahsedebilmek için bilginin üç temel unsuru olan gizliliğin (bilgiye sadece yetkili kişilerin erişimi), bütünlüğün (bilginin sadece yetkili kişiler tarafından değiştirilmesi) ve erişilebilirliğin (bilginin yetkili kişilerin talebi halinde kullanılabilir olması) sağlanması gerekmektedir. Rehbere uyum ile bilginin bu üç unsurunun korunması hedeflenmektedir. Rehberin hazırlanmasında temel amaç, rehbere uymakla zorunlu tüm kurumlarda siber güvenlik ve bilgi güvenliği alanında yapılacak çalışmaların belirli bir çerçeve dâhilinde yürütülmesine ve bu tedbirlere uyum konusunda yapılacak denetimlerin aynı bakış açısıyla yapılmasına olanak sağlanmasıdır.

Bilgi güvenliğinde Türkiye nezdinde hazırlanmış, içerisinde teknik tedbirleri bulunduran referans doküman niteliğindeki BİGR'nin, ihtiyaç halinde yaşayan bir doküman olarak değişiklik yönetimi kurgusu içerisinde güncellenmesi ve geliştirilmesi ile sürekliliğinin sağlanması önemlidir.

Bilgi ve iletişim güvenliğine yönelik belirlenen tedbirlerin uygulamaya geçirilmesi ile ülke nezdinde siber güvenlik alanında dayanıklılığın ve iş sürekliliğinin artırılması hedeflenen BİGR ile 24 aylık uyum ve(ya) geçiş süreci ve alınacak tedbirlere yönelik aksiyonlar oluşturulmuştur. Rehbere uyum sağlamakla sorumlu tutulan kurum ve kuruluşların; bilgi varlıklarını gruplandırmaları, bu grupların kritiklik seviyelerini ve bu seviyelere yönelik BİGR tablolar bölümünde belirle-

nen tedbirlere ilişkin uygulanma durumlarını veya eksikliklerini ve yapılacak çalışmaları belirleyerek dokümante etmelerinin yanısıra, belirlenen takvimin 6-24 aylık bölümünde mevcut bilgi sistemlerini kritiklik derecelerine uygun tedbirler ile uyumlu hale getirmesi, yeni kurulacak bilgi sistemlerinde ise BİGR'de yer verilen tedbirlere uyulması gerekmektedir.

Rehberin ilgili bölümlerinde uyum süreci aşağıdaki şekilde tanımlanmaktadır;

- Bilgi sistemleri, personel ve fiziksel mekanlar dâhil kurumun tüm bilgi varlıklarının gruplandırılması diğer bir deyişle varlık gruplarının tanımlanması.
- Bu grupların her birine ilişkin olarak varlık sahipleri ve ilgili bilgi işlem personeline (sistem yöneticisi, yazılım personeli vb.) uygulanacak anket ile belirlenecek puanların karşılığı olacak biçimde varlık grubu kritiklik seviyelerinin belirlenmesi.
- Rehberde belirlenen kritiklik seviyelerine uygun Rehber ekinde yer alan toplam 661 adet tedbirlere yönelik varlık grupları bazında mevcut durum ve boşluk analiz çalışmalarının yapılarak ihtiyaçların ve gerçekleştirilecek faaliyetlerin belirlenmesi.
- Uyum sürecine ilişkin gerçekleştirilecek faaliyetlerin belirlenerek yol haritasının oluşturulması.
- Kritiklik derecesine (1., 2. ve 3. seviye) uygun olarak tedbirlerin gerçekleştirilmesi.
- Çalışmaların BİGR eklerinde belirlenen formatlarda dokümante edilmesi.

Yılda en az bir kez denetlenmesi ve sonuçların DDO'ya bildirilmesi gereken BİGR, bilişim sistemlerinde kullanılan güvenlik yazılımlarında olması gereken veya parametrelerde ayarlanması gereken değerleri vurgulaması açısından (örneğin bilişim sistemlerinde kullanılan antivirüs yazılımlarında otomatik kod çalıştırma (autorun) korumasının açılmasının zorunlu tutulması), diğer Bilgi Güvenliği Yönetim Sistemlerinden (BGYS) ayrılmaktadır. Ayrıca Rehber, varlıkların gruplandırılması ve kritiklik derecelerine göre uygulanacak tedbirlerin belirlenmesi ile de BGYS risk değerlendirme sürecinden farklılaşmaktadır.

Rehbere uyum sürecinde, tüm kurumu ilgilendiren bilgi varlıklarının gruplan-

dırılması ve kritiklik derecelendirme çalışmalarının koordinesi ile sonuçlandırılması ve dokümantasyonun oluşturulmasında zorluk yaşanabildiği görülmüştür. İlaveten tüm dünyada etkileri hissedilen COVID-19 krizi, Rehbere uyum sürecini olumsuz yönde etkilemiş ve kurumlarda yapılması gereken faaliyetlerin zamanında gerçekleştirilememesine neden olmuştur.

Uyum sürecinin tamamlanmasını müteakip 2022 yılının ikinci yarısında ilk denetimler gerçekleştirilmeye başlanmıştır. Bahse konu denetimlere ilişkin usul ve esaslar ile denetim metodolojisi Ekim 2021' de DDO tarafından yayımlanan "*Bilgi ve İletişim Güvenliği Denetim Rehberi*" ile belirlenmiştir.

Bahse konu Rehberde; en az iki kişiden oluşacak denetim ekibinin sahip olması gereken yetkinlikler kapsamında ISO/IEC 27001 Baş Denetçi Sertifikası, CISA (Certified Information Systems Auditor/Sertifikalı Bilgi Sistemleri Denetçisi) Sertifikası veya TSE tarafından verilen D1 tipi Ağ ve Sistem Denetçisi veya D2 tipi Uygulama Denetçisi sertifikaları şart koşulmuş olmakla birlikte kamu kaynaklarının etkin, ekonomik ve verimli kullanımı amacıyla kamu kurum ve kuruluşlarında bu denetimleri gerçekleştirecek iç denetçiler için istisna getirilerek bu sayılanlar veya bu sertifikalar yoksa bilgi güvenliği eğitimi almış ve iç tetkikçi ve(ya) iç denetçi olarak görev yapmış olmak şeklinde esnetilmiştir.

Ayrıca kamu kurumlarından görevlendirmeler yoluyla da denetim ekiplerinin oluşturulması hususuna yer verilmiştir. Bununla birlikte Rehber denetimlerinde özellikle tedbirlerin etkinliğinin değerlendirilebilmesi için ağ ve sistem, veri tabanı, yazılım gibi farklı uzmanlık alanlarında teknik yeterlilik gerektiği de aşikârdır.

Rehber denetimlerinin öncelikli ve esas olarak kurum iç denetçileri tarafından gerçekleştirilmesi gerekli olmakla birlikte denetimleri gerçekleştirecek yetkin personelin bulunmaması halinde ise dış kaynak kullanımı da (başka kurumlardan geçici personel görevlendirme veya hizmet alımı) diğer yöntemler olarak belirlenmiştir. BİGR'de yer alan tedbirlerin denetlenmesi için denetimi gerçekleştirecek personelde ileri düzeyde BT denetim yetkinliğine gereksinim duyulmaktadır. İç Denetim Koordinasyon Kurulu (İDKK) tarafından hazırlanan 2021 yılı *Kamu İç Denetim Genel Raporu*'nda[6], kamu kurumlarındaki iç denetim birim-

6 2021 yılı Kamu İç Denetim Genel Raporu için bkz: https://ms.hmb.gov.tr/uploads/2022/08/2021-Kamu-Ic-Denetim-Genel-Raporu-Son-Hali.pdf

lerinde görev yapan iç denetçilerin sadece yedisinin CISA sertifikasına sahip olduğu görülmektedir (İDKK, 2022a). Rehber denetimlerinden gereken faydanın sağlanması için bu sayının artırılmasına yönelik projelerin hızlıca hayata geçirilmesi oldukça önemlidir.

Rehber denetimlerinin sonucunda uygulama sürecinin etkinliği ve tedbir etkinlik durumunun belirlenmesi şeklinde iki temel hedef bulunmaktadır. Bu süreçte denetim ekibince oluşturulacak dokümanların formatına BİGDR eklerinde ulaşılabilmekte olup formata uyulması ihtiyacı özel olarak belirtilmektedir.

BİGDR'de tanımlı denetim metodolojisi; halihâzırdaki kamu iç denetim uygulamalarına benzer uygulamalar taşımakla birlikte farklılıklar da içermektedir. İç denetim jargonunda ön çalışma olarak isimlendirilen süreç, Rehber'de denetimin planlanması; saha çalışması süreci, denetim prosedürlerin uygulanması; raporlama, aşaması ise denetim sonuçlarının raporlanması olarak isimlendirilmektedir. Üç aşamanın her bir aşamasında gerçekleştirilecek çalışmalar, çalışma kâğıtlarıyla kayıt altına alınması ve belirlenen hususların Rehber ekinde verilen formatlar kullanılarak oluşturulacak dokümanlar aracılığıyla, 04 Ocak 2023 tarihinde DDO tarafından devreye alınan *Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi (BİGDES)* sistemine işlenmesi öngörülmüştür.

4. REHBER DENETİMİNDE İYİLEŞTİRİLMESİ GEREKEN ALANLAR VE ÇÖZÜM ÖNERİLERİ

Rehber denetimi uygulayıcılarına fayda sağlaması açısından iyileştirilmesi gereken alanlar ve bunlarla ilgili çözüm önerilerini ele alan, akademik değerlere uygun olarak yürütülen araştırmanın çalışma kümesi, süre kısıtı olması nedeniyle 5018 Sayılı Kanunun 3/b maddesinde tanımlanan merkezi yönetim kapsamındaki kamu idarelerinde görev yapan rehber denetimini yürüten kamu iç denetçileridir. Rehber denetimi hakkındaki görüşlerini ve tutumlarını ortaya çıkarmak amacıyla hazırlanan soruların doğru analizi, çözüm önerilerinin belirlenmesi ve araştırma odağının kaymaması için uzun ve karmaşık ifadelerin yer almadığı yapılandırılmamış beş sorudan oluşan anket yöntemi çalışmada uygulanmıştır. Rehber denetimi gerçekleştiren kamu iç denetçi sayısının oldukça sınırlı olması ve söz konusu denetim türünün sınırlı sayıdaki kamu idaresinde 2022 yılında ilk kez uygulanması, araştırmanın sınırlılığını oluşturmaktadır. Hazırlanan anket çalışması gönüllülük esasına göre örneklem olarak belirlenen dokuz kamu

idaresinde görev yapan yirmi bir kamu iç denetçisiyle gerçekleştirilmiştir. Tüm katılımcılar anket sorularını eksiksiz cevaplandırarak sorulara yönelik herhangi bir kaçınma eğilimi sergilememiştir. Araştırma yönteminde insan-hayvan üzerinde deneysel çalışma uygulaması bulunmadığından etik kurul iznine ihtiyaç duyulmamıştır.

Rehber denetimi faaliyetlerinde; kamu kurum ve kuruluşlarında kurum içinden görevlendirilen iç denetçilerin bilgi ve tecrübe paylaşımları, denetimlerde sahada karşılaşılan zorluklar ve uygulama sonuçlarının anonimleştirilerek değerlendirilmesi neticesinde iyileştirilmesi gereken alanlar ve çözüm önerileri şu başlıklar altında ele alınmıştır.

- Varlık grubu kritiklik derecelendirme puanlamaların güncellenmesi,
- Bulgu tablosuna bulgu tanımı ifadesinin eklenmesi,
- Bulgu izleme sürecinin iyileştirilmesi,
- Denetim raporunun her sayfasının e-imza ile imzalanması,
- BİGDES denetim görüşü bölümü uygulanması gereken toplam tedbir sayısı algoritmasının güncellenmesi,
- Tedbir maddelerine KamuNet'in teşvik edilmesine yönelik ilave yapılması,
- İç denetçilerin sertifika süreçlerinin desteklenmesi,
- Rehber denetimi yapabilecek iç denetçi havuzunun oluşturulması.

4.1. Varlık Grubu Kritiklik Derecelendirme Puanlamaların Güncellenmesi

Kamu idarelerinin varlık grup derecelendirmelerinin güvenilir olması oldukça önemlidir. Dolayısıyla hem ilgili kamu kurumunun BT güvenliğinin sağlanması hem ilgili kurumunun daha etkin çalışabilmesi hem de vatandaşın doğru bilgiye ulaşabilmesi için varlık kriterlerinin doğru şekilde sınıflandırılması gereklidir (Özçayan ve Aslan, 2021, s. 32).

BİGR kapsamında varlık gruplarına uygulanacak tedbirler, varlık grupları bazında gerçekleştirilen anket sonucuna göre tespit edilen kritiklik dereceleri baz

alınarak belirlendiğinden, anket puanlamasına göre üçlü ölçekte seviyelendirme işleminin Rehber uyum sürecinde kilit kontrollerden biri olduğu aşikârdır. Anketlerin; her bir varlık grubu için varlık sahibi, yazılım geliştiricisi ve sistem yöneticisi gibi ilgili kişilerce doldurularak farklı farklı alanlarda görev yapan ve süreçte yer alan uzman personelin veri toplama aşamasında yer aldığı Delphi metodunun (Bahar ve Somuncu Demir, 2021, s.37) uygulanması ve puanlama yapılarak sonuçlara göre varlık grubu seviyelerinin belirlenmesi gerekmektedir.

Güvenlik perspektifinde hazırlanan BİGR'nin tedbir maddeleri incelendiğinde, kritiklik derecelerine göre uygulanması öngörülen üçüncü seviye bazı tedbirlerin oldukça ileri seviyede belki de sadece milli güvenliği tehdit edebilecek ve(ya) askeri sistemlerde uygulanması gerekecek önlemler içerebildiği değerlendirilmektedir. Denetim uygulamalarındaki tecrübe edilen sonuçlar da kurum kültürü, bütçe kısıtlamaları, personel yetersizliği veya birebir vatandaşa yönelik özellikle kamuya açık gizlilikten daha yüksek oranda erişilebilirlik unsurunun ön planda olduğu iş ve işlemlerde üçüncü seviyedeki tedbirlerin uygulanması veya sonuçlarından bazı hizmet süreçlerinin olumsuz etkilenebildiği ya da buna yönelik ciddi kaynak planlamalarına ihtiyaç olabileceği görülmüştür.

Bu nedenlerle, anket sonuçlarına göre tedbirlerin uygulanması için kritiklik dereceleri belirlenirken uygulanmakta olan anket puan aralıklarının yukarı yönde revize edilmesi veya kritiklik derecelendirmelerinde beşli ölçeğe geçilmesinin daha fazla fayda sağlayabileceği düşünülmektedir. Yapılan değerlendirmede mevcut her iki Rehberin kurgusu ve ekli tablolarda yer alan tedbirlerin yeniden beşli ölçeğe göre kritiklik seviyelerinin belirlenmesi süreçte radikal bir değişiklik ve çalışma gerektireceğinden ilk aşamada üçlü ölçekle devam edilmesi ve kritiklik derecelendirme sürecinde kullanılan sınır değerlerin yukarı yönlü revize edilmesinin bu aşamada hızlıca uygulanabilir etkin bir öneri olduğu sonucuna varılmıştır.

Örnek olarak bir kurumda fiziksel ve sanal sunuculardan oluşan 'Sunucu Sistemleri' varlık grubu tanımlandığını ve bu varlık grubuna yönelik kritiklik derecelendirme anket sonuçlarının, aşağıda yer alan örnek olarak oluşturulan Tablo 1'de verildiği gibi olduğunu varsayalım.

Tablo 1: Sunucu Sistemleri Varlık Grubu Anket Sonuçları Örnek Tablosu

Boyut	Soru No	Şıkların Puanları					Soru Puanı
		a	b	c	d	e	
İşlenen Veri Açısından							
Gizlilik	1	1 puan	2 puan	3 puan	5 puan		3
Bütünlük	2	1 puan	2 puan	3 puan	5 puan		3
Erişilebilirlik	3	1 puan	2 puan	3 puan	5 puan		5
Etki Alanı Açısından							
Etkilenen Kişi Sayısı	4	1 puan	2 puan	3 puan	4 puan	5 puan	5
Toplumsal Sonuçlar	5	1 puan	2 puan	3 puan	5 puan	6 puan	3
Kurumsal Sonuçlar	6	1 puan	2 puan	3 puan			3
Sektörel Etki	7	1 puan	2 puan	3 puan	5 puan		5
Bağımlı Varlıklar	8	1 puan	2 puan	3 puan	5 puan	6 puan	5
Anket Puanı (Tüm soruların puanlarının toplamı)							32

Kaynak: Yazarlar tarafından oluşturulmuştur.

Bu senaryoda; yürütülen iş ve işlemlerin doğası gereği ikinci seviye tedbir uygulanmasının daha uygun olacağı değerlendirilmekle birlikte kritiklik derecesinin 3. seviye belirlenmesi nedeniyle uygulanması gerekecek ilave tedbirlere ilişkin donanım, yazılım, personel, eğitim ve lisans ihtiyaçlarına yönelik beş örneğe aşağıda yer verilmiştir.

- 3.1.6.33 "*Kripto Ağ Cihazlarının Kullanım*" tedbiri kapsamında kripto ağ cihazı kullanımı,
- 3.1.6.36 "*Veri Transferi*" tedbiri kapsamında veri diyotu kullanımı,
- 3.1.11.9 "*Düzenli Kırmızı Takım Tatbikatlarının Yapılması*" tedbiri kapsamında kırmızı takım tatbikatları yapılması,
- 5.1.2.8 "*Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi*" tedbiri kapsamında işletim sistemindeki erişim kontrolü, ilgili servisler (SELinux, AppArmor vb.) aracılığıyla zorunlu erişim kontrolü (MAC) modeline göre yapılması,

- 5.3.2.15 "*Disk ve İmajların Şifreli Olarak Saklanması*"na ilişkin ilave sıkılaştırma tedbiri.

Bahse konu BİGR EK.C1'de verilen anket sorularının puan değerleri kullanılarak herhangi bir varlık grubunun alabileceği minimum ve maksimum puanlara ilişkin sınır değerler aşağıdaki Tablo 2'de gösterildiği gibi 8 (sekiz) ile 40 (kırk) puan olarak belirlenebilmektedir.

Tablo 2: BİGR'nin Anket Sonuçlarına Göre Varlık Grubu Alabileceği Sınır Değerler

Soru No	Minimum Puan	Maksimum Puan
1	1	5
2	1	5
3	1	5
4	1	5
5	1	6
6	1	3
7	1	5
8	1	6
Toplam	**8**	**40**

Kaynak: Yazarlar tarafından oluşturulmuştur.

Hâlihazırda BİGR'de mevcut uygulamada anket puanı 18'den küçük ise 1. derece, 18 (dâhil) – 28 puan aralığı 2. derece ve 28 ve daha yüksek olanlar ise 3. derece (en kritik ve en fazla tedbir) şeklinde belirlenmektedir.

Yukarıda açıklanan hususlar ve edinilen tecrübelerden hareketle BİGR'de yer alan "*Anket Puanına Karşılık Gelen Kritiklik Derecesi*" tablosundaki değerlerin gözden geçirilmesi, 3.Derece kritiklik seviyesinin sadece milli güvenliği doğrudan etkileyen sistemlere yönelik olacak biçimde iyileştirilmesine ihtiyaç bulunduğu değerlendirilmektedir. Konuya ilişkin mevcut durum ve yapılabilecek iyileştirmeye yönelik karşılaştırmalı öneri tablosu aşağıda verilmiştir.

Tablo 3: Anket Puanına Karşılık Gelen Kritiklik Derecesi Değişiklik Önerisi

Kritiklik Derecesi	Anket Puanı	
	BİGR Mevcut Durum	**Önerilen**
1. Derece	**18**'den küçük ise	**23**'den küçük ise
2. Derece	**18** (dâhil) ile **28** arasında ise	**23** (dâhil) ile **33** arasında ise
3. Derece	**28** ve daha yüksek ise	**33** ve daha yüksek ise

Kaynak: Yazarlar tarafından oluşturulmuştur.

4.2. Bulgu Tablosuna Bulgu Tanımı İfadesinin Eklenmesi

Denetim sonuçları doğrultusunda ilgili birimlerin ihtiyaç duyulan, gerekli aksiyonları alabilmesi ve denetim standartları gereği denetim raporlarının açık ve anlaşılabilir olması oldukça önemlidir (Yanık ve Karataş, 2017). BİGDR'nin "*Bulguların Tespiti, Değerlendirilmesi ve İzlenmesi*" başlıklı maddesinde belirlendiği biçimde "*EK-G Bulgu Tablosu*"na işlenerek denetlenen birime iletilen bulguların (özellikle kısmen etkin olarak belirlenen tedbirler için) denetlenen birim tarafından anlaşılması, denetim kapsamına alınan varlık grubu içindeki hangi bilgi varlığında eksiklik olduğunu ifade edecek ve ilgili tedbir maddesinin etkin olarak uygulanması için ne yapması gerektiğini bildirecek bir yapının bulunmaması nedeniyle gerçekleştirilecek düzeltici faaliyetin belirlenmesi ve buna yönelik doğru aksiyonların alınması hususunda güçlük yaşanmaktadır.

Ayrıca denetim sonucunda elde edilen bulguların, denetlenen birimle paylaşımı sırasında farklı varlık gruplarına yönelik aynı tedbirle ilişkili bulguların bulunması durumunda konunun anlaşılmasının daha da güçleşebildiğinden denetim ekibi ile denetlenen birimler arasında iletişim problemleri ile karşılaşılabilmektedir. Bulguların anlaşılabilirliği bakımından EK-G Bulgu Tablosuna ilave bir sütun ile "İlgili *Olduğu Tedbir Maddesi*"nden sonra "*Bulgu Tanımı*" ifadesinin aşağıdaki tablodakine benzer biçimde eklenmesinin sürece önemli katkı sağlayacağı değerlendirilmektedir.

Tablo 4: Önerilen Bulgu Tablosu Örnek Gösterimi

Sıra No	Bulgu Kodu	İlgili Olduğu Tedbir Maddeleri	Bulgu Tanımı
1	2022.1.1.U02.Y	U02 Kurumsal bilgi varlıklarının varlık grubu altında belirtilmesi	Yazıcıların ve kartlı geçiş sisteminin varlık grubunda yer almadığı belirlenmiştir.
2	2022.1.2.T01.Y	FELAKET KURTARMA VE İŞ SÜREKLİLİĞİ YÖNETİMİ 3.1.13.1. Yedekleme Planının Oluşturulması	Yedekleme planın mevcut değildir.
3	2022.1.3.T02.Ç	DOSYALARIN VE KAYNAKLARIN GÜVENLİĞİ 3.2.4.1. Denetim Kayıtları, Yapılandırma Dosyaları, İz Kayıtları vb. Bilgilerin Kullanıcı Verisiyle Aynı Ortamda Saklanmaması	İz kayıtlarının merkezi iz kayıt sistemine gönderilmediği belirlenmiştir.

Kaynak: Yazarlar tarafından oluşturulmuştur.

4.3. Bulgu İzleme Sürecinin İyileştirilmesi

Denetim sonuçlarının değerlendirilmesi ve izlenmesi süreci kamu kurumlarının hesap verilebilirliğinin ve uygulama sonuçlarının görülebilmesinde, kurumlarda sağlam bir bilgi tabanı oluşturulmasında kulanılabilecek en güçlü kamu yönetimi araçları arasında yer almaktadır (Kusek ve Rist, 2004, s. 170). Dolayısıyla BİGDR "*Bulguların Tespiti, Değerlendirilmesi ve İzlenmesi*" başlıklı maddesi bulguların değerlendirilmesi ve izlenmesi kısmında kurum kaynakları ile gerçekleştirilen denetimlerde oluşturulacak izleme sisteminde tanımlanan süreçte tespit edilen bulguların izleme sürecinin beklenen faydayı sağlayabilmesi amacıyla süreçteki adımların, rol ve sorumlulukların netleştirilmesi ihtiyacı bulunduğu düşünülmektedir. Bu amaçla aşağıdaki tabloda verilen Bulgu Tablosu Eylem Planının BİGDR'ye ilave edilmesinin izleme sürecine katkısı olabileceği değerlendirilmektedir.

Tablo 5: Bulgu Tablosu Örnek Eylem Planı

Sıra No	Bulgu Kodu	Tedbir Alt Başlığı	İlgili Olduğu Tedbir Maddeleri	İlgili Birim	İlgili Personel	Tamamlanma Tarihi
1	2022.1.1.U02.Y	-	U02 Kurum bilgi varlıklarının mutlaka bir varlık grubu altında tanımlanması	Bilgi Güvenliği Dairesi Başkanlığı	Ali BİLGER (Uzman)	26.05.2023
2	2022.1.2.T01.Y	FELAKET KURTARMA VE İŞ SÜREKLİLİĞİ YÖNETİMİ	3.1.13.1. Yedekleme Planının Oluşturulması	Sistem ve Sunucu Yönetimi Dairesi Başkanlığı	Zeynep BERBER (Mühendis)	26.10.2023
3	2022.1.3.T02.Ç	DOSYALARIN VE KAYNAKLARIN GÜVENLİĞİ	3.2.4.1. Yapılandırma Dosyaları, Denetim Kayıtları, İz Kayıtları vb. Bilgilerin Kullanıcı Verisiyle Aynı Konumda Depolanmaması	Yazılım Geliştirme Dairesi Başkanlığı	Emin ER (Bilişim Uzmanı)	12.07.2023

Kaynak: Yazarlar tarafından oluşturulmuştur.

Esasen iç denetim faaliyetlerinde önemli bir yeri olan, yönetim ve karar alma süreçlerini desteklemek amacıyla özel amaçlı bir yönetim fonksiyonu olarak da görülen (Kusek ve Rist, 2004, s. 12) izleme faaliyetinden istenilen faydaya ulaşabilmek için bilgi güvenliği yönetim sisteminde yürütülmekte olan "*Düzeltici Faaliyet*" tanımlanması ve sürekli iyileştirmeyi tanımladığı değerlendirilen izleme sistemine ilişkin bölümün netleştirilmesi veya en azından varsa BGYS içinde veya buna benzer biçimde bulgu tanımlamalarının "*Bulgu Tablosu*"na ilavesine ilişkin önceki maddede açıklanan önerilerin hayata geçirilmesi ile denetim eki-

bince kısaca tanımlanacak olan bulgu tanımlarına yönelik Düzeltici Faaliyetler ile alınacak ve(ya) alınmış aksiyonların kayıt altına alınmasının sağlanmasının izleme sürecinin etkinliğine ve uygulanabilirliğine katkı sağlayacağı değerlendirilmektedir.

Diğer taraftan; varlık gruplarının yapısının dinamik olmasından dolayı bulgu yazılan bir varlık bileşeninin izlemenin yapıldığı dönem süresince farklı bir varlık grubuna taşınması, kurumlarda denetimi gerçekleştiren denetim ekiplerinin her sene bu denetimi en az bir defa yapmaları ve sonuç odaklı izleme ve değerlendirme sürecinin de en az bir denetim kadar uzun sürebileceği gibi nedenlerle sınırlı denetim kaynağı ile izleme sürecinin zorlukları da dikkate alınmalı, her bir izleme için kurum içinde "İzleme Raporu" oluşturularak yeknesaklığın sağlanması gereklidir.

4.4. Denetim Raporunun Her Sayfasının e-imza ile İmzalanması

Son yıllarda yaşanan dijital dönüşüm süreci kamu yönetimini ciddi oranda etkilemiştir. Bürokratik işlem fazlalığı ve gereksiz prosedürler e-devlet uygulamalarıyla birlikte azaltılarak zaman ve maliyet açısından önemli ölçüde kazanç elde edilmesine rağmen iş yapış tarzındaki bürokratik işlemlerin büsbütün ortadan kaldırıldığı da söylenemez (Taş vd., 2017, s. 2317). Örneğin denetim raporunun her sayfasının imzalanması gibi.

BİGDR "*3.3.1. Denetim Raporunun Hazırlanması ve Kuruma Sunumu*" başlıklı bendi hükümleri kapsamında denetim raporunun her sayfasının e-imza ile imzalanması süreci denetim ekibindeki denetçi sayısı ve raporun sayfa sayısına bağlı, oldukça zaman almaktadır. Oysa ki kamu kurum ve kuruluşlarının birçoğunda e-imza kullanılan *Elektronik Belge Sistemleri (EBYS)* üzerinden yazışmalar yürütülmektedir. Bu nedenle söz konusu sistemlerin kullanıldığı kurumlarda, kurum iç denetçileri tarafından hazırlanan raporların, ayrıca her sayfasının e-imza ile imzalanması ihtiyacı bulunmadığına dair bir kolaylık getirilmesinin, sürece ciddi katkı sağlayacağı değerlendirilmektedir.

4.5. BİGDES Denetim Görüşü Bölümü Uygulanması Gereken Toplam Tedbir Sayısı Algoritmasının Güncellenmesi

Denetim Rehberi ekindeki örnek formata göre denetim görüşü (*EK-H*) içinde yer verilen tedbirlerin etkinlik durumlarına ilişkin özet tabloda; her bir varlık grubuna uygulanması gereken toplam tedbir sayısı, bu tedbirlerin etkinlik durumları sayısı "*Etkin*", "*Etkin Değil*", "*Kısmen Etkin*" şeklinde belirlenmiştir. Bu bakımdan; aşağıdaki tabloda sunulduğu biçimde seçilen varlık grubunda uygulanan tedbirlerin elli adedi etkin, otuz adedi etkin değil ve yirmi adedi kısmen etkin ise uygulanması gereken toplam tedbir sayısının bu üç durumun toplamı olacak biçimde yüz adet olması ve doğal olarak bu toplamda tedbir uygulanma durumu "*Uygulanabilir Değil*" olan tedbirlerin yer almaması beklenir.

Hal böyle iken BİGDES sisteminde gerçekleştirilen otomatik hesaplamalarda, varlık gruplarına uygulanması gereken tedbir sayısı; EK-B'de belirlenen üst tedbir grupların esas alınması nedeniyle EK-F "*Tedbir Etkinlik Durumu*" tablosunda yer alan tedbirlerin uygunmasına ilişkin durumları gösteren sütunda "*Uygulanabilir Değil*" olarak belirlenen tedbirler dahil olarak hesaplanmaktadır.

Bu nedenle, aşağıdaki tabloda gösterildiği gibi uygulanabilir olmayan tedbir bulunması durumunda tedbir etkinlik durumlarına ilişkin toplam sayı ile BİGDES hesaplama sonuçlarında bulunan uygulanması gereken tedbirlerin toplamı örtüşmeyecektir.

Tablo 6: Uygulanması Gereken Toplam Tedbir Sayısı Hesaplama Örneği

Mevcut Durum	Uygulanması Gereken Toplam Tedbir Sayısı	Etkin Tedbir Sayısı	Etkin Olmayan Tedbir Sayısı	Kısmen Etkin Tedbir Sayısı	Uygulanabilir Değil Tedbir Sayısı
Denetim Rehberi	100	50	30	20	Tabloda yer verilmemiştir.
BİGDES Hesaplama Sonuçları	100	50	30	20	0
	130	50	30	20	30

Kaynak: Yazarlar tarafından oluşturulmuştur.

Tedbir etkinlik durumlarının toplamının, uygulanması gereken toplam tedbir sayısını göstermesi üst yöneticinin de imzaladığı anılan dokümanın tutarlılığı bakımından önemlidir. Bu nedenle; BİGDES hesaplama algoritmasında, üst tedbir grupları bazında uygulanması gereken toplam tedbir sayısından EK-F tabloda tedbir uygulanma durumu "*Uygulanabilir Değil*" olarak belirlenen tedbirlerin çıkarılarak "*Uygulanması Gereken Toplam Tedbir Sayısı*"nın belirlenmesi için gerekli güncellemenin yapılması önerilmektedir.

4.6. Tedbir Maddelerine KamuNet'in Teşvik Edilmesine Yönelik İlave Yapılması

İlgili kurumda gerçekleştirilen rehber denetiminde, kamu kurumları arasında çeşitli amaçlar için gerçekleştirilen veri transferlerinde ve bilgi paylaşımında KamuNet kullanım oranının rehberin mevcut haliyle değerlendirilemediği, bu nedenle de Kamu kurum ve kuruluşlarının KamuNet'i kullanmalarını teşvik ve hangi düzeyde/oranda KamuNet'i kullandıklarının değerlendirilmesi amacıyla BİGR tedbir maddeleri ve benzer biçimde BİGDR eki tablolara aşağıdaki tedbir maddelerinin ilave edilmesiyle KamuNet kullanımının teşvik edilebileceği, bunun da sürece olumlu katkı sağlayacağı değerlendirilmektedir.

Tablo 7: BİGR Eki Tablolar İlave Edilebilecek KamuNet Tedbir Maddeleri

Sıra No	Tedbir No	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3. VARLIK GRUPLARINA YÖNELİK GÜVENLİK TEDBİRLERİ				
3.1. Ağ ve Sistem Güvenliği				
3.1.6. Ağ Güvenliği				
X[7]	3.1.6.X	1	Kamu idareleri arasında gerekli olan veri iletişiminin KamuNet üzerinden yapılması	Kamu idarelerindeki siber güvenlik risklerinin azaltılması amacıyla aralarındaki gerekli veri iletişiminin, genel ağ yerine daha güvenli sanal bir ağ üzerinden sağlanması için KamuNet ağına dâhil olunmalıdır. Kurumun üst yönetimince kabul edilen bilgi güvenliği yönetim sistemi politikasına uygun şekilde KamuNet ile ilgili politika ve prosedürler tanımlanmalıdır.
X	3.1.6.X	1	KamuNet üzerinden sunulan/alınan hizmetlerin envanterinin tutulması	KamuNet üzerinden sunulan/alınan hizmetlerin envanteri tutulmalı ve güncelliği sağlanmalıdır.
X	3.1.6.X	2	Kamu kurum ve kuruluşlarının işletmeci ile arasındaki KamuNet ağı erişiminin yedekliliğinin sağlanması	Kamu idarelerinin işletmeci ile arasındaki KamuNet ağı erişimi farklı güzergâh ve santrallerde yedeklenmelidir.

Kaynak: Yazarlar tarafından oluşturulmuştur.

BİGR eki tablolarda yer alan tedbir maddelerine ilave edilebilecek KamuNet'e ilişkin tedbir önerileri Tablo 7'de, bu önerilere ilişkin BİGDR eki tablolara ilave edilebilecek denetim madde önerileri ise Tablo 8'de sunulmuştur.

7 BİGR'nin ilgili Tablosunda DDO tarafından belirlenecek tedbir sırasına göre numaralandırılacaktır.

Tablo 8: BİGDR Eki Tablolar İlave Edilebilecek KamuNet Tedbir Maddeleri Denetim Yöntemleri Önerisi

Sıra No	Tedbir No	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3. VARLIK GRUPLARINA YÖNELİK GÜVENLİK TEDBİRLERİ				
3.1. Ağ ve Sistem Güvenliği				
3.1.6. Ağ Güvenliği				
X[8]	3.1.6.X	Kamu idareleri arasında gerekli olan veri iletişiminin KamuNet üzerinden yapılması	Mülakat, Güvenlik Denetimi	KamuNet ağına dâhil olundu mu? KamuNet ağı aktif olarak kullanılmakta mıdır? Kamu idareleri arasındaki veri iletişiminin ne kadarı KamuNet üzerinden yapılmaktadır? KamuNet gereksinimleri karşılanmakta mıdır? Kurum üst yönetimince kabul edilen bilgi güvenliği yönetim sistemi düzenlemelerine uygun şekilde KamuNet ile ilgili politika tanımlanmış mıdır?
X	3.1.6.X	KamuNet üzerinden sunulan/alınan hizmetlerin envanterinin tutulması	Mülakat, Güvenlik Denetimi	KamuNet üzerinden sunulan/alınan hizmetlerin envanteri tutulmakta mıdır? Bu envanterin güncelliği nasıl sağlanmaktadır?
X	3.1.6.X	Kamu kurum ve kuruluşlarının işletmeci ile arasındaki KamuNet ağı erişiminin yedekliliğinin sağlanması	Mülakat, Güvenlik Denetimi	Kamu kurum ve kuruluşlarının işletmeci ile arasındaki KamuNet ağı erişiminin yedekliliği sağlanmış mıdır?

Kaynak: Yazarlar tarafından oluşturulmuştur.

8 BİGR'nin ilgili Tablosunda DDO tarafından belirlenecek tedbir sırasına göre numaralandırılacaktır.

4.7. İç Denetçilerin Sertifika Süreçlerinin Desteklenmesi

Tüm kamu kurumları ile kritik altyapı hizmeti sunan işletmelerin uymakla yükümlü olduğu BİGR'e uyum ve tedbirlerin etkinliğinin en az yılda bir defa denetlenerek sürecin etkin bir şekilde izlenmesi planlanmıştır. Farklı kurumlarda yer alan iç denetçiler ile yapılan bilgi alışverişlerinde çeşitli nedenlerle (denetimi gerçekleştirecek yetkinlikte iç denetçi kaynağı olmaması, kurumun rehber uyum sürecini tamamlayamaması nedeniyle tedbir uyum sürecinin değerlendirilememesi gibi) halihazırda rehber denetimi yapılamadığı görülmüştür. Kamu kaynaklarının etkin, ekonomik ve verimli kullanımı amacıyla süreklilik arz eden bu denetimler için ihtiyaç duyulan yetkin denetçi kaynağının oluşturulması, sürecin maliyet etkin bir biçimde sürdürülebilirliği açısından elzemdir. Bu bakımdan kamu kurumlarında Rehber denetimlerini gerçekleştirebilecek sınırlı sayıdaki iç denetçi kaynağının nitelik ve niceliğinin artırılmasına yönelik çalışmalara ihtiyaç duyulmaktadır.

BİGDR ile belirlenen denetim ekibinin sahip olması gereken yetkinlikler "*ISO/IEC 27001 Baş Denetçi Sertifikası*", "*CISA Sertifikası*" veya TSE tarafından verilen D1 tipi "Ağ ve Sistem Denetçisi" veya D2 tipi "*Uygulama Denetçisi*" sertifikalarıdır.

BT alanında denetim yapacak denetçi, veri koruma, kayıt yönetimi süreçleri, güvenlik, kontroller ve teknoloji süreçlerinde uzmanlığa sahip olmalıdır. Denetçi ayrıca iş stratejisiyle uyumu belirlemek için yeterli işlevsel bilgiye ve iş bilgisine sahip olmalıdır. Uluslararası bilgi teknolojileri denetimi standartları arasında kabul edilen ISACA ITAF (IT Audit Framework) 1006 standardı denetçinin değerlendirilen alanlarda teknik beceri, bilgi ve/veya deneyime sahip olmasını gerektirir (ISACA, 2021) .

Bununla birlikte bu duruma bir istisna getirilerek kamu kurum ve kuruluşlarında Rehber denetimlerini gerçekleştirecek iç denetçilerin yukarıda sayılan sertifikalara sahip olmaması durumunda iç denetçinin bilgi güvenliği eğitimi almış olması da yeterlidir. Ancak Rehber denetimlerinde özellikle alınan tedbirlerin etkinliğinin değerlendirilebilmesi için denetimi gerçekleştirecek personelde ileri düzeyde BT denetim yetkinliğine gereksinim duyulmaktadır.

İDKK tarafından hazırlanan 2021 yılı Kamu İç Denetim Genel Raporu'nda[9],

9 2021 yılı Kamu İç Denetim Genel Raporu için bkz: https://ms.hmb.gov.tr/uploads/2022/08/2021-Kamu-Ic-Denetim-Genel-Raporu-Son-Hali.pdf

kamu kurumlarındaki iç denetim birimlerinde görev yapan iç denetçilerin sadece yedisinin CISA sertifikasına sahip olduğu görülmektedir. Rehber denetimlerinden gereken faydanın sağlanması için bu sayının artırılmasına yönelik projelerin hızlıca hayata geçirilmesi oldukça önemlidir.

Kamu kurum ve kuruluşlarında Rehber denetimini gerçekleştirebilecek, BT konusunda yetkin kısıtlı iç denetim kaynağının olgunluk seviyesini artırmak amacıyla BİGDR'de belirlenen temel sertifikalar olarak sayılan CISA, TSE D1 (Ağ ve Sistem Denetçisi) ve D2 (Uygulama Denetçisi) gibi sertifikasyonların teşvik edilmesi, kamu yararı çerçevesinde ihtiyaç duyulan sertifikalarla ilgili eğitim ve sınav ücretlerinin kurumlar tarafından karşılanması amacıyla projelerin hayata geçirilmesi için DDO ile İDKK koordinasyonunda çeşitli fonların (IPA, AB vb.) kullanımının sağlanmasının sürece katkı sağlayacak anahtar çözümlerden biri olduğu görülmüştür.

4.8. Rehber Denetimi Yapabilecek İç Denetçi Havuzunun Oluşturulması

Bir önceki öneride belirtildiği üzere yıllara sari bir yapıda BT konusunda yetkin iç denetçiler tarafından icrası gereken Rehber denetimlerinin maliyet etkin biçimde sürdürülebilirliği; ancak ve ancak kamuda istihdam edilen yetkin iç denetçi kaynağının etkin biçimde kullanımı ile mümkündür. Bu bilinçle BİGDR'de söz konusu denetimlerin farklı kamu kurumlarında görev yapan iç denetçilerin denetimin gerçekleştirileceği idarelerde geçici olarak görevlendirilmesi yoluyla yapılmasına da müsaade edildiği görülmektedir.

Bununla birlikte uygulamada zaten sınırlı sayıdaki BT konusunda yetkin mevcut iç denetçi kaynağının kamuda etkin olarak kullanımının koordinesinde sorunlar yaşanabildiği ve Rehber denetimi gerçekleştiremeyen çok sayıda kurum olduğu görülmüştür. Bu nedenle, kurumunda iç denetçi bulunmayan veya BİGDR'de belirlenen yetkinliklere sahip denetim kaynağı mevcut olmayan ve(ya) rehber denetimlerini hizmet alımı yoluyla gerçekleştiren kamu kurum ve kuruluşlarının denetimlerinin, diğer kamu kurumlarında görev yapan iç denetçiler tarafından kurum dışı görevlendirme yoluyla yapılmasına yönelik kamu personel yönetimine zarar vermeden İDKK ve DDO koordinesinde bu denetimleri yapma yetkinliği bulunan iç denetçilerin olduğu bir denetçi havuzunun oluşturulması için yasal altyapının oluşturulması kaynakların ve denetim faaliyetlerinin etkili, etkin ve ekonomik kullanılmasını sağlayacaktır.

İç denetçilere istekleri dışında farklı bir görev verilemeyeceği, yaptırılamayacağı ve atanamayacağına ilişkin merî mevzuat hükümleri dikkate alınarak denetçi havuzunun gönüllü iç denetçiler tarafından oluşturulması gerektiği aşikardır. Bu nedenle; Rehber denetimlerini gerçekleştirecek gönüllü iç denetçilerden denetçi havuzu oluşturulması, havuzda yer almanın teşviki amacıyla denetimlerin görev kabul onayı ile gerçekleştirilmesi ve havuzun genişletilmesine yönelik BT konusunda yetkin iç denetçi atamalarının teşvik edilmesi amacıyla kurumlara sağlanan kontenjanlardan muaf tutulması, işin niteliği nedeniyle Rehber denetimlerinde görevlendirilecek iç denetçilere ek mali olanakların sağlanması da düşünülmelidir.

SONUÇ

Dijital dönüşüm ve siber güvenlik çalışmalarını yalnızca yeni teknolojileri devreye almak olarak algılamaktan ziyade bu dönüşümün, kurumsal yeniden yapılanma modeli olarak, yeni yönetim ve denetim yapısının tasarlanması şeklinde düşünülmesi gerekmektedir. Siber güvenlik ekosistemini sadece BT olarak değil, bir beka sorunu olarak gören kamu idareleri, BT alanında ortaya çıkabilecek olası krizlerle karşılaşmamak için diğer risklerde olduğu gibi BT risklerini de öngörmek ve bu risklere karşı önlemlerini almak ve ihtiyaç duyulan denetimleri ilgili kurumlarda gerçekleştirmek zorundadır. Dünyada siber güvenliği tek seferde sağlanan ya da alınan bir ürün olarak görmeyerek bunu bir süreç olarak değerlendiren ve bu alanda söz sahibi olacak ülkeler bahsedilen riskleri ön görerek önlem alanlardan olacaktır.

Birçok alanda olduğu gibi dijital dönüşüm ve siber güvenlik alanında da ülkesel gelişmeler oldukça önemli bir durum haline gelmekle birlikte siber dünyada ülkelerin geldiği aşama net olarak bilinememektedir. Sun Tzu'nun "Savaş Sanatı - *The Art of War*" adlı eserindeki "*Kendini ve rakibini biliyorsan korkmana gerek yok, kendini biliyor ancak rakibi bilmiyorsan kazandığın her galibiyet için bir mağlubiyette yaşayacaksın, kendini ve düşmanını da bilmiyorsan her durumda yenilirsin*" (Tzu, 2019) ifadesinden hareketle Türkiye'nin de milli siber ekosistemini geliştirmesi ve açıklarını kapatması gereklidir.

Siber saldırıların artacağı yakın gelecekte kurumlar ikiye ayrılacaktır. Birinci grup, siber saldırıya uğradığını bilenler; ikinci grup ise bu saldırıya maruz kaldığını fark etmeyenler olacaktır. Türkiye'de "Ülke olarak olası bir siber saldırıya ve(ya) savaşa kurum ve kuruluşlar ne kadar hazır?" sorusuna cevap verebilmek için öncelikle denetim faaliyetlerinin yapılabilirliğinin sorgulanması oldukça önemlidir.

İDKK tarafından yayımlanan "*Kamu İdarelerindeki İç Denetim Faaliyetlerine İlişkin Duyuru*"[10] dikkate alındığında kamu kurum ve kuruşlarının tamamında ya iç denetim birimi bulunmamakta ya da iç denetim birimi bulunmasına rağmen kurumlar Rehberde öngörülen denetimi gerçekleştirecek yetkinlik ve yeterlikte iç denetçiye sahip değillerdir (İDKK, 2022b). BİGR'de bu gibi denetim kaynağı

10 Duyuru metni için bkz: https://www.hmb.gov.tr/duyuru/kamu-idarelerindeki-ic-denetim-faaliyetlerine-iliskin-duyuru.

bulunmayan durumlarda denetimin hizmet alımı yoluyla özel sektörden karşılanacağını belirtilse de gerek mesleki gelişimin sürdürülmesi, gerek iç denetim atamalarının sağlanması, gerek siber güvenlik alanında uzman kalifiye personelin yetiştirilmesi gerekse de kamu kaynaklarının verimli, etkili ve ekonomik olarak kullanılması için kamu kurumlarında gerçekleştirilecek denetimlerin kamu iç denetçileri eliyle yürütülmesinin daha faydalı olacağı değerlendirilmektedir.

BİGDR denetiminin birincil uygulayıcısı olan iç denetçilerin Rehberde kendilerine tanımlanan uyum sürecinin ve tedbirlerinin etkinliğinin değerlendirilmesi olarak özetlenebilecek Rehber denetimlerinin yanısıra görev yaptıkları kurumlarda tüm birimlerde dijital dönüşüm farkındalığının sağlanmasına ve dijital dönüşüm yol haritasının ilgili üst kademe yönetimince oluşturulmasına katkıda bulunması, faaliyetlerin gerçekleştirilmesi ile ilgili kurumsal kültürün Rehber çerçevesinde iyileştirilmesi oldukça önemlidir. Öte yandan iç denetimin denetim fonksiyonunun yanısıra danışmanlık fonksiyonunun da bulunması nedeniyle iç denetçinin rehberdeki bazı rol ve sorumluklarda danışılan rol olarak da yer alması alanında uzman teknik personel olarak değerlendirilen BT alanında görev yapan iç denetçilerin bilgi ve tecrübelerinden daha fazla faydalanılmasına olanak sağlayacaktır.

Bu çalışmayla, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanan Bilgi ve İletişim Güvenliği Rehberi ile Bilgi ve İletişim Güvenliği Denetim Rehberine dikkat çekmenin yanı sıra çalışmada belirtilen sınırlılıklar çerçevesinde belirlenen kamu iç denetçilerine yapılandırılmamış beş sorudan oluşan anket yönteminin uygulanması sonucunda karşılaşılan ve iyileştirilmesi gereken alanlar belirtilerek atılacak iyileştirici adımlar için aşağıda özetlenen hususlarda çözüm yolları önerilmiştir.

- Varlık grubu kritiklik derecelendirme puanlamaların güncellenmesi,
- Bulgu tablosuna bulgu tanımı ifadesinin eklenmesi,
- Bulgu izleme sürecinin iyileştirilmesi,
- Denetim raporunun her sayfasının e-imza ile imzalanması,
- BİGDES denetim görüşü bölümü uygulanması gereken toplam tedbir sayısı algoritmasının güncellenmesi,
- Tedbir maddelerine KamuNet'in teşvik edilmesine yönelik ilave yapılması,

- İç denetçilerin sertifika süreçlerinin desteklenmesi,
- Rehber denetimi yapabilecek iç denetçi havuzunun oluşturulması.

Yapılan bu ve benzeri akademik çalışmaların literatüre katkı sağlayacağı gibi uygulayıcılara da yol göstereceği temenni edilmektedir.

KAYNAKÇA

Ağdeniz, Ş. (2021). Bilgi ve İletişim Güvenliği Denetiminde Kamu İç Denetçilerinin Rolü ve Yetkinliklerine İlişkin Bir Araştırma. *Alanya Akademik Bakış*, 5(2), 525-545. DOI: 10.29023/alanyaakademik.869215.

Ak, T. (2019). İç Güvenlik Yönetimi Açısından Kritik Altyapılarını Korunması. *Assam Uluslararası Hakemli Dergi 13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı*, 42-51.

Aloul, F.A. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, 3(3), 176-183. DOI:10.4304/jait.3.3

Appelbaum, D., ve Nehmer, R.A. (2017). Using Drones in Internal and External Audits: An Exploratory Framework. *Journal of Emerging Technologies in Accounting*, 14, 99-113.

Arslan, Y ve Özbilger H.İ. (2022). Ulusal Mevzuat Perspektifinde Bilgi İşlem Birimlerinin İç Denetiminde Bir Model Önerisi, *Denetişim*. 13(26), 1-12.

Bahar, M. ve Somuncu Demir, N. (2021). Delphi tekniği uygulama sürecine yönelik örnek bir çalışma: Çok fonksiyonlu tarım okuryazarlığı. *Bolu Abant İzzet Baysal Üniversitesi Eğitim Fakültesi Dergisi*, 21(1), 35-53. https://dx.doi.org/10.17240/aibuefd.2021.21.60703-814729

Barrigon, C.F. (2020). Innovation and Digital Auditing The Journey of The European Commission's IAS Towards State-Of-The-Art Technologies. *ECA Journal*, 97-100.

Bartz, D. ve Alper A. (2023). U.S. Bans New Huawei, ZTE Equipment Sales, Citing National Security Risk, REUTERS, https://www.reuters.com/business/media-telecom/us-fcc-bans-equipment-sales-imports-zte-huawei-over-national-security-risk-2022-11-25. 14.03.2023 tarihinde erişildi.

BBC (2018). Facebook Scandal 'Hit 87 Million Users', https://www.bbc.com/news/technology-43649018. 05.07.2023 tarihinde erişildi.

Bıçakçı, S. (2013). *21. Yüzyılda Siber Güvenlik*. Bilgi Üniversitesi Yayınları.

Bilge, S. ve Kiracı, M. (2010). *Kamu Sektöründe İç Denetim ve İç Denetimin Başarıyla Uygulanmasında Rol Oynayan Faktörler (Kamu İç Denetçileri Üzerine Bir*

Araştırma). Gazi Kitabevi.

Chu, B. ve Holt, T.J. (2012). *Examining the Creation, Distribution, and Function of Malware On-Line*. Bibliogov Publisher.

DDO. (2020). Bilgi ve İletişim Güvenliği Rehberi. Ankara: T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi.

DDO. (2021). Bilgi ve İletişim Güvenliği Denetim Rehberi. Ankara: T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi.

DDO. (2023). Dijital Devlet Stratejisi. https://cbddo.gov.tr/dijital-devlet-stratejisi. 15.01.2023 tarihinde erişildi.

Darıcılı, B. A. (2014). Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırılar, *Uludağ Üniversitesi Sosyal Bilimler Dergisi*, 7(2), 1-16.

DPT (2000). Uzun Vadeli Strateji ve Sekizinci Beş Yıllık (2001-2005) Kalkınma Planı. Ankara: T.C. Başbakanlık Devlet Planlama Teşkilatı.

Gupta, M. (2020). *Asian Journal of Government Audit*. (Ed.) Singh K. ASOSAI.

ISACA. (2021). Blockchain Framework Audit Program. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-25/new-resource-evaluates-blockchain-controls. 03.02.2023 tarihinde erişildi.

ITU. (2021). Global Cybersecurity Index 2020. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf, 15.03.2023 tarihinde erişildi.

İDKK. (2022a). 2021 Yılı Kamu İç Denetim Genel Raporu, chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://ms.hmb.gov.tr/uploads/2022/08/2021-Kamu-Ic-Denetim-Genel-Raporu-Son-Hali.pdf. 05.02.2023 tarihinde erişildi.

İDKK. (2022b). Kamu İdarelerindeki İç Denetim Faaliyetlerine İlişkin Duyuru, https://www.hmb.gov.tr/duyuru/kamu-idarelerindeki-ic-denetim-faaliyetlerine-iliskin-duyuru. 11.02.2023 tarihinde erişildi.

Karagöz, U. (2022). Bilgi ve İletişim Güvenliği/Denetimi Rehberleri ve İç Denetim. İdarecinin Sesi Dergisi, 210.

Kavitha, V. ve Preetha. S. (2019). Cyber Security Issues and Challenges - *A Review. International Journal of Computer Science and Mobile Computing*, 8(11),

1-16.

Kızılboğa, R. (2013). İç Denetim Sisteminde Denetçilerin Bağımsızlık ve Tarafsızlığının Önemi. *Siyasal Bilgiler Dergisi*, 1(1), 107-121.

Kusek J. Z. ve Rist R.C. (2004). *Ten Steps to a Results-Based Monitoring and Evaluation System: A Handbook for Development Practitioners*, World Bank Publications.

Lambet, P. (2017). Equifax Data Breach, 143 Million Only Tip of the Iceberg. *Int'l J. Data Protection Officer, Privacy Officer & Privacy Couns*, 30, 33-34.

Lois, P., Drogalas, G., Karagiorgos, A. ve Tsikalakis, K. (2020). Internal Audits in the Digital Era: Opportunities Risks and Challenges. *EuroMed Journal of Business*, 15(2), 205-217. http://doi.org/10.1108/emjb-07-2019-0097.

Meral, S. ve Bülbül, H.İ. (2022). Kamu Kurumlarının Bilgi Güvenliği Politikalarının Kurumsal Bilgi Güvenliğinin Sağlanması Açısından Etkinliğinin Analiz Edilmesi, *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji*, 10(2), 314-329. DOI: 10.29109/gujsc.1001706.

Morgan, S. (2019). Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021. 12.03.2023 tarihinde erişildi.

Nelson N.N., ve Madnick, S (2020). Case Study of the Capital One Data Breach, Information Institute Conferences, Las Vegas, NV, Mar 30 Apr 01, 2020, https://www.researchgate.net/publication/340012934_A_Case_Study_of_the_Capital_One_Data_Breach. 12.03.2023 tarihinde erişildi.

OECD (2003). Emerging Risks in the 21st Century. Paris: OECD Publications Service.

Otia, J. E. ve Bracci, E. (2022). Digital Transformation and the Public Sector Auditing: The SAI's Perspective. *Financial Accountability & Management*, 38, 252–280. https://doi.org/10.1111/faam.12317.

Özçayan, G. ve Aslan, N. (2021). Standardızatıon of Trıtıum By Cıemat/Nıst Method Wıth Lıquıd Scıntıllatıon Countıng in Turkey and Uncertaınty Budget . *Turkish Journal of Nuclear Sciences*, 33(1), 26-36.

Özen, A. ve Gürel, F.N. (2022). Kamu Denetiminde Dijital Dönüşüm: Dijital İkiz Yöntemi. *İzmir Sosyal Bilimler Dergisi*, 2(1), 16-23.

Özkaya, E. (2018). *The Art of Human Hacking: Learn Social Engineering with Internationally Renowned Expert*. Packt Publishing.

Özkaya, E. (2023). Güncel Küresel Siber Eğilimler ve Alınması Gereken Önlemler. 6. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi, Ankara: 14-15 Mart 2023.

Page, G. (2102). North Korea's Lazarus hackers are exploiting Log4j flaw to hack US energy companies. https://techcrunch.com/2022/09/08/north-korea-lazarus-united-states-energy. 13.03.2023 tarihinde erişildi.

Ping, G. (2016). What should we do before 5G? https://www.huawei.com/us/huaweitech/publication/winwin/25/what-should-we-do-before-5g. 11.03.2023 tarihinde erişildi.

Pizzi, S., Venturelli, A., Variale, M. ve Macario, G.P. (2021). Assessing the Impacts of Digital Transformation on Internal Auditing: A Bibliometric Analysis. *Technology in Society*, 67, 1-11.

Potii, O. (2018). Cybersecurity Ecosystem. https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2018/05_Kiev/ITU%20Seminar%2015.05.18%20-%20Oleksandr%20Potii.pdf. 13.03.2023 tarihinde erişildi.

Sağıroğlu, Ş. ve Şenol M. (Ed.) (2018). *Siber Güvenlik ve Savunma*: *Farkındalık ve Caydırıcılık.* BGD Siber Güvenlik ve Savunma Kitap Serisi 1, Grafiker Yayınları.

Savita, M. ve Patil, M. (2017). A Brief Study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5), 1938-1940.

Schwab, K., Marcus, A., Oyola, J.R., Hoffman, W. ve Luzi, M. (2011). Personal Data: The Emergence of a New Asset Class. An Initiative of the World Economic Forum. https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf. 11.03.2023 tarihinde erişildi.

Selimoğlu, S. ve Saldı, M.H. (2022). İç Denetimin Blok Zincir Yoluyla Siber Güvenlik Yönetimine Adaptasyonu. *Denetim ve Güvence Hizmetleri Dergisi*,

2(2), 121-134.

Shepardson, D. (2023). Exclusive: White House Sets Deadline For Purging Tiktok From Federal Devices, REUTERS, https://www.reuters.com/technology/white-house-gives-agencies-30-days-impose-federal-device-tiktok-ban-2023-02-27. 14.03.2023 tarihinde erişildi.

Stewart, J., ve Subramaniam, N. (2010). Internal Audit İndependence and Objectivity: Emerging Research Opportunities. *Managerial Auditing Journal*, 25(4), 328-360.

Taffel, S. (2021). Data and Oil: Metaphor, Materiality and Metabolic Rifts. *New Media & Society*, 0(0). 140-175.

Taş, İ. , Uçacak, K. ve Çiçek, Y. (2017). Türk Kamu Yönetiminde Yaşanan Dijital Dönüşümün Bürokratik İşlemlerin Azaltılması Üzerindeki Etkileri. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi Kayfor 15 Özel Sayısı*, 2303-2319.

Tzu, S. (2019), *The Art of War.* (Çev.) Giles, L., Karbon Kitaplar.

Tulgar M., Zaim A. ve Aydın M.A. (2022). Ulusal Bilgi ve İletişim Güvenliği Rehberi: IOT Güvenliği İçin Bir Uygulama Örneği. İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 21(42), 353-382.

UDHB (2014). Kurumsal SOME Kurulum ve Yönetim Rehberi. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/kurumsal-some-reh-v1.pdf. 29.02.2023 tarihinde erişildi.

Verma, A. ve Charu, S. (2022). Cyber Security: A Review of Cyber Crimes, Security Challenges and Measures to Control. *Vision: The Journal of Business Perspective*, 09(0), 24-45.

Yanık, S. ve Karataş, M. (2017). Denetim Raporlarının Geleceği: Yeni Düzenlemeler ve Ülke Uygulamaları. *Muhasebe ve Finansman Dergisi*, (73), 1-26. DOI: 10.25095/mufad.396739.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ (BTK DERGİ)
CİLT: 1 SAYI: 1 TARİH: TEMMUZ - EYLÜL 2023 ISSN: 2980-1311

DİJİTALLEŞEN DÜNYADA DÖNÜŞEN YARDIM ANLAYIŞI: DİJİTAL YARDIM KAMPANYALARI

Canan Gönüllü[1]

Özet

Modern çağda ve modern insanın yaşayış biçimlerinde meydana gelen değişmeler, Türk toplumunda eski zamanlardan bu yana çeşitli görünümleri olan sosyal dayanışma ve yardımlaşmayı da dönüştürmüştür. Dijitalleşmeyle beraber, sosyal ilişki ve pratiklerin yeni bir görünüm sergilediği görülmektedir. Bu çalışmada yardım ve dayanışma gibi kavramlar, toplumsal bütünleşmenin aracı olarak incelenecek ve dönüşen toplum yapısıyla birlikte, yardımlaşma anlayışında meydana gelen değişimler de değerlendirilecektir. Çalışmada üzerinde durulması planlanan ana nokta; sosyal devlet anlayışı gereği, devletin kurumsal olarak sağlamış olduğu sosyal desteklerden ya da Sivil Toplum Kuruluşları (STK) aracılığıyla sağlanan yardımlardan ziyade, yardım kampanyalarının özellikle dijital ortamlarda servis edilmesi ve sosyal medya aracılığıyla duyurulan ihtiyaçlarda, sosyal medyanın rolünün incelenmesidir.

Yardım kampanyaları kimi zaman devlete bağlı organlar ve STK'lar gibi tüzel kişilerce kimi zaman ise bireysel kullanıcılar tarafından başlatılabilmektedir. Kampanyayı başlatanların hedef kitlesi aynı olsa da ortaya çıkan sonuçlar farklılaşabilmektedir. Çalışmada, sosyal mecralarda duyurulan kampanyaların kullanıcıların sosyal medya hesapları, içerik analizi ile incelenip betimlenecektir. Dijital kampanyalar olarak da adlandırabilecek bu yardım faaliyetlerinde ortak olarak öne çıkan birlik duygusu, güvenilirlik gibi kavramlar ve bu kavramların vurgularındaki gerekçeler konusundaki benzerlikler ve farklılıklar ortaya koyulacaktır.

Araştırma sonucunda, hem bireysel hem de kurumsal kampanyalarda, kendilerinden yardım beklenilen kişiler arasında birlik, beraberlik, aidiyet, başarmak, yetmek gibi işteşlik bildiren ifadelerin kullanıldığı görülmüştür. Buna rağmen, özellikle bireysel kampanyaların, resmi kurumlar tarafından onaylanmadan ve sadece sosyal medyada başlatılması durumunda, yardım yapan kimselerin güven duygusunu zedeleyebilecek durumlarla karşılaşılabileceği sonucuna ulaşılmıştır.

Anahtar Kelimeler: *Dijitalleşme, Yardımlaşma, Toplumsal Bütünleşme, Dijital Yardım Kampanyası, Destek.*

[1] Doç. Dr., BurdurMehmet Akif Ersoy Üniversitesi, Fen-Edebiyat Fakültesi, Sosyoloji Anabilim Dalı cgunullu@mehmetakif.edu.tr, ORCID: 0000-0002-7387-1718

THE UNDERSTANDING OF AID TRANSFORMED IN A DIGITALIZED WORLD: DIGITAL AID CAMPAIGNS

Abstract

The changes in the modern age and the lifestyles of modern people have also affected the social solidarity and cooperation, which has various appearances in Turkish society since the past. It is seen that the digitalization that occurs in relationships and actions also resonates in social practices. In this study, concepts such as aid and solidarity will be examined as a means of social integration and the change in the understanding of cooperation will be evaluated together with the transforming social structure. The main point planned to be focused on in the study, in accordance with the social state understanding, it is the service of aid campaigns, especially in digital environments, rather than the social supports provided by the state institutionally or the aid provided through NGOs. And iban number sharing, and especially the campaigns that demand cash support from the public.

Campaigns can sometimes be initiated by legal entities such as state institutions and NGOs, and sometimes by individual users. Even though the target audience of the initiators is the same, the situations that arise may differ. Institutional and individual campaigns were examined in the study. The features of the corporate campaigns, which are reflected in the visuals, the languages used and the press, were examined. In individual campaigns, it was tried to reach the accounts that started the individual campaign and the processes of these accounts that were reflected in the press were interpreted with the help of content analysis. The similarities and differences in the sense of unity, reliability and rationale of digital campaigns have been revealed.

As a result of the research, for those who are expected to help in both individual and corporate campaigns; It has been observed that expressions indicating cooperation such as unity, togetherness, belonging, success, and competence are used. Despite this, it has been concluded that, especially if individual campaigns are started only on social media without being approved by the official authorities, situations that may damage the trust of the donors may be encountered.

Keywords: *Digitalization, Solidarity, Social Integration, Digital Aid Campaign, Support.*

GİRİŞ

Toplum içinde bireylerin var olabilme serüveni, sosyalizasyon süreci olarak tanımlanmakta ve bu tanımlamanın biçimleri zaman zaman araştırmalara konu edilmektedir. Farklı zamanlarda yapılan farklı tanımlamalarda ortak noktalar ya da ayrılan yönler bulmak mümkündür. Bireylerin yaradılışlarının bir gereği olarak bir topluma ya da topluluğa dâhil olma ihtiyacı, farklı disiplinlerin de incelediği bir konudur. Bireylerin hem biyolojik gelişimlerini sağlama ve sürdürmede hem de başkalarına olan bağımlılığın zorunlu bir sonucu olarak diğerleriyle ilişkide olma hali; beraberinde bireylerin toplumsal bir varlık haline gelmesine aracılık etmektedir (Berger ve Luckman, 2008, s. 73).

Teknolojinin günümüzde almış olduğu son hal; yeni iletişim teknolojileri olarak değerlendirilmekle birlikte internet ve sosyal medya bu tanımlamaların önemli birer nesneleri haline gelmektedir. Yeni medya ortamları söz konusu olduğunda fiziksel bir mekân anlayışı ortadan kalkmaktadır ancak buna rağmen bireylerin bu sanal toplumlar içinde de nesnel ve sosyo-kültürel olarak şekillendiği görülmektedir. O halde bireylerin toplumsallaşma anlayışının değişmesi de kaçınılmaz hale gelmektedir (Yengin, 2012, s. 345-346). Yani, günümüzde bireylerin içinde bulunduğu toplumların iletişim süreçleri biçim değiştirmekte ve yeniden inşa edilen bir toplumsallaşma süreci görülmektedir.

Bireyler, günlük yaşantılarında kullanmakta oldukları teknolojik gereçlerle hayatlarını kolaylaştırmakta, ilişkilerini düzenlemekte, eğlenceden eğitime birçok ihtiyacını karşılayabilir hale gelmektedir. Bireylerin kullanmakta olduğu hizmetlerin birçoğu internet ortamlarına taşınmış durumdadır. Örneğin, bankaların sunmuş olduğu mobil bankacılık ya da internet bankacılığı, telefon bankacılığı gibi hizmetlerle, bireylerin fiziki olarak hesaplarında bulunan paralara dokunmadan ve hatta o paraları görmeden diledikleri gibi kullanabilme durumları da ortaya çıkmıştır. Bu durum, değişen ve dönüşen yardım anlayışına katkı sağlayan durumlardan biri haline gelmiştir.

Devlet Planlama Teşkilatı, sosyal yardımı "yerel ölçüler içinde asgari seviyede dahi kendisini ve bakmakla yükümlü olduğu kişileri geçindirme olanağından kendi ellerinde olmayan nedenlerden dolayı yoksun kalmış kişilere resmi kuruluşlar veya kanunların verdiği yetkiye dayanarak yarı resmi veya gönüllü kuruluşlarca muhtaçlık tespitine ve kontrolüne dayalı olarak yapılan, kişileri en kısa

sürede kendi kendilerine yeterli hale getirmek amacını taşıyan parasal ve nesnel sosyal gelirden oluşan bir sosyal güvenlik yöntemi ve bir sosyal hizmet alanıdır" şeklinde tanımlamaktadır (DPT, 2011, s. 51). Günümüzde de tanımlamada sayılan pek çok durumun gerekçe gösterilerek dijital platformlarda başlatılan yardım kampanyalarına rastlamak mümkün hale gelmiştir.

Sosyal mecraların avantajlarından faydalanılarak başlatılan kampanyaların sosyolojik olarak pek çok durumu beraberinde getirdiği de görülmektedir. Bireyler yardım yapma motivasyonlarını çeşitli gerekçelerle dijital ortamlardan sağlamakta ve bu durumun sonuçları da deterministik bir yapı göstererek başka durumları doğurmaktadır. Çalışmanın problemi de bu noktada ortaya çıkmaktadır. Dijitalleşen dünyada yardım kampanyalarının da dijital hale gelmesinin olumlu ya da olumsuz sonuçlarının incelenmesi bir gereklilik haline gelmektedir.

Bu çalışmada, yardım kavramı ve toplumsal önemi açıklanmaya çalışılmış, ardından konu özelinde, dijital bir görünüm sergilemeye başlayan yardım kampanyalarının içerikleri analiz edilmiştir. Yardımlaşmanın, toplumsal bütünleşme, yurttaşlık, birlik olma gibi toplumsal değerlerle olan ilişkisinin önemi vurgulanırken aynı zamanda, yardım isteme biçimlerindeki dilin ayrıştırıcı olabilme ve damgalama ya da etiketleme teorileriyle ilişkilendirilebilme potansiyelleri de araştırmaya konu edilmiştir. Ayrıca özellikle bireysel kampanyalarda, kampanyanın tekil kişilerin, son derece kişisel ihtiyaçlarının karşılanması söz konusu olabilmekle birlikte, durumun dilenciliğin yeni bir versiyonu olarak değerlendirilip 'sanal dilencilik' kavramsallaştırılmasının kullanılması da söz konusu olmuştur.

Yardım kampanyalarında, yardım davranışının sergilenmesi için manevi değerlerin kullanılmaya çalışıldığı, kampanyaların ise kimi zaman bu değerlerin kullanılarak gerçekleştirilmesine rağmen istenmeyen sonuçlarının ortaya çıkabildiği sonucuna ulaşılmıştır.

1. YARDIM KAVRAMI VE TOPLUMSAL ÖNEMİ

Toplumsal bağlılık duygusu, bir toplumda ya da daha dar ölçekte bir toplulukta, toplumsal yapı arasındaki yardımlaşma ve dayanışmayı sağlayan, direnç ya da atılım gösterilmesinde itici güç olan temel unsurdur (Bozkurt, 2006, s. 25). Yani toplumsal bütünleşmenin en değerli bileşenlerinden birisinin toplumsal bağlılık duygusu olduğu söylenebilmektedir. Toplumsal bağlılık duygusunun oluşmasın-

da da kültür önemli bir belirleyicidir.

Kültür, bu yönüyle bakıldığında, bireylerin bazı değerleri kazanmasında ve kazanmış olduğu değerleri bireysel yaşantılarında konumlandırmalarında önemlidir. Bireylerin kültür aracılığıyla kazanmış olduğu adalet, sorumluluk gibi değerler de toplum içinde empati kurabilme kapasitelerini artırıcı bir özellik kazanmaktadır (Stilwell, 2001, s. 12). Cinsiyet, ırk gibi farklı özellikleri de barındıran kültürel ve sosyal faktörlerin, bireylerin duygularını nasıl ifade edeceği üzerinde de etki sahibi olduğu bilinmektedir (Stebnicki, 2000, s. 13). Bireyler, içinde doğup büyüdükleri ya da özümsedikleri toplumun değerleri üzerinden toplumsal cinsiyet kalıpları ya da değer yargıları geliştirme eğilimine sahip olabilmektedir. Bireyde yerleşmiş olan değerlerin aidiyet duygusuyla ilişkilendirilmesi de böylece mümkün hale gelebilmektedir.

Bu yönüyle incelendiğinde, bireylerin kendilerine yabancı olarak gördükleri kimselerle empati kurabilmesi görece daha zordur (Katz, 1963, s. 6). Bireylerin etnosentrik -yani kendilerinden olanı yüceltmeleri- yaklaşımının bu durumu körüklediği bilinmektedir (Katz, 1963, s. 21). Bu durumda, empatinin kurulabilmesinin önemli şartlarından birinin; bireylerin benzer kültürel özellikler taşıyan ortamlardan gelmesi olduğu söylenmektedir (Smith, 1996, s. 102). Empatinin yardım etme davranışıyla doğrudan ilişkisi olduğu da bilinmektedir (Schultz, 2001, s. 13). Bireylerin, yardıma ihtiyacı olan kişinin yerine kendisini koyabilmesi durumu, olayları onun perspektifinden değerlendirmesini ve yardım etme davranışı sergilemesini kolaylaştırmaktadır (İckes, 1997, s. 314).

Yapılan araştırmaların (Kalish, 1971; Kadushin ve Kadushin, 1990; Thakkar ve Kanekar, 1989) da bu durumu destekler nitelikte sonuçlar verdiği görülmektedir. Yardım etme davranışının empati kurabilmekle ilişkisi olduğunun bilinmesine ek olarak, bu davranışın nasıl gerçekleştiği ile ilgili de kuramsal açıklamalar (Thakkar ve Kanekar, 1989: s. 381-387) mevcuttur. Yardıma ihtiyacı olan kişiyle empati kurabilen kişinin, karşısındaki kişiyi ve durumu anlaması dolayısıyla sıkıntı duyması ve bu sıkıntıyı giderebilmek ve kendini rahatlatmak amacıyla da yardımda bulunması durumu söz konusu olabilmektedir. Dökmen'e (1997: 145) göre, karşısındaki kişiyle kurduğu empati sonucu yardım davranışı gösteren bireylerin, diğerkâm bir davranışla ve sıkıntıdaki kişiyi rahatlatmak amacıyla yardım davranışında bulunması durumu söz konusu olabilmektedir. Davranışlar

incelendiğinde birinci tip yardımın temelinde egoist bir güdünün, ikinci tip yardımın temelinde ise diğerkâm bir güdünün bulunduğu görülmektedir. Bireylerin yardımda bulunma davranışı pek çok araştırmaya konu edilen durumlardan biridir ve araştırmaların bir kısmı göstermektedir ki (Feldman, 1996, s. 435-436); yardım etme eğilimi, diğer insanların faydasından ziyade, yardımda bulunan kişinin kendisini rahatlatması açısından da önemlidir.

Bu noktada yardım davranışının bireysel etkilerinden ziyade toplumda görünüşünün ve temellerinin incelenmesi de önem kazanmaktadır. Durkheim'ın (2006, s. 163) da üzerinde durduğu mekanik ve organik dayanışmanın toplumdaki görünürlüğü önemli olan bir konudur. Küçük grupların bir arada yaşamakta olduğu, yüz yüze ilişkilerin yoğun olduğu, ortak geçmişin önemli yer tuttuğu ve toplumsal değişimin görece yavaş geliştiği topluluklarda mekanik dayanışmanın görüldüğü bilinmektedir. İş bölümünün çok fazla çeşitlenmemesi, bu toplumların belirleyici özelliklerinden biridir. Bireylerin benzer çalışma ve yaşam şartlarına sahip olduğu gözlemlenmektedir. Güçlü gelenekler, toplumsal dinamiklerin belirleyiciliği, toplumsal iletişim ve toplumsal kontrol mekanizmalarının gücü önemlidir. Diğer yandan ise, sanayileşme süreciyle birlikte değişen toplum yapıları sonrası; tarımsal yapıların çözülmesi sonucu yaşam merkezleri olarak kentlerin tercih edildiği bir görünüm ortaya çıkmıştır. Yüz binlerce insanın ortak mekânları paylaştıkları kentlerde, homojenlik yerini heterojenliğe bırakmış ve yüz yüze ilişkiler azalırken, uzmanlaşma hem çeşit hem de artış göstermiştir. Bu yeni toplumda da organik dayanışmanın örnekleri görülmektedir.

Yardım davranışının temelleri incelendiğinde; aidiyet duygusu, ortak kültürün paylaşılması gibi durumların görüldüğüne daha önce de değinilmiştir. Toplumun görece organik dayanışma türünde davranış gösteriyor olması, yardımlaşma kültürünün ortadan kalktığı anlamını taşımamaktadır. Bireylerin aidiyet duygusunun gelişmesi ya da gelişmiş olması için mutlak suretle yüz yüze ilişkilerin yoğun yaşanması durumu gerçekleşmek zorunda değildir. Tarihsel olarak incelendiğinde de yardımlaşmanın farklı biçimlerinin toplumların geçmişlerinde her zaman görüldüğü ortaya çıkmaktadır. Türk toplumsal yaşamında da sosyal yardımlaşmanın tarihin eski zamanlarından beri önemli bir yer tuttuğu bilinmektedir. M.Ö. 3000 yıllarında Orta Asya'daki Türklerin kurmuş olduğu vakıflar, bu durumun önemli örneklerinden biridir. Vakıfların kurulmasındaki amacın bir çeşit sosyal güvenlik kurumunun oluşturulması ve o zamanki kültürün önemli

bir öğesi olan hayvanların korunması olduğu görülmektedir. Cengiz Han yasalarında yoksulların ve yaşlıların korunmasına yönelik önlemler görülmektedir. 4. yüzyılda da Anadolu'da düşkün, yaşlı, hasta, öksüz ve yetimler ile öğrencilere yapılan yardımlardan da söz etmek mümkündür (Şeker, 2008, s. 44-45).

Sosyal dayanışmanın en temel ahlaki amaçlarından birinin, bireylerin şerefli ve haysiyetli bir varlık olmasından kaynaklı olarak, herkesin şahsiyetli bir hayat sürdürebilmesi olduğu görülmektedir. Böylesi bir hayat sürdürülebilmesi için karşılıklı yardımlaşmanın önemli bir unsur olduğu sonucuna ulaşılabilmektedir (Seyyar, 2008, s. 416).

2. DİJİTAL PLATFORMLARDA BİREYLER VE İLİŞKİLER

Bireylerin yüz yüze ilişki içindeyken, iletişimin çok boyutlu yönlerini kullanabilmek konusunda daha fazla imkâna sahip olduğu bilinmektedir. İletişim içinde bireylerin birbirlerine mesaj gönderdiklerinde, mesajların içinde kelimelerin, sembollerin ve hatta mimiklerin de iletilmesi söz konusudur. Daha önce bahsi geçen empatinin kurulabilmesi için bu unsurların aynı anlamı ifade etmesi de iletişim konusunda ciddi bir kazanımı beraberinde getirebilmektedir. Empatik iletişimin gelişmesi için bu ortak unsurlar önemli bir yer tutmaktadır (Katz, 1963, s. 33). Ancak durum, bu noktada birtakım değişimler göstermektedir. Gelişen teknolojinin bireylerin birbirlerine seslerinden ziyade görüntülerini video formatında ve anlık olarak aktarabilmesine de imkân tanımaktadır. Böylece bireyler, fiziki olarak aynı mekânı paylaşmıyor olsalar da kapsamlı bir iletişimin içinde olabilme fırsatını yakalayabilmektedir.

Bireyler, yüz yüze iletişimde iken duygu ve düşüncelerini karşı tarafa aktarabilmek için pek çok durumdan eş zamanlı olarak faydalanabilmektedir. Ses tonu, jest ve mimiklerin duygu ve düşüncelerin aktarılmasında, iletişimi destekleyen unsurlardır ancak mesafeler arası iletişimde duygu ve düşüncelerin aktarımı konusunda yaşanan zorluğun üstesinden gelebilmek için bireyler, 'emoji' adı verilen sembolleri kullanmaktadır (Toksöz ve Kahraman, 2017, s. 248). Emojiler, mesajı alan kişinin, mesajı gönderen kişinin jest ve mimiklerinin ne/nasıl olduğunun, anlık olarak görselleştirebilmesi için yardımcı konumunda yer almaktadır. İmgelem yardımıyla sembolik unsurların desteğinin alınması, empatiyi güçlendirebilen bir unsur olarak karşımıza çıkmaktadır.

Kapitalizmin birikime dayalı üretim anlayışının, toplumsal birer aktör olarak bireylerin yaşantılarında da birtakım değişikliklere sebep olduğu bilinmektedir. Bireylerin birbirleriyle olan toplumsal ilişkilerinde bile 'altyapının' izlerini görmek mümkün hale gelmiştir. Eskiden karşılıklı konuşma ve anlayışla kazanılan ortak değerlerin bir kısmının kaybolmaya yüz tuttuğu görülmektedir. Bireylere mutlu olmak için para kazanmaları gerektiği telkin edilmektedir. Bu durum, bireyleri para kazanmaya zorlarken, aile ve çevrelerine ayıracakları zamanında da azalmasına sebep olmaktadır. İnsan ilişkileri dâhil olmak üzere, bireyler için her şey tüketilebilecek bir meta haline dönüşmektedir (Öztürk, 2013, s. 102). Ancak bununla birlikte, bireylerin salt insan olmasından ve içinde yaşadığı toplumun değerlerini taşıyor olmasından kaynaklı olarak da değerlerini sürdürme istek ve davranışları gözlemlenebilmektedir. Özellikle toplumsal olayların anlamlandırılmasında kullanılan mekân kavramının, sadece fiziksel araçlarla değil aynı zamanda toplumsal ilişki örüntülerini anlamlandıran ve onlarla anlam bulan bir yapı sergilediği de unutulmamalıdır (Birekul, 2015, s. 101). Mekânsal birliklerin sadece fiziki birliktelikler olmadığı; aynı zamanda manevi unsurların en güçlü şekilde aktarımının aracısı olduğu söylenebilmektedir.

Her şeyin dönüştüğü dünyada, hayatımızı sarmış durumda olan şeylerin hepsinin de sanal ön eki alarak yeni bir toplumsal gerçeklik inşa ettiği görülmektedir. Bu yeni oluşuma 'paralel dünya' adlandırması da yapılabilmektedir. Paraların, mekânların, zamanların, kimliklerin ve hatta cemaatlerin sanal ön ekiyle yeniden tanımlandığı yeni oluşumda sanal tipolojilerin sınıflamasını yapmak da mümkün hale gelmiştir. Bu yeni oluşum sadece kavramsallaştırmada da kalmayıp 'e-' ön eki alarak günlük yaşantımızın her kademesinde görünür olmaya başlamıştır. E-ticaret, e-imza, e- kimlik ya da devletin kullanmış olduğu en büyük sanal mecra olan e-devlet hayatımızda yer almaya başlamıştır. Bireylerin de eylemlerini gerçekleştirdikleri yeni davranış örüntülerinden yola çıkarak, çağımızın insanına dijital insan demek mümkün hale gelmiştir (Timisi, 2005, s. 89). Sanal ön eki ya da farklı kavramsallaştırmalarla sosyal platformlarda yapılan işlemler, gerçek yaşantımızı etkiler hale gelmiştir. Hatta gerçek kurumlardaki işlemleri sanal platformlar aracılığıyla çözebilmek, bireylere büyük kolaylıklar sağlamaktadır.

Sosyal medya çalışmalarının günümüzde sayısı giderek artmaktadır. Sosyal medya platformlarından olan Facebook ile ilgili yapılmış bir çalışmada (Ersöz Günindi, 2016, s. 308), bireylerin profillerini sıklıkla düzenledikleri, yeni yazı-

lar yazdıkları, paylaşılan ve beğenilen fotoğraflarına özen gösterdikleri sonucuna ulaşılmıştır. Bireylerin paylaştıkları fotoğraflarda görünüşlerinden ziyade fotoğrafların diğer kullanıcılarda nasıl bir izlenim uyandırdığına odaklandıkları sonucuna ulaşılmıştır. Bunda kullanıcıların, sürekli olarak izlendiğini bilmeleri etkin rol oynamaktadır. Böylece bireyler, diğer kullanıcıların gözünde bazı özelliklerini öne çıkarabilirken, istemedikleri özelliklerini saklayabilmektedir. Kişilerin diğer kullanıcılara 'ben mutluyum' mesajını verebilmekte ve hatta gittikleri yerlere ait konumlarını paylaşarak da 'ben sosyalim' mesajını iletmektedir.

Simülasyon ve simülakr kavramlarıyla çözümlemeler yapan Baudrillard'ın tespitleri, günümüz sosyal mecralarında yürütülen sosyal ilişkilerde ve görünümlerde bir karşılık bulabilmektedir. Ona göre gizlemek (dissimuler), hâlihazırda bireylerin sahip oldukları şeylere sahip değilmişçesine davranmayı gerektirmektedir. Ancak simüle etmek bireylerin gerçekte sahip olmadıkları şeylere, sahipmiş gibi yapmasıdır. Birinci kavram esasen varlığa; ikinci kavram ise yokluğa gönderme yapmaktadır. Kavramlar biraz derine inilerek incelendiğinde simüle etmenin yalnızca basit bir '–mış gibi yapmak' olmadığı anlaşılmaktadır. Bu durumu açıklamak için hasta birey üzerinden bir anlatım gerçekleştirilebilmektedir. Bir birey hastaymış gibi yaptığında uzanarak diğerlerini hasta olduğuna inandırmaya çalışmaktadır. Ancak bir birey hastalığı simüle etmeye karar verdiğinde, kendisinde bu hastalığa ait semptomların da görülme ihtimali çok yüksektir (Baudrillard, 2017, s. 16).

3. DİJİTALLEŞEN YARDIM

Günümüz toplumlarında teknolojik gelişmelere bağlı olarak bireylerin yaşantıları birkaç on yıl önceye göre büyük ölçüde değişmiştir. Sosyal ilişkiler yerini sanal sosyal ilişkilere bırakırken, günlük yaşantılarımızda da teknolojik aletlerin her anlamda hayatımızda daha fazla yer kapladığı ve bu durumun çoğalarak varlığını sürdürdüğü görülmektedir.

İletişimin bu gelişimine ek olarak toplumsal yapıdaki değişimlerin de değerlendirilmesi gerekmektedir. Teknolojik gelişmelere paralel olarak toplumların pek çok alanda gelişim gösterdiği bilinmekle birlikte, toplumsal yapı içindeki dayanışma türlerinin de mekanikten organiğe doğru bir değişim gösterdiği ve hatta organik dayanışmanın mekanik dayanışma üzerinde hâkimiyet kurduğu görül-

mektedir (Öztürk, 2013, s. 102). Bu durumun, günümüz tüketim biçimleriyle de doğrudan ilişkili olduğu söylenebilmektedir.

Bireylerin toplumsal bir varlık olarak toplum içinde gerçekleşen birtakım durumlara kayıtsız kalmadığı bilinmektedir. Doğal ya da doğal olmayan birtakım olaylar sonucu, bireylerin yaralanması, ölmesi ya da mallarına ve mülklerine zarar gelmesi sonucu ilk yardım ve kurtarma ekiplerinin yetersiz kalması durumu (Kasapoğlu ve Ecevit, 2001, s. 1) zaman zaman görülebilmektir. Sadece bununla da kalmayıp aynı zamanda bireylerin maddi yetersizlikler sonucu birtakım sağlık hizmetlerinden yararlanamama durumları da ortaya çıkabilmektedir. Bireylerin eskiden bu yana engelliler, yoksullar, kimsesizler ya da pek çok farklı alanı da işaret edebilen güçsüzlere ve toplum içinde çeşitli imkân ve hizmetlerden yeterince faydalanamayan mağdurlara yardım ettikleri gözlemlenmektedir. Bazı bireylerin de başka bireylerin ilgi ve bakımına muhtaç hale gelmesi söz konusu olabilmektedir (Yolcuoğlu, 2014, s. 57). Böyle durumlarda bireyler yakın çevrelerinden başlayarak birtakım yardım isteklerinde bulunabilmektedir. Bu durumlar için devlet destekli yardımların edinilmesi de mümkün olabilmektedir. Ancak kimi zaman daha büyük çapta yardımların yapılması gerekliliği de doğmaktadır.

Bu noktada, finansman kanallarının yeni bir biçimi olarak karşımıza çıkan kitlesel fonlama platformaları da gündeme gelmektedir. Kitlesel fonlamanın bilgi sistemlerine ek olarak girişimcilik uygulamalarının aktif bir biçimde çalışmasına ek olarak yardım kampanyalarına olan destekleri de bilinmektedir (Sakarya ve Bezirgân, 2018). Kitlesel fonlamanın daha kısa zamanda daha büyük yardımlar yapabilmesi durumu söz konusu olabilmektedir.

Dijital teknolojiler çok fazla zıtlığı bünyesinde barındırmaktadır. Merkeziyetçi olmadığı düşünülen bilgi ve iletişim yapısında ağların oluşumları, düzenlenmesi ve yeniden üretilmesi hem herhangi bir sınıra tabi tutulmaksızın hem de çok hızlı bir biçimde gerçekleşmektedir. Hareketler bu açıdan bakıldığında kişiselleştirilebilir bir yapı ve aynı zamanda daha az kontrol edilebilir bir görünüm sergilemektedir. Dijital teknolojilerin bu özellikleri göz önünde bulundurularak değerlendirildiğinde, bir seçim kampanyasından işgal hareketlerine kadar pek çok eylemi kapsar bir nitelik taşıyabilecek potansiyele sahip oldukları görülmektedir (Gerbaudo, 2017, s. 478). Bu açıdan bakıldığında dijital ağlar aracılığıyla hem görünür hem de görünmez olmak mümkün olmaktadır. Bireyler günlük yaşantılarında da

yardım davranışı sergilerken, görünür olma ya da görünmez olma durumundan faydalanmaktadır.

Sosyal medyada oluşan çevrimiçi toplulukların bir araya gelme biçimleri; planlı ya da plansız topluluklar olarak ayrılmıştır. Bu ayrıma göre bir plan dâhilinde ve bir tarih ya da kimliği olan taraftar kulüpleri gibi topluluklar planlı topluluklardır. Ancak birdenbire ortaya çıkan, bir plan dâhilinde gelişmeyen ve genel olarak geçici bir süreliğine ya da isimsiz olarak belli bir amaç ya da konu için ortaya çıkan topluluklar da bulunmaktadır. Bir yardım kampanyası için herhangi bir 'hashtag' olarak da nitelendirilen başlık etiketi altında birleşen bireylerin oluşturduğu topluluklar bu tür topluluklardır ve plansız topluluklar olarak anılmaktadır (Eren Çetin ve Ayhan, 2020, s. 53). Plansız topluluklar aracılığıyla herhangi bir olaya, duruma, düşünceye katılım davranışı, çevrimiçi platformlarda gözlenmektedir.

Yapılan bir çalışmada (Eren Çetin ve Ayhan, 2020, s. 58); kullanıcıların katılım gösterme davranışının belirli biçimlerde ortaya çıkabileceği saptanmış ve bu biçimler, 4 farklı başlık altında toplanmıştır. Bu çalışmaya göre sosyal medya platformlarında kullanıcılar; doğrudan katılım (içerik üreterek), dolaylı katılım (duyurarak), sabit katılım (beğenerek), pasif katılım (sadece takip ederek) davranış sergilemektedir.

Bireylerin yardım kampanyalarına katılım davranışları da yukarıda sayılan katılma biçimlerinin tümünde görülebilmektedir. Kullanıcıların özellikle toplumsal olaylar söz konusu olduğunda sanal mecralarda takınmış olduğu tavırlar başka çalışmalara da konu edilmiştir. Örneğin, 'slaktavizm' kavramsallaştırılmasının yapıldığı çalışmada (İnceoğlu ve Çoban, 2015, s. 52), bu kavram; internet aracılığıyla gerçekleştirilen imza kampanyalarına katılmak ya da kullanıcıların profillerinde yer alan fotoğraflarını, kişisel bilgi ya da ilgi alanlarını güncellemek suretiyle sanal etkinliklere destek vermelerini içeren eylemler ile açıklanmaktadır. Bu eylemlerde kampanyalara destek sağlanmaktadır, daha fazla insana ulaşabilmesi için eylemler gerçekleştirilmektedir, ancak kullanıcılar sandalyelerinden bile kalkmadan bu eylemlerde bulunmaktadır. Yegen'e göre (2015, s. 52), kavramsallaştırmanın çıkış noktası da tembel ve aktivizm kelimelerinin seçilmesidir. Kavramın, 'Tembel eylemcilik' olarak anıldığı da görülmektedir. Yine benzer bir kavramsallaştırma kliktivizm kelimesiyle yapılmaktadır ve tıklayarak eylem gös-

teren bireyler, bu kavramsallaştırmaya konu edilmektedir (Tarhan, 2013).

Bireylerin sosyal medyada oluşturmuş ve bireylere göstermekte oldukları kullanıcı profilleri tamamen kullanıcının istekleri doğrultusunda olmaktadır. Bireyler kimliklerini isterlerse gizli, isterlerse de açık olarak kullanmaktadır. Toplumsal olarak arzulanan kimliklere sahip olmak için, bireyler kimliklerini gizleme ihtiyacı da duymaktadır (Turkle, 1995, s. 7). Yani bireyler gerçek isim ve kimliğiyle ya da tamamen hayali bir kullanıcı adı ve profiliyle de sosyal medyada bulunabilmektedir. Esasen incelenmesi gereken bir başka durum, bireyler gerçek isim ve kimlikleriyle var oldukları platformlarda gerçekten kendi benliklerini mi sunmaktadır yoksa daha önce de değinilmiş olduğu gibi görünmesini istediği ve kendileri tarafından oluşturulmuş olan profille mi var olmaktadır? Konuyu bu açıdan ele alan bir başka çalışmada (Nguyen, 2017, s. 34), katılımcıların kendi profillerindeki fotoğraflardan zaman zaman rahatsızlık duyduklarını ve onları silmeyi tercih ettikleri sonucuna ulaşılmıştır. Kullanıcıların amacı, kötü anıları çağrıştıran hatırlatıcılardan kurtulmak ve kişisel vitrinlerinin mükemmel görünmesi yönündeki istekleridir. Sosyal medyada kullanıcıların inşa etmiş oldukları kimliği yeniden düzenlemek de kendi ellerindedir.

4. ARAŞTIRMANIN YÖNTEMİ: DİJİTAL YARDIM KAMPANYALARININ GÖRÜNÜMLERİ

Bireylerin ve kurumların farklı şekillerde ve gerekçelerle yardım kampanyaları başlatmaları, teknolojik gelişmelerden bağımsız bir durumdur. Geçmişten bugüne bireyler ve kurumlar, yardıma ihtiyacı olduğunu düşündüğü kişiler ya da -çeşitli sebeplerle- kendileri için yardım talebinde bulunabilmektedir. Günümüzde ise, bu durumun toplumdaki görünürlüğünün şekil değiştirdiği gözlemlenmektedir. Artık bireyler ve kurumlar, bilişim teknolojilerinden faydalanarak herhangi bir konu için, kapsamlı kampanyalar başlatabilmekte ve bu kampanyalar çok geniş yankı uyandırabilmektedir.

Bu araştırmanın amacı, öncelikle dijital yardım kampanyalarının incelenmesidir. Bu kampanyaların sosyal medyaya ve basına yansıyan görünümleri çözümlenirken, bireylerin ve kurumların genel olarak hangi sebeplerle ve ne şekilde dijital yardım kampanyası başlattıkları ve yürüttükleri incelenecektir. Başlatılan kampanyaların incelenmesi konunun ana odağını oluşturduğu için, özellikle sos-

yal medya üzerinden yürütülen kampanyaların sloganları, afişleri ya da görselleri ve basına yansıma şekilleri incelenmeye değer bulunmuştur. Bu noktada özellikle, yardıma ihtiyacı olanlara sağlanan destekler ve bu desteklerin sosyal devlet anlayışı çerçevesinde gerçekleşmesinden ziyade, günümüzün bir gerçekliği olan dijital yardım kampanyalarının incelenmesi temel amaç olarak belirlenmiştir.

Araştırmada bu sebeple içerik analizinden faydalanmak gerekliliği doğmuştur. Sosyal eylemlerin genellikle sadece gerçekleştirilen eyleme anlam veren kavram, kural, gelenek ve inançlarla açıklanamayacağı, bunların içinde bulunduğu kültürel sistemin de yorumlanması gerektiği fikri (Neuman, 2014, s. 134-136; Kuyucuoğlu, 2015, s. 682) de merkeze alınarak yorumsamacı bir yaklaşım kullanılmıştır. Dijital olarak başlatılan ve sürdürülen yardım kampanyaları tespit edilmiş ve bu kampanyalar arasından çalışmanın kurgulanma biçimine uygun olanlar seçilmiştir. Seçim yapılırken, amaçlı örneklemeden faydalanılmıştır. Yardım kampanyalarının seçilmesinin öncelikli kriteri, bireysel ya da kurumsal başlatılma durumu olarak belirlenmiştir. Ardından bireysel kampanyalardan da basında yer bulmuş olanlar tespit edilerek süreç, derinlemesine incelenmiştir. Çözümlemeler yapılırken, kampanyanın duyurulmasını sağlayan görseller, dil ve içerik açısından dikkate alınmıştır.

4.1 Veri Toplama Süreci

Araştırmanın verilerinin toplanabilmesi için öncelikle sosyal mecralara ve basına yansıyan yardım kampanyaları tespit edilmiştir. Kampanyalar bir araya getirildikten sonra kampanyanın başlatıldığı gerekçeler ve kampanyaları başlatan kişiler ya da kurumlar çözümlenmiştir. Kampanyaların çeşitli gerekçelerle gerçek ya da tüzel kişiler tarafından başlatıldığı sonucuna ulaşılmış ve bulgular "Kurumsal Kampanyalar" ve "Bireysel Kampanyalar" şeklinde iki ayrı tema çerçevesinde incelenmiştir.

Bu kampanyaların ne zaman başladığı ve ne kadar sürdüğü ulaşılan veriler değerlendirilerek tespit edilmiştir. Kurumsal kampanyalarda bu noktada sıkıntı yaşanmasa da bireysel kampanyalarda, kurumsal kampanyalarda ortaya çıkmayan birtakım sıkıntılar tespit edilmiştir. Bireysel kampanyalarda ilk paylaşımı yapan hesaba ulaşılmaya çalışılmıştır ancak ilk hesabın kapatıldığı ya da gönderilerin silindiği durumlarda basında çıkan haberler kullanılmıştır.

Veriler toplanırken, özellikle her yardım kampanyasının çok yönlü incelemesinin gerçekleştirilebilmesi için ele alınan kampanyalar, kurumsal kampanya temasında incelenebilecek 5 adet kampanyayı ve bireysel kampanyalar temasında incelenebilecek 4 adet kampanyayı kapsayacak şekilde kısıtlı tutulmuştur. Çalışmada yer alan yardım kampanyalarıyla ilgili görseller incelenmiştir. Ancak görsellerin bir kısmında sadece kampanya isimleri ve iletişim numaraları bulunuyorken, özellikle bireysel kampanyalara ait elde edilen görsellerin, kampanya için özel ve profesyonel biçimde hazırlanmış olan görseller olmadığı görülmüştür. Bu sebeple, kampanyanın sosyal medyada kullanıldığı şekliyle bu görseller çalışmaya dâhil edilmemiştir. Bu durum, verilerin bir program aracılığıyla çözülmesinin önünde de bir sınırlılık olarak değerlendirilmiştir. Kampanyaların sunuş biçimleri dolayısıyla kullanılan dili de çözümleyebilmek ve her bir kampanyayı kendi içinde detaylı olarak inceleyebilmek gerekçesiyle de analizler, bir program aracılığıyla gerçekleştirilmemiştir. Bu sebeple istatistiki veri sunabilmek mümkün olmamıştır.

4.2 Veri Değerlendirme Süreci

Görsellerin, haberlerin ve süreçlerin incelendiği bu çalışmada, amaçlı örneklem tekniği ile seçilmiş kampanyalar incelenmiştir. Amaçlı örneklem, araştırmada belli niteliklere sahip kişiler, olaylar, nesneler ya da durumlara göre bir seçim yapılacaksa kullanılmaktadır (Büyüköztürk, vd., 2009: 91). Elde edilen veriler, içerik analizi yöntemi ile çözümlenmiştir. İçerik analizi, "iletilerin açık olan içeriğinin nesnel ölçülebilir ve doğrulanabilir bir açıklamasını yapabilmek amacıyla kullanılmaktadır" (Fiske, 1996: s. 176). Bu yöntem, özellikle bilgisayar destekli içeriklerin çoğalmasına paralel olarak sayıca fazla olan ve hacimli içeriklerin daha sistemli ve kolay biçimde incelenmesine imkân sağlamaktadır (Yıldırım, 2015: s. 116).

Veri toplama süreci Haziran 2022 ile Ağustos 2022 tarihleri arasında gerçekleştirilmiştir. Yardım kampanyalarının iki değişken üzerinden incelenmesi esas alınmıştır. Bunlardan birincisi kurumsal olarak başlatılan ve bakanlıklar, belediyeler gibi kurumsal kimlik çatısı altında başlatılmış olan kampanyalardır. İkincisi ise, tekil kullanıcılar ya da herhangi bir tüzel kişiliği olmayan gruplar tarafından başlatılmış olan ve herhangi bir valilik onayı ya da izni olmayan kampanyalardır.

Dijital yardım kampanyalarının incelendiği bu çalışmada, dijital yardım kampanyasını başlatan kişi ya da kurumların kullanmış olduğu dil de inceleme kapsamına alınmıştır. Özellikle sloganlarda hangi kelimelere vurgu yapıldığı ve bağışları talep ederken sunmuş oldukları gerekçeler derinlemesine incelenmiştir. Çok yönlü analiz gerçekleştirebilmek için de kampanyaların basındaki sunuş şekillerinden de faydalanılmıştır. Değerlendirmeler gerçekleştirilirken, kampanyaların hedefine ulaşıp ulaşmadığı, yardımları hangi kanal aracılığıyla talep ettiği ve topladığı, süresi, sonuçları detaylandırılmaya çalışılmıştır.

4.3 Araştırmanın Bulguları

Yapılan taramalarda dijital yardım kampanyalarının başlatılması için birden fazla sebebin kullanıldığı görülmektedir. Çözümleme yapılırken, başlatılan kampanyaları kurumsal ve bireysel kampanyalar olarak kategorize etmek uygun görülmüştür. Kurumsal kampanyalar konusunda olumsuz bir duruma rastlanıldığıyla ilgili hiçbir veriye ulaşılamazken; bireysel kampanyaların kimi zaman resmi izinler alınmadan yapılabildiği ve bu sebeple herhangi bir denetime tabi olmadığına da bağlı olarak yardımların yerine ulaşmaması sonucunu beraberinde getirdiği de görülmektedir.

Tablo1. Yardım Kampanyaları ve Nitelikleri

Kurumsal Kampanyalar	Bireysel Kampanyalar
Biz Bize Yeteriz Türkiyem	Gökalp'in Kahramanı Sen Ol
Birlikte Başaracağız	Ramazan'a Kol Kanat Olalım
Bilgisayar Tablet İnternet Destek Projesi	Asude Defne Özkan
Kalbe Dokun Gönül Kazan	sma_tip1mirbahattin
Bir Aradayız İdlib'in Yanındayız	

4.3.1 Dijital Kampanyalar

4.3.1.1 Biz Bize Yeteriz Türkiye'm

Covid-19 salgını sırasında kurumsal yardım kampanyalarının başlatıldığı görülmektedir. Bu kampanyaların en büyüğü; Aile, Çalışma ve Sosyal Hizmetler bakanlığı tarafından başlatılan "Biz Bize Yeteriz Türkiye'm" kampanyasıdır. Bu kampanya, bizzat Cumhurbaşkanı tarafından açıklanmış ve süresiz olarak başlatılmıştır. "Biz Bize Yeteriz Türkiye'm" kampanyasının görselinde sadece bağışta bulunabilmek için gerekli olan iban numaraları ve kampanyaya kısa mesaj aracılığıyla destek olmak isteyenler için gerekli kısa mesaj numarası yer almaktadır. Kampanya hakkında bilgi alınabilecek herhangi bir iletişim numarası ya da web sitesi adresi görülmemektedir. Ancak bu kampanyada sosyal medyada etiketleme yapılabilmesi için slogan; (#) hashtag ile yazılmıştır. Kampanyaya ait sloganın kullanıldığı ve kurumsal uzantılı (bizbizeyeteriz.gov.tr) bir web sitesi bulunmaktadır. Bu web sitesinde de kampanyaya ait bağış bilgilerinin düzenli aralıklarla düzenlendiği verisine ulaşmak mümkündür. Kampanyaya ait görsel aşağıda yer almaktadır.

Kampanyanın afişinde Türk Bayrağı'nın kullanılması aidiyet hissine yapılan bir vurgu olarak değerlendirilebilmektedir. Slogan seçilirken de "biz" kelimesinin özellikle tercih edildiği düşünülmektedir. Bu kelimenin seçimi, birlik ve beraberliğin vurgulanması ve aidiyet hissinin güçlendirmesini de beraberinde getirebilmektedir. Bir salgın karşısında bireylerin birbirlerine yetiyor olma durumu bütünleşmeyi de sağlayan bir durum olarak değerlendirilebilmektedir.

Kampanyanın, ekonomik durumu yeterli olan vatandaşların yapmış olduğu bağışların, salgın süresince ekonomik olarak zor duruma düşen vatandaşlara destek olması sistemiyle ortaya çıktığı söylenmektedir. Kampanyanın, devleti temsilen cumhurbaşkanlığınca başlatılmış olması, güven duygusunu besleyen bir durum olarak değerlendirilmektedir. Bunu da kampanyaya yapılan yardım miktarlarının büyüklüğüyle ölçmek mümkündür.

Yapılan bir araştırma (Bilgiç ve Seferoğlu, 2020, s. 55) da benzer sonuçlara ulaşarak, çevrimiçi platformlarda düzenlenen yardım ve imza kampanyalarının, duyarlı bir yurttaş olma potansiyelini yansıtma ve erken yaşta duyarlı yurttaş olma olgusunun farkına varılmasına araç niteliğinde olduğunu vurgulamaktadır. Bahsi geçen çalışmada, bireylerin yardım davranışı konusundaki motivasyonlarına değinilmesi, bu çalışmadan ayrılan en önemli noktalardan biridir. Dijital kampanyalara katılımın, vatandaşlık üzerinden çözümlemesinin yapılması da önemli bir diğer noktadır. Bireylerin, devlet eliyle başlatılan kampanyalara katılım davranışı sergilemesi, katılımın hangi türü olduğu fark etmeksizin, sürdürülebilir bir sosyal sorumluluk anlayışını da beraberinde getirmektedir.

4.3.1.2 Birlikte Başaracağız

Kurumsal kampanyalardan sayılabilecek olan "Birlikte Başaracağız" sloganıyla başlatılan kampanya, İstanbul Büyük Şehir Belediyesi tarafından başlatılmıştır. Bu kampanya Covid-19 salgınından sonra bölgesel çapta ve süresiz olarak başlatılmıştır. Ancak sosyal medya gücüyle duyurulan kampanyaya desteğin bölge çapıyla sınırlı kalmadığının hedeflendiği görülmektedir. Kurumsal yerel yönetim hesabı kullanılarak başlatılan kampanyada insan nüfusuna yapılan vurgu dikkat çekmektedir. Öne çıkarılan ana düşünce, toplumsal bazda birliktelik, dayanışma ve bütünleşme sağlanmasıdır. Birbirlerine uzatılan iki el ile sembolize edilen ve kampanya görselinde yer alan görselin altında "#" (hashtag) kullanılarak kam-

panyanın adının yazıldığı görülmektedir. Bu durum, kampanyanın sosyal medya platformlarında bu etiket altında konuşulmasının da hedeflendiğinin önemli bir göstergesidir. Kampanya afişinde hem iletişim numaraları hem de iban numaralarının verildiği görülmektedir. Kampanya 30 Mart 2020 tarihinde başlatılmıştır. Görselde yer alan ve kurumsal uzantılı web sitesinde hem kampanyaya katkı sağlamak isteyenler hem de kampanyadan faydalanmak isteyenler için çevrimiçi başvuru sistemi oluşturulmuş ve kampanyaya ait verilerin anlık olarak sunulduğu görülmektedir. Kampanyaya ait görsel aşağıda yer almaktadır.

Kampanyanın afişinde farklı meslek mensupları oldukları düşünülen 11 kişiye yer verilmiştir. Çocuklar, yetişkinler ve yaşlıların yer aldığı afişte, bireylerin hepsinin güler yüzlü olduğu dikkat çekmektedir. "16 milyon İçin Çalışıyoruz" sloganı kalp içinde yazılmış ve bir duygu bağı kurulmayı hedeflediği düşünülmektedir. Bu kampanyada da "birliktelik" en önemli vurgu odağı olmuştur. Başarmak kelimesi de bir ekip gibi bir zorluğun üstesinden gelinmesine işaret eden bir durumdur ve aidiyet hissini pekiştirecek kelimelerden biri olarak karşımıza çıkmaktadır. Vatandaşların, bu kampanyaya da güven duydukları, yapılan yardım miktarlarıyla anlaşılabilecek bir durum olarak değerlendirilmektedir.

4.3.1.3 Bilgisayar Tablet İnternet Destek Projesi

Dijital yardım kampanyalarının belli bir konu odaklı olarak başlatılanları da mevcuttur. Bunlardan biri, Devrek Kaymakamlığı ve İlçe Milli Eğitim Müdür-

lüğü tarafından ortak başlatılan "Bilgisayar Tablet İnternet Destek Projesi"dir. Kampanya 05 Ekim 2020 tarihinde ve süresiz olarak başlatılmıştır. Kampanyaya ait görselde birden fazla slogan kullanıldığı dikkat çekmektedir. Kampanya duyurulurken "Tableti Olmayan Öğrenci Kalmasın", "Uzaktan eğitime erişemeyen öğrencilerimize tablet, bilgisayar, internet paketi sağlayarak engelleri birlikte kaldıralım" ve "Mutlu çocuklar için sorumluluk al!" ifadeleri yer alıyor olmasına rağmen, sosyal medyada gündem oluşturabilmek için planlanmış bir hashtag bulunmamaktadır. Ancak görselde iban numarası verilmiştir. Dijital yardımların en büyük yayılma alanı sosyal mecralardır ve sosyal mecralarda yayılımın hızı hashtagler aracılığıyla sağlanmaktadır. Bu açıdan kampanya için hashtag oluşturulmaması, geniş kitlelere ulaşmasının önünde bir engel gibi görülmektedir. Ayrıca görselde sadece Devrek Kaymakamlığı'na ve Devrek İlçe Milli Eğitim Müdürlüğü'ne ait olan web siteleri ile Devrek Milli Eğitim Müdürlüğü'nün Twitter hesabının bağlantıları paylaşılmıştır. Yardımların anlık ya da düzenli olarak takip edilebileceği bir web sitesi tasarlanmamıştır. Bu tasarımın sağlanması, güvenilirlik açısından katkı sunabilecek mahiyettedir. Görselde kullanılan fotoğrafta gülümseyen 3 tane çocuğa yer verildiği görülmektedir. Çocukların kampanya sonucunda tablete ulaşabilmesi slogandan da anlaşılabileceği gibi mutluluk olarak düşünülmekte ve hedef kitleye sorumluluk yüklendiğinin ifadesiyle birlikte yardım yapma davranışı göstermeleri için motive etmeyi amaçladığı düşünülmektedir. Bireylerin kendileri için sorumluluk alabileceği kişilerin, aidiyet hissettiği kişiler olduğu ön kabulüyle, bu kampanya da "birlik" duygusuna yapılan vurgu dikkat çekmektedir. Kampanyaya ait görsel aşağıda yer almaktadır.

Bu kampanyanın da devlet kurumları olan kaymakamlık ve milli eğitim müdürlüğü tarafından başlatılmış olması, yerel olarak başlatılmış olsa da bireylerin, kampanyaya ilgi göstermesini sağlayan unsurlardan biri olarak değerlendirilmektedir. Bireylerin, yapılan yardımların, devlet kurumları tarafından yine vatandaşlar için kullanılacağını düşünmesi, bu kurumlara duyulan güveni de besleyebilecek potansiyel taşımaktadır. Yani esasen, kampanyaların devlet kurumları tarafından başlatılması başlı başına güvenin oluşmasını sağlarken, vatandaşların devlet kurumları aracılığıyla yardım alıyor olması bu kurumlara olan güveni artırma potansiyelini de taşımaktadır.

Bu tür devlet destekli yardım kampanyaları, dünyadan çeşitli örnekleri de barındırmaktadır. Örneğin Belçika'da hükümet pandemi sürecince on iki bin beş yüz öğrencinin uzaktan eğitimden faydalanabilmesi için dizüstü bilgisayar kampanyası başlatmıştır. Hükümetin de iki yüz bin Euro katkı sağlamış olduğu kampanyaya birçok kurum destek vermiştir (Sözen, 2020: s. 312).

4.3.1.4 Kalbe Dokun Gönül Kazan

Dijital Yardım kampanyalarından eğitim desteği içeren ve kurumsal kampanyalardan bir diğeri; "Kalbe Dokun Gönül Kazan" kampanyasıdır. "Askıda Tablet" sloganını da kullanan kampanyayı, Gaziantep Valiliği; Büyükşehir Belediyesi, Şehitkâmil Belediyesi, Şahinbey Belediyesi, Gaziantep Sanayi Odası, Ticaret Odası, Güneydoğu Anadolu İhracatçı Birlikleri (GAİB), Ticaret Borsası, Organize Sanayi Bölgesi ile Esnaf ve Sanatkârlar Odaları Birliği ile organize etmiştir. Kampanya 21 Eylül 2020 tarihinde başlatılmış, 100.000 tablet hedefini belirlemiştir. Covid-19 sürecinde uzaktan eğitime geçilmesinden kaynaklı olarak alt yapı eksiklikleri sebebiyle benzer birçok kampanyaya rastlanmıştır. Kampanyada birden fazla slogan yer almaktadır. "Askıya bir tablet de sen koyarsan hiçbir öğrencimiz eğitimden geri kalmayacak" ifadesi dikkat çekmektedir. Bu kampanyaya ait sosyal medya etiketlemesi kullanılmıştır. Kampanya görselinde "#gönülseferberliği" hashtag'inin görülüyor olması, kampanyadan sosyal medya aracılığıyla da yardım beklendiğinin göstergelerinden biridir. Gaziantep Sosyal Yardımlaşma ve Dayanışma Projesi'nin iban numarası da görselde yer almaktadır. Avuç içine konumlandırılmış kalp görselinin sloganda yer alan gönül kazanmak eylemine yapılan bir atıf olduğu düşünülmektedir. Yardım yapma davranışının, gönül kazanmakla ilişkilendirilmesi, bireylerin manevi duygularına yapılan bir göndermeyi

de içermektedir. Bireylerin gönül kazanarak iyi hissetmesinin asıl odak olduğu düşünülmektedir. Kampanyaya ait görsel aşağıda yer almaktadır.

Bir önceki kampanyaya benzer şekilde, bu kampanyada da sürecin, bağışçılar tarafından takip edilebileceği bir çevrimiçi araç olmadığı dikkat çekmektedir. 2021 yılında yapılan bir çalıştay raporuna göre de insani yardımlardaki zorluklar incelenmiş ve etik problemler ön plana çıkmıştır. Bu sebeple hükümetlerin, bağış toplayanların ve bağışçıların belirli aralıklarla konuyla ilgili bilgilendirilmesinin ve denetleme mekanizmalarının hassas ve şeffaf bir şekilde işlemesi gerektiği sonucuna ulaşılmıştır (Roberts ve Faith, 2020). Kurumsal olduğu için bağışçılarda güven duygusunu sağlama potansiyeli yüksek olsa da kurumsal kampanyalarda da takip mekanizmalarının geliştirilmesi gerekliliği dikkat çekmektedir.

4.3.1.5 Bir Aradayız İdlib'in Yanındayız

Dijital yardım kampanyası kurumsal olarak sadece Türkiye'deki vatandaşlar için değil; zaman zaman insani destek, güvenlik ve sosyal yardım gerekçeleriyle de düzenlenmektedir. "Bir Aradayız İdlib'in Yanındayız" kampanyası bu durumun örneklerinden biri olarak değerlendirilmektedir. Kampanya 14 Ocak 2020 tarihinde süresiz olarak başlatılmıştır. İçişleri Bakanlığı öncülüğünde ve AFAD koordinasyonunda, 8 STK ortaklığında başlatılmıştır. Kampanyaya ait görseller aşağıda yer almaktadır.

Kampanya görsellerinde tek bir slogan kullanılarak destek veren kuruluşların logoları yer almaktadır. Kampanyaya bağış yapabilmek için gerekli olan kısa mesaj numaraları için başka bir görsel hazırlanmış ve bu ikinci görselde kampanyanın sosyal mecralarda dağılımını kolaylaştıran ve etki alanının büyümesine aracı olan etiket "#İblibinYanındayız" hashtag'iyle kullanılmıştır. Kampanyaya ait bilgilerin yer aldığı herhangi bir web sitesine görsellerde yer verilmemiştir. Bu kampanyada da 'Bir Aradalık' vurgusu dikkat çekmektedir. Sivil Toplum Kuruluşlarıyla iş birliği kurulmasının özellikle üzerinde durulduğu düşünülmektedir. Çünkü Sivil Toplum Kuruluşları, insani iyilik halini niteleyen ve bunun için uğraş veren yapılardır. Kampanyayla ilgili kurumsal ortaklıkların da kurulması, başlı başına devlet kurumlarına olan mevcut güveninin pekiştirilmesi anlamını taşımaktadır. Kurumsal kampanyalarda yardımların yerine ulaşmaması endişesinin ve buna yönelik haberlerin olmadığı dikkat çeken bir başka durumdur.

4.3.2 Bireysel Dijital Kampanyalar

4.3.2.1 Gökalp'in Kahramanı Sen Ol

Bireysel kampanyalar çeşitli sebeplerle başlatılmaktadır. Bu kampanyalardan biri, sosyal paylaşım platformlarından olan Instagram'da "gokalp__kucuk" kullanıcı adıyla başlatılmış olan "Gökalp'in Kahramanı Sen Ol" kampanyasıdır. Kampanya için birden fazla hashtag çalışması gerçekleştirilmiştir. Kampanya 2020 yılının Nisan ayında başlatılmış ve 2,4 milyon dolar hedefiyle başlatılmıştır. Kampanya hem sosyal mecralardan kullanıcıların desteklerini isterken hem de basında duyurulmuştur. Kampanyayı başlatan aile sosyal medyada aktif ola-

rak fotoğraf ve video paylaşmıştır. Kampanya yürütülürken bu sebeple kurumsal kampanyalarda olduğu gibi tek bir afiş hazırlanarak paylaşım yapılmamıştır. Kampanya için kullanılan görsellerden biri aşağıda yer almaktadır.

Kampanya yürütülürken bağışçılara "kahraman" kelimesi kullanılarak seslenilmesi uygun görülmüştür. Bağışlar, https://www.gofundme.com/f/gokalp039a-adim-olun adresinde toplandığı için bireyler hem yardımları yaparken yorum yapabilmiş hem de toplanan yardımları anlık olarak takip etmişlerdir. Kampanya duyurulduktan yaklaşık 5 ay sonra hedeflenen bağış miktarına ulaşılmıştır. Aile bu durumu hem sosyal medya hesaplarında hem de yine basın aracılığıyla bağışçılara duyurmuştur (Milliyet, 2020, 4 Eylül). Kampanya süresince binlerce takipçi kazanan hesap, SMA hastası olan çocuğun ifadeleriyle takipçilerine "kahramanlarım" kelimesiyle seslenerek paylaşımlar yapmıştır. Bireylerin yardımda bulundukları kişilerden geri bildirim aldıklarında motive olacağı ön kabulüyle bu davranışın sergilendiği düşünülmektedir. Yine aidiyet duygusunun kurulması için gerekli durumların oluşturulduğu gözlemlenmektedir.

Yapılan araştırmalardan bazıları göstermektedir ki; kimi kullanıcılar, yüz yüze iletişimde ifade edemedikleri birtakım şeyleri, çevrimiçi iletişimde rahat-

lıkla dile getirmektedirler. Online disinhibisyon olarak da tanımlanan bu durum, bireylerin çevrimiçi ortamlarda, kendilerini sosyal baskılardan uzak olarak düşünmelerinden kaynaklanmaktadır ve sosyal baskıyı önemli bir ölçüde ortadan kaldırmaktadır (Kerstens ve Stol, 2014; Suler, 2004). Bu kampanyada da günlük yaşantıda yardım istenmesi halinde yapılamayacak olan; "Kahramanım Olur Musun?" söylemi kullanılmıştır.

Bu tür bireysel kampanyalarda hasta olan çocukların yüzlerinin açık bir biçimde kullanılıyor olması, daha önce de bahsi geçtiği gibi bireylerin empati yapmalarına da sebebiyet vermekte ve empatinin yardım davranışına yönlendiren bir durum olduğu bilinmektedir. Görselde, çocuğun arkasında var olduğu figüre edilen pelerin ve duvardaki süper kahraman çizimleri, kahramanlık temasının yoğun olarak kullanıldığının göstergeleridir. Sloganda kırmızı olarak yazılmış olan "sen" kelimesi, Süperman adlı süper kahramanın logosundan esinlenerek üretilmiştir. Doğrudan seslenişin, bireyler üzerindeki etkisinin de kullanılmak istenildiği açıktır. Yine görseldeki çocuğun üzerindeki kıyafette de süper kahraman logosunun olduğu görülmektedir. Kampanyaya destek olarak kahraman olacakları, kampanya görseline rastlayan kişilerin akıllarında şekillendirilmeye çalışılan ana düşünce olarak görülmektedir.

4.3.2.2 Ramazan'a Kol Kanat Olalım

Ağrı'da elektrik teline takılmış olan kuşu kurtarabilmek için direğe çıkan ve akıma kapılıp 2 kolunu birden kaybeden 17 yaşındaki Ramazan Taşdemir'in haberi basında yer almıştır. Bu haber sonrası Twitter'da "ByAras10" kullanıcı isimli hesap "HayallereDokunuyoruz" hashtag'i ile 'Ramazan'a Kol Kanat Olalım' kampanyasını başlatılmıştır. Kampanyada kullanılan görsel aşağıda yer almaktadır.

Sosyal medyada dikkat çeken haber sonrası kazanın gerçekleştiği il olan Ağrı'da yerel yönetimler yardım taahhüttü vermişlerdir. Ayrıca taraftar kulüpleri de destek olmuşlardır. Haberin basında yankı bulmasından sonra Ramazan Taşdemir'in "kanatsız güvercin" olarak anılmaya başladığı görülmektedir (Hürriyet, 2018, 23 Haziran). Başlatılan kampanyaya destek verdiğini açıklayan bir futbol kulübünün de desteğiyle Ramazan Taşdemir için başlatılan yardım kampanyası, Ramazan Taşdemir'in protez kollarının takılması için ameliyatının yapılmasına vesile olmuştur. (Hürriyet, 2019, 18 Ocak). Bu örnekteki dijital yardım kampanyasının diğer bireysel kampanyalardan ayrılan en önemli özelliği ihtiyaç sahibi kişi tarafından değil; onun adına sosyal medya kullanıcılarından birinin atmış olduğu bir adımla başlamış olmasıdır. Bu kampanyanın sloganı incelendiğinde de "birlik" duygusuna yapılan vurgu dikkat çekmektedir. Bu örnekte, bir taraftar grubunun kampanyayı sahiplenici bir tutum sergilemesi birlikte başarmayı

motive eden ve mevcut aidiyet duygusundan da faydalanarak başarılı bir şekilde sonlandırılmış durum, basında da geniş yer bulmuştur.

Bu kampanya, dijital kampanyaların geniş kitlelere ulaşıyor olduğunun önemli bir örneğidir. Bireysel kullanıcılar tarafından başlatılan bir kampanyanın bir spor kulübü tarafından sahiplenilmesi, aidiyet duygusunun da kampanyalarda ne kadar öne çıkabildiğinin başka bir göstergesi olarak karşımıza çıkmaktadır.

4.3.2.3 Asude Defne Özkan

Twitter'da tekil bir kullanıcı olarak "asudedefneozkan" kullanıcı adıyla video çeken bir kadın, 09 Mayıs 2019 tarihinde ABD'de bir üniversite tarafından kabul aldığını ve eğitim masrafları için desteğe ihtiyacı olduğunu ifade etmiştir. Kullanıcının videosu ünlüler tarafından da etkileşim aldığı için geniş bir etkileşim ağı oluşmuştur. Kullanıcıların bir kısmı kadının başlatmış olduğu kampanyanın detaylarını sorgulamıştır ancak destek olup kampanyaya nakdi yardım yapanların olduğu da görülmüştür. Ancak yardımlar toplanınca kullanıcı bütün paylaşımlarını silerek ortadan kaybolmuştur. Kullanıcının hesaplarındaki paylaşımları kaldırmasının ardından durum, başka haberlere de konu olup bireylerin sorumluluk duygularından faydalanıldığını, ancak bu kampanyaya destek veren bireylerin de "hedefi ve yardıma ihtiyacı olan idealist gençlere yardım ediyorum" bakış açısıyla duygusal bir tatmin yaşadıklarını belirten ifadelere rastlanmıştır. (Milliyet, 2019, 13 Mayıs).

Yapılan bazı sosyolojik çalışmalarda, geleneksel söylemde 'dilencilik' olarak tanımlanan eylemin, yoksulluktan dolayı değil; meslek olarak yapıldığını öne sürmektedir (Birtek, 2014, s. 128). Daha önce de bahsedildiği üzere sanal dilencilik olarak literatüre kazandırılmış olan kavramın bir biçimi bu kampanyada görülmektedir. Kampanyayı başlatan kişinin, kampanyayı başlatma amacı, yoksulluğun aksine, daha iyi şartlarda eğitim alabilmek olarak belirtilmiştir. Kampanya, eğitime destek olunmasını isteyerek bireylerin ilgisini çekmeyi başarmıştır.

Bu yardım kampanyası, dolandırıcılık olarak kayıtlara geçen kampanyalardan biri olarak karşımıza çıkmıştır. Bir sosyal paylaşım platformunda, bireylerin birkaç görselle ya da birkaç video ile yardım istemesi, yardımları topladıkları hesapların herhangi bir resmi denetime tabi olmadan bunu yapması, insanların iyilik duygularını zedeleyen bir durum olmaktadır. Yardım yapan kimselerin, sonra-

sında dolandırıldıkları gerçeğiyle karşılaşmaları, sonraki yardım davranışlarına da etki etme potansiyelini taşımaktadır. Yasal boşlukların bu konuda doldurulması ve denetimlerin sıklaştırılması gerekliliği oluşmaktadır.

4.3.2.4 sma_tip1mirbahattin

Sosyal mecralardan olan Twitter ve Instagram'da sma_tip1mirbahattin kullanıcı adıyla bir üye bireysel yardım kampanyası başlatmıştır. Bu yardım kampanyasında çeşitli banka hesap numaraları paylaşılarak bağış toplanmıştır. Hesaptan paylaşılan görsellerde, çocuğa ait hastane görüntüleri kullanılarak duygusal cümlelerle yardım talebinde bulunulmaktadır. Kampanyada kullanılan görsellerden biri aşağıda yer almaktadır.

Paylaşımlarda kullanılan fotoğrafların SMA hastalığı sebebiyle yaşamını kaybetmiş bir çocuğa ait olduğu, çocuğun ailesi tarafından fark edilmiş ve aile tarafından hukuki süreç başlatılmıştır. Bireysel olarak başlatılan kampanyaların esasen yerel yönetimlerden alınması gereken özel izinler sonucu gerçekleşmesinin yasal yükümlülüğü bulunmakla birlikte, sanal mecraların denetlenebilirliği konusundaki problemlerden dolayı sıkıntılar yaşanması muhtemel hale gelmiştir.

Bu kampanyadaki durum, muhtaçmış gibi davranılarak toplumun temelini oluşturan dayanışma, yardımlaşma, bölüşme, paylaşma gibi değerleri alet ederek bu değerlerin istismarını içermektedir. Kampanyada görüldüğü gibi, hasta bir çocuğun görsellerinin kullanılarak gerçek olmayan bir bağış kampanyasının öğrenilmesi durumu ortaya çıktığında insanların aldatılmış olduklarını düşünmelerine sebep olmaktadır (Kükrer, 2014, s. 7). Bu durum da çalışmada üzerinde durulduğu üzere, çeşitli değerlerin temele alınarak bireylerin güvenle yardım davranışında bulunmasına engel olacaktır.

Bir önceki kampanyadaki dolandırıcılık örneği, bu kampanyada da dikkatleri çekmektedir. Kullanıcılar hasta bir çocuğa yardım ettiklerini sanıyorken, esasen dolandırıcılık niyetindeki insanlara para aktarmışlardır. Hasta çocukların kişisel verilerinin açık bir şekilde yer aldığı görsellerin dijital mecralarda kullanılması; hasta çocuklar hayatını kaybettiğinde ya da sağlıklarına kavuşmaları halinde de dijital izler olarak sanal mecralarda kalabilmekte ve sonrasında kötü niyetli insanların bu görselleri kötü amaçlarla kullanmasına aracılık edebilmektedir. Bu noktada yeniden sosyal ağlar aracılığıyla paylaşılan görsellerin yasal yükümlülükleri konusunda yaptırımların geliştirilmesi ve uygulanması konusu gündeme gelmektedir.

SONUÇ

Bireyler sosyal medya aracılığıyla yeni ilişkilere, yeni mekânlara ve yeni davranış örüntülerine sahip olma imkânına ulaşmıştır. Bireysel bir erdem kabul edilen yardımseverlik anlayışı da teknolojik gelişmelere bağlı olarak yeni biçimlere bürünmüştür. Etkileşimin akıllı cihazların çalışır durumda olduğu her mekân ve zamana yayılması, toplumsal olanı da başka bir biçime döndürme özelliği göstermektedir.

Gündelik yaşantılarımızda kullanmakta olduğumuz pek çok hizmete internet üzerinden erişebiliyor olmamız, ilişkilerin yeni biçimlerini şekillendiren en temel unsurdur. Bireyler sosyal medyayı eğlence, haber alma, alışveriş, hizmet alma gibi pek çok gerekçe ile kullanırken, aynı zamanda yardım faaliyetlerinde de aktif olarak kullanma davranışı da geliştirmeye başlamıştır.

Eskiden yardıma ihtiyacı olan kimselerin tespiti ve bahsi geçen kimselere yardım ulaştırılması yakın ve yakın çevre temaslı kişilerle kısıtlıyken; günümüzde çevrimiçi başlatılan bir yardım kampanyasıyla aynı mekânları ve hatta aynı coğrafyaları bile paylaşmadığımız kimselere ulaşabilmek mümkün hale gelmiştir. Bireyler dijital platformlarda gerçekleşen yardım faaliyetlerine çeşitli biçimlerde katılım sağlayabilmektedir. Genel olarak bir sloganla başlatılan yardım kampanyalarına, yardıma ihtiyacı olan kişilere ait görsellerle sunularak belirtilen bir banka hesap numarası aracılığıyla yardımseverlerden destek beklenmektedir.

Bu görsellerin ya da sloganların çeşitli hashtag adı verilen etiketleme biçimiyle paylaşılması, sosyal medya kullanıcılarının davranışları arasındadır. Etiketlemenin içeriğin tanımlanmasına (Akar, 2010, s. 79) olan katkısı bilinmekte ve paylaşılan haberin, görselin, sloganın hem daha kolay ulaşılabilir olmasını sağlamakta hem de dikkatleri bu yöne çekmek için güçlü bir aracı olabilmektedir. Kişiler esasen etiketleme davranışında bulunurken, Goffman'ın (2004, s. 24) da belirttiği gibi karşıdaki kişilere verilen izlenimi denetim altında tutma yönünde bir istek sergilerken, sunmuş oldukları kimlikleri de vitrinleri olarak ötekine açmaktadır.

Bu davranışta, hem sanal anlamdaki etiketlemenin hem de toplumsal ilişkilerimizde kullandığımız şekliyle etiketlemenin etkilerini görmek mümkündür. Kimi zaman kullanıcılar, etiketleme davranışında bulunarak kendilerinin yardımsever, iyi, duyarlı bir insan olduklarını göstermek isterken, bazı zamanlarda kendilerinden olmayanların tespitini gerçekleştirmek istemektedir.

Dijital platformlarda düzenlenen yardım kampanyaları konusunda kullanıcılar, farklı tanımlamalar yapabilmektedir. Bu yardım kampanyalarıyla ihtiyacı karşılanan ihtiyaç sahiplerinin olduğu bilinmektedir. Ancak günümüzde artan dijital yardım kampanyalarına tepki olarak 'sosyal medya dilenciliği' gibi bir kavramsallaştırmanın yapıldığı da görülmektedir (Gedikoğlu vd. 2019). 'Sanal dilencilik' ya da 'e-dilencilik' kullanımı da mevcuttur (Günhan, 2019). Bu olumsuzluğun yardım kampanyalarının dolandırıcılık amacıyla kullanılmasında (Habertürk, 2020) etkili olduğu düşünülmektedir. Ayrıca türü ne olursa olsun, dilencilik söz konusu olduğunda, kavramın da temelinde doğrudan insanların merhamet duygularına oynayarak menfaat elde etmeye çalışmak olduğu bilinmektedir (Çelebi, 2009: s. 159).

Bireylerin yardım yaparken, şeffaflık arayışı, güvenilir kaynakları aracı etmesi, en muhtaç olanı bulma arzusu gibi isteklerinin olduğu söylenmektedir. Ancak dijital platformlarda gerçekleşen yardım kampanyalarının hem bu özellikleri taşıyor nitelikte olması hem de dolandırıcılığa kapı aralıyor olması yine daha önce bahsi geçtiği şekliyle sosyal medyanın bizatihi kendisinden kaynaklanan bir durum olarak karşımıza çıkmaktadır.

Diğer taraftan kampanyaların özellikle sloganları dikkate alındığında "birlikte, bütünlük, el uzatmak, kahramanlık, destek olmak" gibi değerlere yapılan vurgu dikkat çekmektedir. Karşıdaki kişinin empati kurmasına, yardım davranışı gösterildiğinde bireylerin aidiyet hissetmelerine sebep olabilecek sloganların tercih edilmesi, yardım davranışını etkileyen durumlardan biri olarak da karşımıza çıkmaktadır.

Sonuç olarak, hemen her işlemin çevrimiçi ortamlarda yapıldığı günümüzde, yardım yapma davranışının da sanal mekânlarda ve sanal cemaatler aracılığıyla gerçekleştirildiği bir durum gözlemlenmektedir. Geleneksel biçimde gerçekleştirilen yardımlarda da karşılaşılması muhtemel şekilde, bireylerin iyilik halinin ve iyilik yapma isteğinin sanal mecralarda da suiistimal edilmesi durumuna rastlanılmaktadır. Özellikle bir iban numarası paylaşılarak para talebinde bulunulması her ne kadar 2860 sayılı kanuna göre kabahat olarak sayılıp yasal yaptırımı olsa da sosyal medyanın denetimsizliğinden dolayı, kimi zaman, çalışmada da konu edildiği şekilde bu eylemin yapıldığı görülmektedir. Bireysel kullanıcıların, bu gibi eylemlerle karşılaşma sıklığına bağlı olarak, bireylerin dolandırılmasının,

yardımda bulunma davranışına da etki etmesi muhtemeldir. Bu çalışma ile sosyal medyada dönüşen yardım anlayışı sınıflandırılmaya ve çözümlenmeye çalışılmıştır. Çalışma, dijital yardım kampanyaları konusunun daha fazla çalışılması gerektiğine dikkat çekmek istemektedir. Bu yönüyle, çalışmanın sınırlılıkları ve yöntemi dikkate alındığında, kendisinden sonraki çalışmalara da kaynaklık etmesi mümkündür.

KAYNAKÇA

Aile, Çalışma ve Sosyal Hizmet Bakanlığı. (2020). Milli dayanışma kampanyası biz bize yeteriz Türkiyem. https://www.ailevecalisma.gov.tr/afyonkarahisar/haberler/milli-dayanisma-kampanyasi-biz-bize-yeteriz-turkiyem/ adresinden 17.02.2022 tarihinde alınmıştır.

Akar, E. (2010). *Sosyal medya pazarlaması: sosyal webde pazarlama stratejleri* (1.bs). Ankara: Efil Yayınevi.

Baudrillard, J. (2017). *Simülakr ve simülasyon*. Ankara: Doğu Batı Yayınları.

Berger, P. ve Luckman, T. (2008). *Gerçekliğin sosyal inşası: bir bilgi sosyolojisi incelemesi* (V. S. Öğütle, Çev.), İstanbul: Paradigma Yayınları (Orijinal eserin basım tarihi 1966).

Bilgiç, H. G., Seferoğlu, S. S. (2020). Z kuşağının sosyal ağlarda karşı karşıya olduğu tehlikeler ve onları bu tehlikelerden korumaya yönelik öneriler. A. G. Baran, O. Hazer ve M. S. Öztürk (Eds.) *içinde Gençlik ve Dijital Çağ*. Ankara: Hacettepe.

Birekul, M. (2015). Toplumsal hareketler ve müzik: söylemden harekete marşlar/ezgiler. *Sosyoloji Divanı* (5). 87-119. Çizgi Kitabevi.

Birtek, F. (2014). Dilencilik suçu. İnönü Üniversitesi Hukuk Fakültesi Dergisi. *5*(2), 121-172.

Bozkurt, V. (2006). *Değişen dünyada sosyoloji* (2.bs). Bursa: Ekin Kitabevi.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş. ve Demirel, F. (2009). Bilimsel araştırma yöntemleri. Ankara: Pegem Akademi.

Devlet Planlama Teşkilatı. (2011). *Sosyal hizmetler ve yardımlar özel ihti-*

sas komisyonu raporu. Ankara.

Dökmen, Ü. (1997). İletişim çatışmaları ve empati (14.bs). İstanbul: Sistem Yayıncılık.

Durkheim E. (2006). *Toplumsal işbölümü* (Ö. Ozankaya, Çev.). İzmir: Cem Yayınları (Orijinal eserin basım tarihi 1893).

Ensonhaber. (2020, 23 Nisan). Bursa'da 18 aylık sma hastası Gökalp yardım bekliyor. https://www.ensonhaber.com/amp/ic-haber/bursada-18-aylik-sma-hastasi-gokalp-yardim-bekliyor adresinden 17.02.2022 tarihinde alınmıştır.

Eren Çetin, Ş. ve Ayhan, A. (2020). Katılımcı kültür olgusu bağlamında sosyal medya: netnografik bir analiz, *Intermedia International e-Journal*, *7*(12). 47-69.

Feldman, R. S. (1996). *Understanding psychology* (4.bs). Mc Graw- Hill. Inc.

Fiske, J. (1996). İletişim çalışmalarına giriş. (S. İrvan, Çev.). Ankara: Bilim ve Sanat Yayınları.

Gazianteppusula. (2020, 21 Eylül). Kalbe dokun gönül kazan tablet bağışla eğitime destek ol. https://www.gazianteppusula.com/haber/kalbe-dokun-gonul-kazan-tablet-bagisla-egitime-destek-ol-haberi-86846.html adresinden 17.02.2022 tarihinde alınmıştır.

Gedikoğlu, E., Özşirin, S. ve Oğuş, K. (2019). Sosyal medya dilenciliği: sosyal medya mecralarında sosyal normların dejenerasyonu, Üsküdar Üniversitesi İletişim Fakültesi 6. Uluslararası İletişim Günleri Dijital Dönüşüm Sempozyumu, Tam Metni içinde (s. 277-304).

Gerbaudo, P. (2017). From cyber-autonomism to cyber-populism: An ide-

ological history of digital activism. *tripleC: Communication, Capitalism & Critique*, *15*(2). 477-489.

Goffman, E. (2004). *Günlük yaşamda benliğin sunumu* (B. Cezar, Çev.). Metis Yayınları.

Günindi Ersöz, A. (2016). Üniversite öğrencilerinin Facebook kullanma alışkanlıkları: sosyoloji bölümü öğrencileri örneği. *Sosyoloji Konferansları*, No: 53 (2016-1). 303-326.

Habertürk. (2019, 11 Mayıs). Asude Defne Özkan kimdir, kaç yaşında sosyal medyada Asude Defne Özkan belirsizliği https://www.haberturk.com/asude-defne-ozkan-kimdir-kac-yasinda-sosyal-medyada-asude-defne-ozkan-belirsizligi-2460436 adresinden 17.02.2022 tarihinde alınmıştır.

Habertürk. (2020, 04 Aralık). SMA'dan ölen çocukları kullandılar! Korkunç dolandırıcılık! https://www.haberturk.com/son-dakika-bu-nasil-vicdan-sma-dan-olen-cocuklari-kullandilar-korkunc-dolandiricilik-haberler-2892062 adresinden 17.02.2022 tarihinde alınmıştır.

Hürriyet. (2017, 15 Ekim). Kuşu kurtaran çobanın elleri kesilecek. https://www.hurriyet.com.tr/gundem/kusu-kurtaran-cobanin-elleri-kesilecek-40610937 adresinden 17.02.2022 tarihinde alınmıştır.

Hürriyet. (2018, 23 Haziran). Kanatsız güvercin proteze koşuyor. https://www.hurriyet.com.tr/gundem/kanatsiz-guvercin-proteze-kosuyor-40875585 adresinden 17.02.2022 tarihinde alınmıştır.

Hürriyet. (2019, 18 Ocak). Elektrik akımına kapılan Ramazan protez kollarına kavuştu. (https://www.hurriyet.com.tr/video/elektrik-akima-kapilan-ramazan-protez-kollarina-kavustu-41087074 adresinden 17.02.2022 tarihinde alınmıştır.

Ickes, W. (1997). *Empathic accuracy* (1.bs). A Division Of Guilford Publications.

İnceoğlu, Y., Çoban, S. (Der.). (2015). İnternet ve sokak (1.bs). İstanbul: Ayrıntı Yayınları.

İstanbul Büyükşehir Belediye Başkanlığı. (2020). https://birliktebasaracagiz.ibb.gov.tr adresinden 17.02.2022 tarihinde alınmıştır.

Kadushin, A. ve Kadushin, G. (1997). *The social work interview: A guide for human service professionals*. New York: Columbia University Press.

Kalish, B. (1971). An experiment in the development of empathy in nursing students. *Nursing Research*, 20, ss. 202-211.

Kasapoğlu, A., Ecevit, M. (2001). *Depremin sosyolojik araştırması* (1.bs). Ankara: Sosyoloji Derneği Yayınları.

Katz, R. L. (1963). *Empathy, its nature and uses* (1.bs). The Free Press Of Glencoe.

Kerstens, J. ve Stol, W. (2014). Receiving online sexual requests and producing online sexual images: The multifaceted and dialogic nature of adolescents' online sexual interactions. *Cyberpsychology: Journal of Psychosocial Research on Cyberspac., 8*(1), Article 8.

Kuyucuoğlu, İ. (2015). Sosyolojinin kuruluşunu etkileyen düşünce akımları ve klasik sosyolojide yöntem tartışmaları. *Uluslararası Sosyal Araştırmalar Dergisi*. 674-687.

Kükrer, M. (2014). Ankara'da dilencilik ve sadaka kültürü [Yayımlanmamış yüksek lisans tezi]. Ankara Üniversitesi Sosal Bilimler Enstitüsü.

Milliyet. (2019, 13 Mayıs). Asude Defne Özkan'a destek olan ünlüler

pişman mı?. https://www.milliyet.com.tr/asude-defne-ozkan-a-destek-olan-unluler-pisman-mi--molatik-11757/?Sayfa=5 adresinden 17.02.2022 tarihinde alınmıştır.

Milliyet. (2020, 4 Eylül). Sma hastası minik Gökalp'e bağışta mutlu son. https://www.milliyet.com.tr/gundem/sma-hastasi-minik-gokalpe-bagista-mutlu-son-6297789 adresinden 17.02.2022 tarihinde alınmıştır.

Nguyen, P. T. (2017). Nostalgic for the present: digital nostalgia and mediated authenticity on Instagram. *Yüksek Lisans Tezi*. Stockholm University.

Neuman, W. L. (2014). *Toplumsal Araştırma Yöntemleri Nitel ve Nicel Yaklaşımlar I*. Ankara: Yayınodası Yayıncılık.

Özkalp, E. (2005). *Sosyolojiye giriş* (14.bs). Bursa: Ekin Kitabevi.

Öztürk, M. (2013). *Tüketici ayartma ya da yoksullaşarak tüketme*. (Z. Kara, Der.), Bauman Sosyolojisi içinde (s. 85-110). İstanbul: Ayrıntı Yayınları.

PusulaGazetesi. (2020, 5 Ekim). Devrek Kaymakamlığı bağış kampanyası düzenledi. http://www.pusulagazetesi.com.tr/devrek-kaymakamligi-bagis-kampanyasi-duzenledi-157513-haberler.html adresinden 17.02.2022 tarihinde alınmıştır.

Roberts, T. and Faith, B. (2021) Digital Aid: understanding the digital challenges facing humanitarian assistance. *Institute of Development Studies*. Brighton. DOI: 10.19088/IDS.2021.030

Sakarya, Ş. ve Bezirgan, E. (2018). Kitlesel fonlama platformları: Türkiye ve yurtdışı karşılaştırması. *Düzce Üniversitesi Sosyal Bilimler Dergisi, 8*(2), 18-33.

Schultz, P. W. (2000). Empathizing with nature: the effects of perspecti-

ve taking on concern for environmental ıssues. Journal of Social Issues, 56(3). 391–406.

Seyyar, A. (2008). *Sosyal siyaset terimleri* (2.bs). Sakarya: Sakarya Yayıncılık.

Smith, H. C. (1996). *Sensitivity to people* (Text Edition). Mcgraw- Hill Book Company.

Sözen, N. (2020). Covıd 19 sürecinde uzaktan eğitim uygulamaları üzerine bir inceleme. *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi. 7*(12). 302-319.

Stebnicki, M. A. (2000). Stress and grief reactions among rehabilitation professionals: dealing effectively with empathy fatigue. *Journal of Rehabilitation*, 66(1). 23-29.

Stilwell, B. M. (2001). Empathy and moral development: implications for caring and justice. *Journal of the American Academy of Child & Adolescent Psychiatry*, 40(5). 614–615.

Suler, J. (2004). The online disinhibition effect. *Cyber Psychoogy & Behavior. 7*(3). 321-326.

Şeker, A. (2008). *Sosyal çalışma mesleği* (1.bs). Ankara: Sabev Yayıncılık.

T.C. İç İşleri Bakanlığı. (2020, 14 Ocak). Bir aradayız İdlib'in yanındayız. https://www.icisleri.gov.tr/bir-aradayiz-idlibin-yanindayiz adresinden 17.02.2022 tarihinde alınmıştır.

Tarhan, U. (2013). Slactivism – slaktivizm & clicktivism – kliktivizm. https://www.ufuktarhan.com/makale/slactivism-slaktivizm-clicktivism-kliktivizm-nedir adresinden 21.02.2021 tarihinde alınmıştır.

Thakkar, B. M. ve Kanekar, S. (1989). Dispositional empathy and causal attribution as determinants of estimated willingness to help. *The Irish Journal of Psychology, 10*(3), ss. 381-387.

Timisi, N. (2005). Sanallığın gerçekliği: internetin kimlik ve topluluk alanlarına girişi. Binark, M. ve Kılıçbay, B. (Der.), internet, toplum, kültür içinde (s. 89-106). Epos Yayınları.

Toksöz, L., Kahraman, C. (2017). Türk üniversite öğrencilerinin emoji algısı. *Uluslararası Sosyal Bilimler Dergisi: Humanitas*, 5(9). 247-256.

Turkle, S. (1995). *Life on the screen: identity in the age of internet* (1.bs). Simon and Schuster.

Yegen, C. (2015). Bir dijital aktivizm biçimi olarak slaktivizm: Change. org örneği. *Karadeniz Teknik Üniversitesi İletişim Araştırmaları Dergisi*, 4(2). 84-108.

Yengin, D. (2012). *Sosyal iletişim aracı olarak akıllı telefonların oluşturduğu uygulama toplumu olgusu: Whatsapp uygulaması*. (T. Kara ve E. Özgen, Ed.), Sosyal Medya Akademi (1.bs). İstanbul: Beta Yayınları.

Yıldırım, B. (2015). İçerik analizi yönteminin tarihsel gelişimi uygulama alanları ve aşamaları. B. Yıldırım (Ed.), İletişim araştırmalarında yöntemler uygulama ve örneklerle (s. 105-154) içinde. İstanbul: Literatürk Academia.

Yolcuoğlu, İ. G. (2014). *Sosyal hizmet/sosyal çalışma bilim ve mesleğine giriş* (2.bs). İstanbul: Nar Yayınevi.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ (BTK DERGİ)
CİLT: 1 SAYI: 1 TARİH: TEMMUZ - EYLÜL 2023 ISSN: 2980-1311

GERÇEKLİK TEKNOLOJİLERİNİN UYGULAMA ALANLARI VE UYGULAMA ZORLUKLARI

Feridun GÜNGÖR[1]

Özet

Bu makale çalışmasının amacı, gerçeklik teknolojileri olarak tanımlanan artırılmış, sanal, karma ve genişletilmiş gerçeklik teknolojilerinin uygulanmasında karşılaşılan zorluklara odaklanmaktır. Zorlukların belirlenmesinin temel amacı ise gelişimi ve inovasyonu hızlandırarak potansiyel riskleri minimize etmektir. Bu makale çalışmasında; internet kaynakları kullanılmış, araştırma şirketlerinin yayınladığı raporlar taranmış, doküman incelemesi yapılmış, konu ile ilgili makalelerden istifade edilmiştir. Ayrıca Avrupa Komisyonu'nun yayınlamış olduğu stratejik raporlar irdelenmiştir. Bu literatür taraması, araştırma sorularını şekillendirmeye ve var olan bilgiyi anlamaya yardımcı olduğu gibi gerçeklik teknolojilerinin uygulanması önünde duran zorluk başlıklarının tanımlanmasını sağlamıştır.

İlk olarak, iş dünyasında şirketler arası iş birliği ve müşteri odaklı çalışma modellerinde karşılaşılan zorluklar incelenmiştir. İkinci olarak girişimcilerin bu teknolojileri kullanırken karşılaştığı yasal düzenlemelerle ilgili zorluklar ele alınmıştır. Daha sonra gerçeklik teknolojine yönelik kullanıcı kabulünü geciktiren sosyal ve teknolojik zorluklar işlenmiştir. Son olarak, finansal zorluklar bu teknolojilerin uygulanmasında karşılaşılan diğer bir kategoriyi oluşturmuştur. Artırılmış ve sanal gerçeklik gözlüklerinin yüksek maliyeti, kullanıcıların bu platformlara erişimini zorlaştırmıştır. Bu durum, artırılmış ve sanal gerçeklik pazarının büyüme potansiyelini kısıtlamıştır. Dolayısıyla yazılım geliştiriciler, bu platformlara içerik üretmekte isteksiz davranmıştır. Sonuç olarak hem maliyetlerin yüksek oluşu hem de platformlarda etkileyici içeriğin az oluşu kısır bir döngüyü başlatmıştır. Bu döngünün kırılması adına gerçeklik teknolojilerine; teknolojik, finansal ve yasal müdahalelerin gerektiği mütalaa edilmektedir.

Anahtar Kelimeler: *Artırılmış Gerçeklik, Sanal Gerçeklik, Karma Gerçeklik, Genişletilmiş Gerçeklik*

[1] Bilgi Teknolojileri ve İletişim Kurumu (BTK) Bilişim Uzman Yardımcısı, feridun.gungor@btk.gov.tr, ORCID: 0009-0003-7724-8725

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ (BTK DERGİ)
CİLT: 1 SAYI: 1 TARİH: TEMMUZ - EYLÜL 2023

APPLICATION AREAS AND IMPLEMENTATION CHALLENGES OF REALITY TECHNOLOGIES

Abstract

The aim of this paper is to focus on the challenges faced in the implementation of augmented, virtual, mixed and extended reality technologies, defined as reality technologies. The main purpose of identifying challenges is to minimize potential risks by accelerating development and innovation. In this article; internet sources were used, reports published by research companies were scanned, documents were analyzed, and articles on the subject were utilized. In addition, the strategic reports published by the European Commission were analyzed. This literature review helped to shape the research questions and to understand the existing knowledge, as well as to identify the challenges facing the implementation of reality technologies.

First, the challenges of inter-company collaboration and customer-centric working models in the business world are examined. Second, the regulatory challenges that entrepreneurs face when using these technologies are discussed. Then, social and technological challenges that delay user acceptance of reality technology. Finally, financial challenges were another category of challenges faced in the implementation of these technologies. The high cost of augmented and virtual reality glasses has made it difficult for users to access these platforms. This has restricted the growth potential of the augmented and virtual reality market. Therefore, software developers have been reluctant to produce content for these platforms. As a result, both the high costs and the lack of impressive content on the platforms have started a vicious cycle. In order to break this cycle, technological, financial and legal interventions in reality technologies are considered necessary.

Keywords: *Augmented Reality, Virtual Reality, Mixed Reality, Extended Reality*

GİRİŞ

Günümüzde hızla gelişen haberleşme teknolojileri, gerçeklik teknolojileri sektöründe büyük bir dönüşüme sebep olmaktadır, bu da kullanıcıların gerçek dünyayı dijital içeriklerle birleştiren etkileşimli deneyimlere olan ilgisini artırmaktadır. Ancak gerçeklik teknolojilerin yeteri kadar anlaşılamaması, gerçeklik teknolojileri ile birlikte kullanılan diğer teknolojilerin soyut kalması gerçeklik teknolojilerine yönelik beklenen yüksek kullanıcı kabul refleksini engelleyici bir rol oynamaktadır. Sosyal hayata dair zorluk faktörü gibi aşılması gereken başka zorluklar da mevcuttur. İş dünyasına ilişkin zorluklar, teknolojik zorluklar, yasal zorluklar, finansal zorluklar bahsedilen zorluklar listesinin başında yer almaktadır. Bu zorlukları detaylıca irdeleyebilmek için birinci bölümde gerçeklik teknolojilerinin tanımı yapılmış, ikinci bölüm altında gerçeklik teknolojilerinin kullanıldığı sektörler incelenerek uygulama alanları somutlaştırılmıştır. Üçüncü bölümde ise bahsedilen zorluklar detaylıca işlenmiş ve son başlık altında sonuç ve önerilere yer verilmiştir.

1. GERÇEKLİK TEKNOLOJİLERİ

Gerçeklik teknolojilerinden bahsedildiğinde öncelikle akıllara artırılmış ve sanal gerçeklik teknolojileri gelmektedir. Öyle ki artırılmış ve sanal gerçeklik terimleri kavramsal olarak birbirlerinin yerine kullanılmaktadır. Ancak her ne kadar artırılmış gerçeklik ve sanal gerçeklik teknolojileri birlikte zikredilse de temelde birbirlerinden sert bir şekilde ayrılmaktadırlar. Bu teknolojilerinin yanında bir de karma gerçeklik ve genişletilmiş gerçeklik teknolojileri bulunmaktadır. Gerçeklik teknolojileri, kullanıcısına vaat ettikleri ve uygulama alanları bakımında büyük ölçüde farklılık göstermelerinin yanında, yazılım geliştirilme süreçlerinde ve kullandıkları ekipmanlar ile de farklılık göstermektedir.

1.1 Artırılmış Gerçeklik

Artırılmış gerçeklik (Augmented Reality - AR) teknolojisi, gerçekte var olan bir nesne, düzlem veya bir işaretçi üzerine sentetik bir nesne yerleştirilerek sağlanmaktadır. Sentetik nesneden kasıt bilgisayar ortamında hazırlanmış çıktılardır. Bu çıktılar üç boyutlu model, resim, metin, animasyon veya video olabilmektedir. Artırılmış gerçeklik teknolojisi uygulanacağı sektöre bağlı olarak birçok amaç için kullanılabilir fakat genel olarak kullanıcıya birim zamanda

gerçek dünya ile ilgili çokça bilgi aktararak kullanıcının durumsal farkındalığını artırmak ve kullanıcının doğru karar verme süresini kısaltmayı amaçlamaktadır (Künüçen, 2021). Artırılmış gerçeklik cihazları, üzerinde gömülü gelen sensörler ile gerçek dünyayı tarar. Bu sayede içinde bulunduğumuz gerçek yaşam ortamı dijital bir ara yüz haline getirilmiş olur. Tasarım sanatçıları tarafından daha önceden tasarlanmış olan sanal nesneler gerçek zamanlı olarak programcı tarafından belirlenmiş noktalara yerleştirilir veya sentetik nesne gerçek bir nesne üzerine giydirilir. Artırılmış gerçeklik, gerçek dünyada bulunan nesnelerin, sadece görsel olarak değil aynı zamanda işitsel, dokunsal, somatosensoriyel[1] ve koku alma da dâhil olmak üzere birden fazla duyuya veri sağlayan, bilgisayar bilimleri tarafından oluşturulan bilgilerle zenginleştirildiği bir deneyim sunmaktadır. Dolayısı ile doğası gereği artırılmış gerçeklik teknolojisi hangi araç ile sağlanırsa sağlansın kullanıcısını bulunduğu ortamdan soyutlamamaktadır.

1.2 Sanal Gerçeklik

Sanal gerçeklik (Virtual Reality - VR) teknolojisi kullanıcıyı bulunduğu ortamdan tamamen soyutlamaktadır. Sanal gerçeklik gözlüğü ile sanal bir dünyaya giriş yapılır. Çeşitli sentetik çevre tasarımları yapan programlarla bu evren daha önce tasarlanmıştır. Kullanıcı, gözlüğü taktıktan sonra sanatçının kendisi için tasarlamış olduğu dünyaya katılmış olur (Künüçen, 2021). Kullanıcının bu dünya ile etkileşime girmesi kullanıcının elinde bulunan konsollarla mümkün olmaktadır. Son çıkan gözlüklerde, kullanıcılar istedikleri zaman konsollardan bağımsız olarak hareket edebilmekte ve gözlük üzerinde bulunan sensörler sayesinde kullanıcının elleri takip edilerek, sentetik nesnelerle etkileşim sağlanmaktadır (Vision Pro, 2023). Tüm bu aparat ve yazılımlar ile kullanıcının fiziksel varlığı sanal bir dünyada simüle edilmiş olur.

İnsanlar gerçek dünyada konumları ve açıları değiştiğinde orta kulakta bulunan denge mekanizması ile duyuları arasında bir bilgi akışı sağlanmaktadır (KKB Kliniği ve ARGE Merkezi, 2023). Sanal gerçeklik ortamında, duyular bir açı değişikliği olduğunu denge mekanizmasına haber verir fakat denge mekanizması bu açı değişikliğini insan vücudunda bulunmakta olan reseptörlerden gelen bilgiler

1 Somatosensoriyel sistem kompleks bir duyu sistemidir. Termoreseptör, fotoreseptör, mekanoreseptör ve kemoreseptör olmak üzere bir dizi reseptörden oluşur. Duyu reseptörleri cilt ve epitel, çizgili kaslar, kemikler ve eklemler, iç organlar ve kardiyovasküleri kapsamaktadır.

ile doğrulayamaz. Meydana gelen bu tutarsızlık neticesinde kişide mide bulantısı baş dönmesi ve huzursuzluk görülebilir.

Mühendisler, kimi uygulama alanlarında kullanılmak üzere sanal gerçeklik kullanıcılarının gerçek dünya ile oryantasyon tutarsızlığını aşmak için sanal gerçeklik gözlüğü yanına başka cihazlar da eklemişlerdir. Örneğin, sanal gerçeklik platformları denen bu araçlar ile kullanıcının sanal dünyadaki açı değişikliği meydana getiren eylemleri gerçek dünyada simüle edilmektedir (Motion Systems, 2023).

1.3 Genişletilmiş ve Karma Gerçeklik

Karma gerçeklik (Mixed Reality - MR) terimi, literatüre artırılmış gerçeklik gözlüklerinin piyasa sürülmesi ile girmiştir. Artırılmış gerçeklikte bilindiği gibi gerçek bir nesne üzerine sentetik bir nesne yerleştirilmektedir. Bu teknolojiye erişmek için herhangi bir artırılmış gerçeklik gözlüğüne sahip olunması gerekmektedir. Günümüzde son kullanıcıya ait akıllı telefonların hemen hemen hepsi artırılmış gerçeklik uygulamalarını kısmen veya tamamen desteklemektedir. Bu kullanım senaryolarında kullanıcı, gerçek bir nesne üzerinde sanal bir nesne görebilmekte fakat bu sanal nesneler ile herhangi bir etkileşime girememektedir. Artırılmış gerçeklik gözlükleri ise kullanıcıların sentetik nesneler ile etkileşime girebilmesine imkân tanımıştır. Bu yetenek sanal gerçeklik deneyimine benzetilmiş ve bu teknolojiye karma gerçeklik denmiştir (Künüçen, 2021).

Blok zinciri, bulut bilişim, uç bilgi işlem gibi teknolojilerin artırılmış, sanal ve karma gerçeklik teknolojileri ile birlikte kullanılmasına ise genişletilmiş gerçeklik (Extended Reality - XR) denilmektedir (Künüçen, 2021) .

2. GERÇEKLİK TEKNOLOJİLERİNİN KULLANILDIĞI SEKTÖRLER

Gerçeklik teknolojileri hemen hemen her sektörde kabul görmüştür. Kullanıcının durumsal farkındalığını artırarak karar verme süresini kısaltması artırılmış gerçeklik teknolojisinin en göze çarpan özelliği olarak öncelikle imalat ve üretim endüstrilerinin dikkatini çekmiştir. Aynı özelliği ile artırılmış gerçeklik teknolojisi sahada askerlerin durumsal farkındalığını artırarak ordunun muhabere yeteneği bir sonraki aşamaya taşımıştır. Gerçeklik teknolojileri, sektörlerin

farklı dilimlerle temsil ettiği büyük bir pasta gibi, insan deneyimini geliştirmek, eğitim ve simülasyon alanlarında faydalar sağlamak, verimlilik ve tasarruf imkanı sunmak, sağlık ve terapi alanında potansiyeller sunmak gibi bir dizi avantajı bünyesinde toplamıştır.

Şekil 2.1. Gerçeklik teknolojilerinin uygulandığı sektörler

2.1 Oyun Endüstrisi

Oyun oynamak insanlarda görüldüğü gibi birçok hayvan türünde de gözlemlenen bir davranıştır. Oyun yolu ile canlılar kendi türlerine özgü birtakım yetenekleri keşfederek geliştirmektedir. İnsanlarda çocukluk dönemlerinde oynanan oyun; çocuğun ilişkileri keşfetmesine yarayan, iskelet ve kas gelişimini olumlu yönde etkileyen kısacası fiziksel ve ruhsal sağlığı için gerekli ve içten gelen bir eylemdir. Bakıldığı zaman oyun tarihinin insanlık tarihi kadar eski olduğu görül-

mektedir (Zeynep Oğuzhan, 2018). İnsanlığın ilk zamanlarında taşlarla, sopalarla bir takım hayvan kemikleri ile oynanan oyunlar günümüzde dijital oyunlara kadar büyük bir gelişim ve dönüşüm göstermiştir. Dijital oyunlar, B2C[2] pazarında sanal ve artırılmış gerçeklik için en yaygın kullanım alanıdır. Son yıllarda Apple, Meta, Sony, HTC ve Valve gibi büyük aktörlerin VR başlıkları için teknoloji geliştirmeleri ve gözlükleri ticarileştirilebilir hale getirmeleri, artırılmış ve sanal gerçeklik teknolojilerini daha geniş bir kitleye ulaştırmıştır. Dijital oyunlarda oyuncunun kendisini oyunun bir parçası gibi hissetmesi, oyun içi karakterler ile bir bağ kurması gerçekçi bir oyun deneyimi için önemli bir unsurdur. Artırılmış ve sanal gerçeklik teknolojileri sanal ile gerçek dünyalar arasındaki duvarın gittikçe incelmesine neden olan teknolojiler olduğu için bu teknolojilerle desteklenmiş olan oyunlar, oyuncular tarafından yoğun ilgi görmektedir.

2.2 Eğitim Sektörü

Eğitim yeni kuşakların toplum yaşamında yerlerini almaları için gerekli bilgi, beceri ve anlayışları edinme, kişiliklerini geliştirme süreçlerinin tamamı olarak tanımlanmaktadır. Bununla birlikte dallarında uzman yetişkin bireyler de yeni bir teknoloji üzerine veya başka bir pozisyonda çalışmak üzere bir eğitime tabi tutulabilirler. Eğitim sürecinin tartışılmaz en değerli katmanı ise eğitim kalitesidir. Eğitim kalitesi, eğitime tabi tutulmuş kişilerin kendi eğitimleri ile ilgili bilgi, beceri ve davranışlarıyla ihtiyaç ve isteklere beklenen düzeyde ve derecede cevap verebilmeleri olgusunu ifade etmektedir (Kayadibi, 2021). Artırılmış gerçeklik teknolojisinin eğitim alanında da tercih edilmesinin birçok nedenden bir kısmı aşağıda listelenmiştir;

- **Özel Ekipman Gerektirmez:** Artırılmış gerçekliğin diğer sürükleyici teknolojilere göre en büyük avantajlarından biri, herhangi bir özel donanım gerektirmemesidir. Kullanıcılar, AR tabanlı bir uygulamaya doğrudan akıllı telefonlarından erişebilmektedir. Ayrıca okul içinde ve kurslarda eğitimi kalıcı hale getirmek için çeşitli materyaller kullanılmaktadır. Bunlar haritalar, dünya küreleri, insan ve çeşitli hayvan iskeletleri gibi farklı farklı birçok materyal olabilmektedir. Artırılmış gerçeklik teknolojisi ile bu materyaller anında erişilebilir sanal nesneler haline getirilmektedir.

2 B2C (Busimess to Consumer): Doğrudan tüketiciye veya işletmeden tüketiciye, ürünleri doğrudan müşterilere satmanın ve böylece herhangi bir üçüncü taraf perakendeciyi, toptancıyı veya diğer aracıları atlayan iş modelidir.

- **Daha İyi Öğrenci Katılımı:** Öğrenciler artırılmış gerçeklik teknolojisi kullanarak derste anlatılan bir konu ile kolayca etkileşime girebilmektedir. Böylece öğrenme, öğrenciler için daha ilgi çekici bir süreç haline gelmektedir. Kimi öğrenciler için en sıkıcı konular bile artırılmış gerçeklik teknolojisinin sağladığı bu etkileşim ile heyecan verici mevzular haline dönüşebilmektedir.
- **Pratik Öğrenme:** Artırılmış Gerçekliğin öğretimdeki bir diğer önemli avantajı, pratik öğrenme vaat etmesidir. Örneğin eğitimin büyük bir gemi motoru gibi taşıması zor, her kurs yeri için teminin maliyetli olduğu bir şey üzerine verildiğini varsayalım. Artırılmış gerçeklik ile bu eğitimi vermek birçok açıdan maliyetsiz olacaktır. Bu aynı zamanda çalışma ortamında iş güvenliği tedbirlerini artırmada önemli bir faktör olarak ön plana çıkmaktadır.
- **Birleşik Öğrenme:** Öğrenciler veya kursiyerler ders kitaplarından öğrendikleri bilgileri iş dünyasında doğrudan kullanamamaktadır. Pratik teoriden oldukça farklı olabildiği gibi bir de kimi bilginin tatbiki için şartlar bir şekilde sağlanamamaktadır. Ancak, çok yönlü bir başarı elde etmek için artırılmış gerçeklik gibi teknolojileri geleneksel öğretim yöntemleriyle birleştirerek başarı sağlanabilmektedir. Okullarda veya kurslarda artırılmış gerçeklik teknolojisi ile öğrenciler derslerde edindikleri tüm teorik bilgilerin pratik uygulamasını tatbik etme esnekliğine sahiptir.
- **Ekonomik:** Üniversitelerin, kolejlerin ve eğitim enstitülerinin artırılmış gerçeklik teknolojisini tüm müfredata entegre etmeyi düşünmesinin en büyük nedenlerinden biri de maliyettir. Kolejler, artırılmış gerçeklik tabanlı bir teknoloji platformuna erişmek için aslında herhangi bir pahalı donanıma ihtiyaç duyulmadığından, başlangıçta yüksek meblağlar harcamak zorunda kalmayacaklardır.
- **Karmaşık ve Soyut Kavramların Daha İyi Açıklanması:** İnsanların, bir kavramı görselleştirildiği zaman daha iyi anlayacaklarına şüphe yoktur. Özellikle soyut veya uzun tanımlamalar gerektiren konuların sunumunda öğrencilere bu kavramların üç boyutlu model gösterimleri tercih edilmelidir.

Eğitimde artırılmış gerçeklik teknolojilerinin kullanıldığı birçok artırılmış ve sanal gerçeklik örneği bulunmaktadır. Eğitim amacı ile geliştirmiştir, çarpıcı birkaç uygulama örneği listelenmiştir;

- Bu bağlamda amacı iskelet, kas gibi insan sistemleri üzerinde bilgi vermek olan bir artırılmış gerçeklik uygulaması incelenmiştir. Şüphesiz gerçek bir kadavra üzerinde çalışmak birçok yönü ile rahatsız edici olabildiği gibi ileri tıp eğitimi haricinde kullanılması da gereksizdir. Bu uygulama ile insan kemik isimleri, bağlantı noktaları, kas çeşitleri, yapıları ve yönleri gibi birçok bilgi kullanıcıya verilmektedir (Octagon Studio, 2022).
- Kendi doğal ortamından dışarı çıkarılamayacak veya çıkarılmaması gereken bir hayvan artırılmış gerçeklik teknolojisi ile kendi boyutlarında ve kendi özelliklerini gösterebileceği şekilde modellenerek sergilenebilmektedir. Artırılmış gerçeklik teknolojisi bu özellikleri ile örgün eğitimde kullanılabildiği gibi okul öncesi eğitimde de tercih edilmektedir. Okul öncesi çocuklar için üretilmiş eğitim kartlarda hayvanların resimleri bulunmaktadır (Nilüfer Koca, 2023). Ebeveynleri tarafından çocuklara okunması için bu kartların arkasında ilgili bilgiler yer almaktadır. Artırılmış gerçeklik teknolojisi destekli bu oyun kartlarının üzerinde ise resim yerine ilgili hayvanların 3B modelleri oluşturulmaktadır.
- Uzay ve Güneş Sistemi oldukça büyüktürler. Burada mesafeler ışık yılları ile ifade edilmektedir. Bir ışık yılı ise ışığın bir yılda aldığı yoldur ki ışığın saniyedeki hızı yaklaşık olarak 300.000 km/sn olarak bilinmektedir. Bu muazzam hız ve büyüklükler anlatımlar sırasında soyut kavramlara dönüşebilmektedir. Bu yüzden güneş sistemi ve diğer yıldız sistemleri eğitim amaçlı olarak modellenmiş ve artırılmış gerçeklik uygulamalarına dönüştürülmüştür (Kırıkkaya & Şentürk, 2018).
- Artırılmış gerçeklik teknolojisinin eğitimde kullanıldığı bir diğer alan ise dil öğreniminde kullanılmasıdır. Genellikle yeni bir dil öğrenmek için sıklıkla tavsiye edilen bir yöntem bol bol pratik yapmak ve dile oldukça fazla maruz kalmadır. Gerçeklik teknolojileri marifeti ile modellenmiş bir partnerle diyalog egzersizleri yapma mümkün hale getirilmiştir (Hsu, 2017).

2.3 Sağlık Endüstrisi

Küresel bazda tüm insanları etkileyen pandemi döneminde eğitim sürecinin dahi sekteye uğradığı görülmüştür. Fakat dünyanın geçtiği tüm çağlarda sağlık en önemli konu olmaya devam etmiştir. Teknolojisinin olmadığı çağlarda veya tek-

nolojiye erişimin bir şekilde kısıtlandığı günümüzde dahi sağlık hizmetine erişmek için insanlar çeşitli yollar aramıştır. Sağlık sektörü devamlı olarak yatırımlar almıştır. Bu yatırımlar ilaç ve aşı üretimine olduğu gibi sektörde kullanılan araç gereçler üzerine de olmuştur. Bu bağlamda sağlık sektörü odağında artırılmış gerçeklik teknolojisi yatırım almaktadır (Kinjoll Dey, 2023).

Konu insan tedavisi olunca birçok farklı yaklaşım görülmektedir. Tarih boyunca duygu ve düşüncelerin anlatım biçimi olan müzik; dinsel, askeri ve eğlence amaçlı olduğu kadar tedavi amacıyla da kullanılmıştır (Mütem, 2023). Farklı ritimler ve etkileyici sözler eşliğinde hastanın şifaya kavuşturulması, müzikle tedavinin temelini oluşturmuştur. Razî, Farabî, İbn Sina, Hasan Şuurî ve Gevrekzade Hasan Efendi gibi bilim adamlarının yaptıkları araştırmalar ve elde ettikleri sonuçları anlatan kitapları kullanan Türklerin, ilk ciddi müzikle tedavi çalışmalarını Selçuklu ve Osmanlılar döneminde uyguladıkları görülür. Eski Türk hekimleri, korku, heyecan, kuşku ve ruhi bunalım gösterenlerin nabızlarındaki değişim ve bu değişimin neden olduğu huzursuzluk için hastalarına çeşitli melodileri dinletirler, bu sırada nabızlarını kontrol ederek hastaya en uygun melodiyi bulurlar, hatta aynı hastaları bir araya getirerek hastalığı tedavi ederlerdi (Erer, S. & Atıcı, E., 2010). Gelişen teknoloji ile birlikte bu tedavi yaklaşımları artarak çeşitlenmiştir. Sağlık Sektöründe gerçeklik teknolojilerinin uygulanmasına yönelik uygulamalar bir kısmı şu şekilde listelenmiştir:

- **Yükseklik Fobisi:** Diğer adıyla akrofobi yükseklikten ve yüksekten düşmekten aşırı korkma halidir. Yükseklik fobisine sahip kişiler asansöre binmekten, merdiven çıkmaktan bile kaygı duyarlar (Cem Kaya, 2023). Yükseklik korkusu farklı derecelerde kendini gösterirken yükseklik korkusunun tedavisinde artırılmış ve sanal gerçeklik teknolojisi kullanılmaktadır (Psikiyatri Hemşireliği, 2019). Artırılmış gerçeklik teknolojisinin sanal gerçeklik teknolojisine nazaran tercih edilmesinin bir sebebi ortamdan tam anlamı ile soyutlanmak istemeyen hastanın tercihidir. Bu tedavi sürecinde hastanın ayakta durmakta olduğu zemine sanal bir uçurum yerleştirilmektedir.
- **Damar Tespiti:** Artırılmış gerçeklik, damar tespitini iyileştirmek için hemşireler ve doktorlar tarafından da benimsenmiş bir uygulamadır. Özellikle hastalar yoğun pigmentli cilde veya küçük kan damarlarına sahip olduğunda damar bulmak zor olabilmektedir (Çankaya vd., 2020). Dolayısıyla bazı has-

talar için kan alınmasının travmatik ve rahatsız edici sonuçları olabilmektedir. Artırılmış gerçeklik odaklı teknolojiler bu sorunları çözmek için uygulanabilir teknolojilerdir. Bu teknoloji, taşınabilir, el tipi bir cihazda bulunan lazer tabanlı bir tarayıcı ve dijital lazer projeksiyonunun bir kombinasyonunu kullanır. Bu, uygulayıcılara deri altındaki damar ağının gerçek zamanlı görüntüsünü görme yeteneği verir.

- **Doktorlar Arasında Artırılmış Gerçeklik ile Sanal İş Birliği:** Bir ameliyat sırasında operasyon odasında olamayan bir doktorun artırılmış veya sanal gerçeklik gözlüğü ile operatör doktorun gördüğü her şeyi görebilmesini, ona tavsiye ve öneri verebildiği tecrübe aktarımı senaryosunu ele almaktadır (Furkan Gençoğlu, 2021). Uzak bir yerde bulunan doktorun elleri sentetik bir görüntü ile operatör doktorun gözlüğünde görülebilmektedir. Hata ve riskleri en aza indirmeyi hedefleyen bu uygulama ayrıca operatör için birçok avantajlar sağlamaktadır.
- **Hastaların Verilerinin Takibi:** Doktorlar ameliyat sırasında birçok hasta verisini ekranlardan takip etmek durumundadırlar. Bu doktorun gözlerinin kimi zamanlarda hastadan başka yöne bakmasını gerektirmektedir. Artırılmış gerçeklik gözlükleri ile doktorlar hasta verilerini gerçek zamanlı olarak gözlüklerden görebilmektedir. Aynı zamanda ameliyat sırasında artırılmış gerçeklik gözlüğü kullanan doktorlar kritik müdahalelerde bulunurken sezgisel davranmak yerine daha çok kanıttan faydalanabilirler.
- **Görme ve İşitme Engelliler için Destek Sağlama:** Artırılmış gerçeklik gözlükleri 3D tanıma yazılımı kullanarak nesnelerin ve insanların görünümünü iyileştirebilmektedir. Ayrıca görme engelleri bulunan bireylerin, artırılmış gerçeklik gözlüklerine verdikleri sesli komutlar ile kayıp eşyaları bulmalarına ve çevrelerinde kolayca gezinmelerine yardımcı olunabilir. İşitme engelliler ve duyma kaybı yaşayan insanlar için geliştirilen bir artırılmış gerçeklik uygulamasında ise konuşan insanların hepsine anlık olarak alt yazı yerleştirilmektedir. Bu işlem sırasında artırılmış gerçeklik gözlüğü konuşmacının sesini alarak işlemekte ve görüntüsünün altına metni yerleştirmektedir (Aisling Ní Chúláin, 2022).
- **Egzersiz ve Spor:** Hareketsiz ve sporsuz bir yaşamın insan hayatını olumsuz yönde etkilediğine dair kanıtlar oldukça fazladır. Hareketsizliğin sigara kadar

ölümcül olduğunu ortaya koyan çalışmalar mevcuttur (Better Health Channel, 2023). Bu bağlamda insanların iskelet ve kas sistemlerini çalıştırmak amacı ile artırılmış ve sanal gerçeklik uygulamaları geliştirilmiştir. Bu uygulamalar aynı zamanda kullanıcının oyun içerisinde kaç kalori yaktığını bilgisini oyun sonunda kullanıcıya sunabildiği gibi çevrimiçi oyun seçeneklerinde bir rekabet ortamı oluşturarak katılımı artırıcı rol de oynamaktadır (Liu vd., 2020).

2.4 Savunma Sanayi

Dünya üzerinde en çok yatırım yapılan, para ve zaman harcanan sektörlerin başında askeriye ve savunma harcamaları gelmektedir. Artırılmış gerçeklik teknolojisi ise savunma sanayinde oldukça ilgi duyulan ve yatırım alan teknolojilerden biri olarak dikkat çekmektedir. Şimdiden birçok ülke ordusunu artırılmış gerçeklik gözlükleri ile donatmaya başlamıştır (Dylan Malyasov, 2022). Dünyada olduğu gibi ülkemizde de artırılmış gerçeklik uygulamalarının savunma sanayine yönelik olarak geliştirildiği gözlemlenmiştir. Türkiye'de askeri amaçlarla kullanılmak üzere Aselsan Sivas ve BİTES Savunma Havacılık ve Uzay Teknolojileri A.Ş. (BİTES) arasında artırılmış gerçeklik gözlüğü üretmek için bir protokol imzalanmıştır (Savunma Haber, 2021). Donanım tarafında artırılmış gerçeklik gözlükleri üretim çalışmaları sürerken yazılım tarafında da aynı şekilde yoğun bir AR-GE faaliyeti yürütüldüğü görülmektedir. Aşağıda, artırılmış gerçeklik gözlükleri ile donatılmış askeri birliklerin kullanması için yerli kaynaklar ile Türkiye'de kodlanan artırılmış gerçeklik uygulamalar listelenmiştir.

- **Zırh Delici Görüş Sistemi:** Zırhlı bir araç içerisinde bulunan bir askere araç içerisinde 360 derece görüş sağlamayı amaçlayan bir artırılmış gerçeklik uygulamasıdır. Bu uygulamada artırılmış gerçeklik gözlüğü ek donanım olarak bir ladybug kamera kullanır. Ladybug kamera donanımı üzerinde çok sayıda yerleşik kamera barındırmaktadır. Yerleşik kameralardan alınan görüntüler gerçek zamanlı olarak birleştirilir ve 360 derece, küresel bir görüntü elde edilir. Alınan görüntüler artırılmış gerçeklik lenslerine anlık olarak aktarılır. Bu askeri uygulama, zırhlı araçların duvarlarını artırılmış gerçeklik kullanıcısı için adeta saydam bir cam haline getirmektedir (Savunma Haber, 2022).
- **Dost Düşman Birliği Tanıma:** Askeri bir operasyonda dost ve düşman birliklerin anlık konumu şüphesiz ki operasyonun kaderi için oldukça önem-

lidir. Bu askeri kaygılar ile geliştiren uygulama dost ve düşman birliklerinin konumunu anlık olarak tüm artırılmış gerçeklik kullanıcısı askeri personel ile paylaşmayı sağlamaktadır. İnsansız hava araçları, uydular veya bizzat bir askerin operasyon sırasında gördüğü dost ve düşman konumları sisteme girilmektedir. Bu sayede bir asker artırılmış gerçeklik ile kendisi için hayati önem taşıyacak bilgileri görebilmektedir.

- **Harita Üzerinden Taktik Belirleme:** Artırılmış gerçeklik ile geliştirilen ve günümüzde hali hazırda kullanılan bir diğer askeri amaçla geliştirilen uygulamada operasyon yapılacak alanın gerçek görüntüsü üzerinde çalışma sağlanmaktadır. Gerçek yükseklik verileri ile çalışılan bu uygulama da taktik ve strateji geliştirmek için uygun koşullar sağlanmaktadır. Öncelikli olarak operasyon öncesi ve operasyon sırasında hızlıca kurulabilen bir ortam olmasının yanı sıra istenilen sayıda katılımcının katılımına olanak sunulmaktadır. Harita üzerinde yerleştirilen bir askerin o noktada görüş alanı, herhangi bir noktanın yüksekliği, noktalar arası mesafeler gibi birçok bilgi operasyonun selameti için faydalıdır. Ayrıca yapay destekli taktik ve strateji geliştirme uygulamalarında alana istenilen savaş araçları yerleştirilerek operasyonun simüle edilmesi yine artırılmış gerçeklik ortamında sağlanmaktadır (Infodefensa, 2018).
- **Mayın İmhası:** Askeri amaçlarla ile geliştirilen bu uygulamada sahada, mayın ve bomba imhası gibi tehlikeli görevlerde operatör hatasını en az seviyeye indirirken kişinin farkındalığını en üst düzeye çıkarmak hedeflenmiştir (Devpost, 2015). Çok iyi eğitilmiş personeller dışında uzmanlık alanı mayın imhası olmayan bir asker alanda kendisini bu işi yapmak zorunda kaldığı bir durum içerisinde bulabilmektedir. Bu ve buna benzer birçok istenmeyen senaryo için geliştirilen artırılmış gerçeklik uygulamasında senaryo şu şekilde işlemektedir. Artırılmış gerçeklik gözlüğü üzerinde çalışmakta olan bir yapay zekâ gözlüğün aldığı mayın görüntülerini işler ve mayının imhası için bir dizi yönergenin uygulanmasını kontrol eder. Gözlük lenslerinden mayının neresine ne kadar süre ve kararlılıkla baskı yapılması gerektiği gibi birtakım komutları alan personel, mayını başarı ile nasıl imha edebileceğini görmüş olacaktır.

2.5 E Ticaret Endüstrisi

Sürekli bir gelişim trendi içerisinde olan e-ticaret, küresel bir pandeminin patlak vermesi ile çok daha hızlı bir gelişim göstermiştir. COVID-19 pandemi krizi

dünya genelinde insanların tüketim alışkanlıklarını önemli derecede değiştirmekle kalmayıp, toplumsal bir dönüşümü de başlatmıştır. Sosyal ve ticari yaşam, söz konusu pandemi sebebiyle büyük oranda dijitalleşmeye zorlanmıştır. Satın anlım süreçlerinde yaşanan endişeleri en aza indirme veya satın alımlarda kısa sürelerde doğru tercih yapma maksadı ile kodlanmış olan uygulama örnekleri aşağıda listelenmiştir.

- **Ev Eşyaları ve Dekorasyonu İçin AR:** Fiziksel mağazalar gerçekte oldukça büyük alanlardır ve mobilyalar bu büyük alanlarda sergilenmektedir. Bu tip yerlerde oldukça büyük olan mobilyalar müşterilere bir yanılsama ile gerçek ebatlarının altında görünebilmektedir. Bu durumun müşteri memnuniyetini etkilemesinden rahatsız olan ve sorunu gidermek isteyen şirketler çözümü artırılmış gerçeklik teknolojisi ile ortadan kaldırmıştır. Kullanıcılar bu tür artırılmış gerçeklik uygulamaları sahip oldukları mobil cihazlar ile kullanabilmektedir. Derinliği algılayan akıllı telefon sensörü ile kullanıcının bulunduğu ortam taranmaktadır. Bu sayede kullanıcının seçtiği ürün, gerçek boyutlarıyla evin ilgili konumuna yerleştirilebilmektedir (Ayda AYOUBI, 2017).
- **Kıyafet ve Takı Tercihi İçin AR:** Kıyafet tercihi müşterilerin oldukça ince eleyip sık dokudukları konulardan bir tanesidir. Oldukça özenli seçimlerin ardından alınıp fakat kullanılmayan kıyafet tercihleri görülebilmektedir. E-ticaret konusunda elektronik ürünlerin alımı, yiyecek siparişleri müşteriler tarafından en kolay benimsenen seçimlerdir. Fakat kıyafet ve takı siparişine duyulan endişeler konusunda çözüm artırılmış gerçeklik teknolojisi ile mümkün olmuştur. Hem akıllı mobil cihazlar ile hem bilgisayarların kameraları tarafından desteklenen bu teknolojide alınmak istenen ürün satın alım yapılmadan önce müşteriler tarafından deneyimlenebilmektedir (Tricia McKinnon, 2022).
- **Metaverse Mağazaları:** Farklı şirketler ve bireysel girişimciler tarafından şimdiden birçok metaverse platformu kurulmuştur. Bu sanal dünyalarda arsa alımları, yatırımcıların rağbeti ve kullanıcı sayılarındaki hızlı artış neticesinde kıyafet üreten şirketler bu sanal evrenlere mağazalarını taşımıştır (Rangoli, 2023). Metaverse platformlarında bulunan sanal mağazalarda satın alınan ürünlerin gerçek hayatta müşteriye gönderilebiliyor olmasının yanında bir de ürünlerin metaverse platformlarında bulunan kullanıcı avatarları için satıldığı görülmektedir.

2.6 Üretim Endüstrisi

Tamir, bakım veya montaj sırasında müşteri veya operatörlere artırılmış gerçeklik uygulamaları ile destek verilmektedir. Büyük endüstrilerde operatörün montaj veya üretim sırasında hata yapması facialara yol açabileceği gibi büyük maddi kayıplara ve zaman israfına neden olabilir. Bu tür artırılmış gerçeklik uygulamalarında amaç tüm süreç boyunca operatörün işlemlerini kontrol ederek doğruluğunu test etmektir. Süreç boyunca bu tip uygulamalar kullanıcılarına hangi tamir veya montaj aracını kullanacaklarına kadar detaylı bilgiler vermektedir (Mura&Dini 2020). Daha basit bireysel kullanıcılar için oluşturulmuş bu tip uygulamalarda ise daha ziyade müşteri memnuniyeti için uygulamalar tasarlanmaktadır. Her ne kadar evde montajı yapılacak ürün mühendisler tarafından sadeleştirilmiş ve montajı kolaylaştırılmış olsa da daha önce bu tip işler yapmamış olan sıradan kullanıcılar için ürün montajları karmaşık olabilmektedir.

2.7 Reklam Endüstrisi

Reklam insanları tüketime davet eden unsurlardan bir tanesidir. Bilindiği gibi reklam, ürünü tanıtmakta ve ürünün satışını artırmaktadır. Fakat ürünün reklamını ürünü alma potansiyeli taşıyan bireye ulaştırmak reklamcılık sektöründe uygulanan bir strateji olsa da uygun araçlar sağlanamamıştır. Genellikle ürün, ana akım medya araçları ile herkese yapılır. İlgili reklam ile bağlantısı olmayan bir kişi ise reklamın mesajını almaya istekli olmaz.

Web 2.0 ile başlayan dönemde kullanıcıların birtakım çıktılar vermesi kendileri ile ilgili dijital bir örüntü oluşturulmuştur. Bu çıktılar kullanıcı yorumları, beğenileri, arama motoru aramaları gibi dijital eylemlerden oluşmaktadır. Nihayetinde kullanıcıya yönelik, kişileştirilmiş bir içerik veya akışın oluşturulması sağlanmıştır. Artırılmış ve sanal gerçeklikte bu veriler ile kullanıcıya yönelik kişileştirilmiş reklamlar farklı bir boyut daha kazanmıştır. Bu teknolojiler ile birlikte ürün gerçek boyutlarında ve 3B model ile 360 derece sunulmaktadır.

2.8 Turizm Sektörü

"Turizm" Latince "Tornus" kelimesinden gelmektedir ve anlamı "dönme hareketi" dir. Turizmin birçok tanımı bulunmaktadır fakat Dünya Turizm Örgütü (WTO) turizmi şöyle tanımlamaktadır: "Turizm; sürekli kalışa dönüşmemek ve

gelir getirici hiçbir uğraşıda bulunmamak şartı ile bireylerin geçici süre konaklamalarından doğan olay ve ilişkilerin tümüdür.". Tanımda sözü edilen konaklamalar, kazanç sağlama amacına yönelik değildir. Konaklama geçici bir süre içindir. Geziyi yapan ve konaklayan kişi bir süre sonra yaşadığı yere geri döner. Öğrenim amacıyla uzun süreli konaklamalar, iş arama amacıyla yapılan geziler turizmin kapsamına girmemektedir (Otel Satın Alma Müdürleri ve Eğitim Derneği, 2020).

Turizmin sıralanmış olan amaçlarına ve turizm etkinliklerinin sınıflandırılma başlıklarına bakıldığında artırılmış ve sanal gerçeklik teknolojilerinin bu başlıklar için birçok yenilikçi çözümler sunduğu görülmektedir. Ayrıca turizmin tanımı ve gelir istatistiklerine bakıldığında artırılmış ve sanal gerçeklik teknolojileri için büyük bir pazar oluşturduğu anlaşılmaktadır (Ebru Avcı, 2020).

Türkiye Cumhuriyeti Millet Kütüphanesi Konferans Salonu yerleşkesinde Bilgi Güvenli Derneği tarafından 19-20 Ekim tarihleri arasında 15. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı tertip edilmiştir. Çeşitli panel ve oturumlara ev sahipliği yapan konferansta Fütürist Otelci Dr. Cem Kınay Sanal Evren ve Türkiye Panelinde turizmle ilgili görüşlerini artırılmış ve sanal gerçeklik odağında paylaşmıştır. "Her şey dahil" sisteminin kurucusu olarak da tanınan Kınay, metaverse platformlarının sağladığı sanallaştırma ile henüz ziyaret edemediği birtakım yerleri ziyaret edebildiğinden bahsetmiştir. Antarktika kıtası ve Peru'da bulunan Machu Picchu antik kenti bunlardan bazılarıdır. Ayrıca Kınay sektör içerisinde bulunan birisi olarak gözlemlerini paylaşmıştır. Konuşmasında, insanların sanal evrenlerde ziyaret ettikleri yerleri gerçek dünyada da ziyaret etmek isteyeceğini belirterek bu ziyaretlerin turizmi tetikleyeceğini savunmuştur. Hâlihazırda bu sebeplerle yazılmış olan birçok artırılmış ve sanal gerçeklik uygulamaları bulunmaktadır (James Şilin, 2019). Tarihi yerlerin modellenerek dönemin mimarisini yansıtan uygulamalar bulunduğu gibi şehrin binlerce yıl sonraki halinin modellenerek sunulduğu uygulamalar bulunmaktadır. Film veya romanlarda tasvir edilen fakat gerçekte olmayan yerler de yine modellenerek sanal evrenlerde ziyarete açılmıştır.

Turizm amaçları ile turistlerin konforunu artırmaya yönelik bir dizi artırılmış gerçeklik uygulamaları da ayrıca kodlanmıştır. Bu uygulamalarda artırılmış gerçeklik ile iç mekân navigasyon teknolojisinden yararlanılmıştır. Ayrıca, uygulama otel çalışanları ve müşteri ilişkilerini sağlayarak memnuniyeti artırmaya yönelik amaçlar için de kullanılmaktadır.

Artırılmış gerçeklik destekli uygulamalardan bir kısmı da ören yerlerinde harap olmuş kale ve surları gerçek görüntüsü ile görmek için kodlanmıştır. Bu uygulama kullanıcıların akıllı telefonlarında kullanılmaktadır. İlgili alan aslına uygun olarak yapının geri kalan kısmı referans alınarak mimarlar ve modelleme sanatçılarının ortak çalışması ile bilgisayar ortamında modellenir. Kullanıcının kamerası yapının referans kısmını parametre olarak alarak modellenen sanal yapıyı ilgili kısma yerleştirir.

Turizm kaygıları ile üretilmiş artırılmış ve sanal gerçeklik uygulamaların bir kısmı müzeler için üretilmiştir (Sönmez & Zabızade, 2022). Sakıp Sabancı Müzesi (Aytekin & Handan, 2016), Topkapı Sarayı, Latife Hanım Köşkü Anı Evi gibi müzeler bunlara örnek olarak gösterilebilir.

3. DİJİTAL DÖNÜŞÜMÜN ZORLU YOLCULUĞU

Gerçeklik teknolojileri her ne kadar hemen hemen her sektöre girmiş olsa da tüm özellikleri ile aktifleşmiş gerçeklik teknolojileri istenilen düzeyde yaygınlaşmamıştır (Berfin Çipa, 2023). İlk olarak, maliyet faktörü, artırılmış ve sanal gerçeklik başlıklarının satışını yavaşlatmıştır. Bu başlıklara sahip yeterli sayıda kullanıcının bulunmaması, geliştiricilerin artırılmış ve sanal gerçeklik oyun ve/veya uygulama geliştirme konusunda isteksiz olmalarına neden olmuştur. Maliyet faktörünün yanı sıra, artırılmış ve sanal gerçeklik içeriğinin yetersizliği, kullanıcıların bu gözlükleri alma konusundaki isteksizliğini daha da artırmıştır. Bu durum, kısır bir döngünün oluşmasına sebep olmuştur. Pandeminin etkisiyle birlikte, sanal gerçeklik sektöründe bu döngünün kısmen kırıldığı gözlemlenmiştir. Ancak yine de artırılmış gerçeklik gözlüklerinin yüksek maliyetleri, sanal gerçeklik pazarına nazaran artırılmış gerçeklik sektöründe daha ciddi zorlukların varlığına işaret etmektedir. Bu zorluklar; gerçeklik teknolojilerinin üretilme süreçlerini, ilgili ekosistem paydaşlarının karşılaştığı zorlukları, bu paydaşları çeşitli yönlerden koruyan yasal düzenlemelerin ilkel kalışını, nihai ürüne dönüşen uygulamaların kullanıcı kabulünü zorlaştıran sosyal ve teknolojilik meydan okumaları içermektedir.

Bu bölümde ilgili başlık altında spesifik olarak işlenen kimi zorlukların tavsiye niteliğinde olduğuna dair değerlendirme yapılabilir ancak bu başlıklar altında işlenen maddelerin barındırdığı majör zorluklara ışık tutulmuştur. Ayrıca *"Yeni bir*

iş/ürün geliştirmede karşılaşılan zorluklar" cinsinden değerlendirilebilecek başlıkların altında yer alan kimi maddeler yukarıda bahsedilen kısır döngünün birer dişlisi rolündedir. Dolayısı ilgili maddeler altında söz edilen zorlukların aşılması için spesifik çözümler gerekmektedir. Fakat bu zorluklar irdelenirken, kendi içinde başka zorluklar ihtiva eden çözümlere mercek tutmak kaçınılmaz olmuştur. Daha anlaşılır olması adına yukarıda söz edilen kısır döngü analiz edilirse;

- **Gözük maliyetlerinin yüksektir ve maliyetlerin düşürülmesi elzemdir:** Bu madde tavsiye niyetliğinde bir başlık olarak değerlendirilmemelidir. Bu başlık kendi içerisinde majör zorluklar barındıran bir konuyu işaret etmektedir. Gözlük üzerinde bulunan kimi modüllerin gözlükten çıkarılması maliyetleri düşürebilir ancak bu da başka sorunları doğurmaktadır.
- **Hedef kullanıcı kitlesi maliyetler nedeniyle gözlük alamamaktadır:** İnsanların maliyetler nedeniyle bir ürünü alamaması "Yeni bir iş/ürün geliştirmede karşılaşılan zorluklar" cinsinden değerlendirilmemelidir. Elbette bu durum, dünyanın herhangi bir yerinde, tarımdan turizme kadar herhangi bir sektörde karşılaşılabilen mevcut bir sorun olarak pazarı daraltan bir faktördür. Ancak bu ve benzeri maddelerin işlenmemesi zorlukların ifade edilmesini güçleştirmektedir.
- **Gözlük talebin az olması artırılmış ve sanal gerçeklik uygulama/oyun geliştiricilerini içerik üretme noktasında isteksiz kılmaktadır:** Bu olumsuz döngüyü kırmak için gerçeklik teknolojileri ile oyun veya uygulama geliştiriciler finanse edilerek sanal ve artırılmış gerçeklik platformları etkileyici içerikler ile doldurulmalıdır. Fakat daha önce de söylendiği gibi bir tavsiye değildir. Bu kendi içinde majör riskler barındırmaktadır. Bu riskleri göze alacak yatırımcılar bulmak veya yatırımcılar için teşvik programları hazırlamak kendi içinde zorluklar barındırmaktadır.
- **Geliştiricilerin oyun/uygulama geliştirmemesi kullanıcıları gözlük almamaya itmektedir:** Bahsedilen bu kısır döngünün son maddesini sadece bir tespit gibi olarak nitelendirerek kendi içinde barındırmış olduğu zorlukları ortaya koymamak bu çalışmanın noksan olmasına sebebiyet verebilirdi.

Bu bölümün giriş kısmında gerçeklik teknolojilerinin içinde bulunduğu bir kısır döngü maddeler halinde ortaya konmuştur. Daha sonra bu maddeler tek tek analiz edilerek alt başlıklarda işlenen konu okumasının nasıl yapılması gerektiği-

ne işaret edilmiştir. Ayrıca, uzun ifadelerin ardından okuyucunun alt bölümler ile ana metin arasındaki ilişkiyi kurmakta zorluk yaşanmaması adına aşağıdaki tablo; zorlukların yaşandığı alanlar ve zorluklara ait alt maddeleri göstermektedir.

Tablo 3.1. Gerçeklik teknolojilerinin uygulama alanında yaşanan zorluklar

ZORLUKLARIN YAŞANDIĞI ALANLAR	ZORLUKLARIN AİT ALT MADDELER
İş Dünyasında Mevcut Zorluklar	Artırılmış ve Sanal Gerçeklik Teknolojilerinin B2B ve B2C İş Modellerine Etkisi ve Zorluklar
	Dış Pazarda Riskler ve Küçük Düşünme Eğilimi
	Artırılmış ve Sanal Gerçeklik Girişimciliğinde Küçük Endüstriye Sahip Ülkelerin Zorlukları
	Artırılmış ve Sanal Gerçeklikte 3B Modellerin Önemi ve 3B Sanatçıların Karşılaştığı Zorluklar
	İnovasyonun Ekonomik Alanlara Uygulanması
	Hikâye Anlatımı: Reklamcılık ve Turizm Sektöründe Gerçeklik Teknolojileri
	Silo Zihniyeti
	Akademik-Endüstri İşbirliğinin Güçlendirilmesi
	Veri Gizliliği ve Kullanıcı İzni Başlıklarında Farkındalığın Artırılması
Yasal Zorluklar	Veri İşleme ve Ağ Güvenliği
	Yönetim ve Mevzuat Uyumunun Önem
	Sanal Gerçeklikte Kullanıcı Deneyimini Güçlendirmek

Sosyal Alan Zorlukları	Ebeveynlerin Artırılmış ve Sanal Gerçeklik Teknolojilerine İlişkin Kaygıları
	Güvenlik ve Gizlilik Endişeleri
Teknolojik Zorluklar	Yüksek Çözünürlüklü İçerik ve Ağ Altyapısının Artırılmış ve Sanal Gerçeklikte Önemi
	Haptik Teknolojiler
	Artırılmış Gerçeklikle Birlikte Kullanılan Teknolojilerin Tanımlanması
	Endüstri 4.0'dan 5.0'a Geçiş
	Altyapı Yetersizliği
	Standartlar ve Uyum
Finansal Zorluklar	Yenilikçi KOBİ'ler İçin Risk Teşvikli Finansman ve Koruyucu Yasaların Önemi
	Özel Finansmanın Artırılmış ve Sanal Gerçeklik Firmalarına Etkisi

3.1 İş Dünyasında Mevcut Zorluklar

Artırılmış ve sanal gerçeklik teknolojilerinin yaygınlaşmasıyla birlikte birçok sektörde B2B[3] ve B2C[4] iş modellerinde önemli değişiklikler yaşanmaktadır. Ancak, bu yeni teknolojilerin etkili bir şekilde uygulanması ve iş modellerine entegre edilmesi çeşitli zorlukları beraberinde getirmektedir. İlk olarak, artırılmış ve sanal gerçeklik teknolojilerinin iş modellerine etkisi üzerinde durmak önemlidir. Bu teknolojiler, işletmelerin ürünlerini ve hizmetlerini sunarken yeni ve etkileyici deneyimler sunma potansiyeline sahiptir. Ancak, bu yeni deneyimlerin tasarlanması, geliştirilmesi ve pazarlanması, geleneksel iş modellerine kıyasla farklılık gösterebilir ve bazı zorluklar ortaya çıkarabilir. Bunun yanı sıra, artırılmış ve sa-

3 B2B: İşletmeden işletmeye (business-to-business)
4 B2C: Doğrudan tüketiciye veya işletmeden tüketiciye (Direct-to-consumer or business-to-consumer)

nal gerçeklik teknolojileriyle ilgili olarak yerel merkezler ve ekosistemlerin kurulması da önemlidir. Bu merkezler, teknoloji geliştirme, eğitim, iş birliği ve yenilikçi projelerin desteklenmesi gibi alanlarda faaliyet gösterir. Ancak, bu süreçte rol dağılımı, finansman, kaynak yönetimi ve iş birliği gibi zorluklar ortaya çıkabilir.

Artırılmış ve sanal gerçeklik teknolojileriyle ilgili olarak dış pazarlara giriş yapmak da önemli bir zorluktur. Dış pazarlara açılmak, yeni iş fırsatları ve büyüme potansiyeli sunmasının yanı sıra bir dizi riski de beraberinde getirir. Özellikle küçük şirketler, bu risklere karşı daha duyarlı olabilir ve küçük düşünme eğilimine girebilir. Teknolojik yeniliklerin hızlı bir şekilde demode olabilmesi, işlerin taklit edilme riski, dil sorunu, üretim maliyetleri, standardizasyon ve rekabet gibi unsurlar, dış pazarlara girişte karşılaşılan zorlukları artırabilir. Benzer şekilde, artırılmış ve sanal gerçeklik girişimciliğinde küçük endüstriye sahip ülkelerin karşılaştığı zorluklar da dikkate değerdir. Bu ülkelerde, teknolojik altyapı, yetenekli iş gücü ve pazarlama imkânları gibi faktörler sınırlı olabilir, bu da girişimcilerin büyüme ve başarı elde etmesini zorlaştırır. Bu başlık özelinde tanımlanmış zorluklar aşağıda listelenmiştir;

Artırılmış ve Sanal Gerçeklik Teknolojilerinin B2B ve B2C İş Modellerine Etkisi ve Zorluklar

Artırılmış ve sanal gerçeklik teknolojileri, insanların hayatına etki etme potansiyeline sahiptir, ancak henüz kullanıcılar için hayal edilen kullanım düzeye ulaşmamıştır. Bu teknolojinin B2C iş modellerinde piyasa değeri yavaş bir şekilde artarken, B2B iş modellerinde daha hızlı bir artış görülmektedir. Kullanıcıların günlük hayatında yaptıkları alışverişler, B2C iş modeline bir örnektir. Gerçeklik teknolojileri ile üretici firmaların ürünlerini doğrudan müşteriye sunmaları ve tedarikçi aracılığıyla müşterilere ulaştırmaları, müşteri memnuniyeti gibi birçok parametre açısından avantajlı görülmektedir. Ancak, küresel ölçekte satıcıların gerçeklik teknolojilerini kullanma oranları hala düşüktür (Radboud Universiteit, 2021).

Dış Pazarda Riskler ve Küçük Düşünme Eğilimi

Dış pazara girmek, birçok riski beraberinde getirebilir ve bazı şirketleri küçük düşünme eğilimine sokabilmektedir. Küreselleşmenin etkisiyle teknolojik yenilikler hızla eskimektedir, bu da şirketleri risk almaya zorlamaktadır. Ayrıca,

şirketlerin başarılı bir fikirle iyi bir iş çıkarmalarına rağmen, daha büyük veya daha zengin girişimciler tarafından işlerinin taklit edilme riskiyle karşı karşıya kalabilirler. Daha büyük bir reklam sermayesiyle işlerin taklit edilmesi, küçük yatırımcılar için büyük bir risk oluşturur. Dil sorunu, üretim maliyetleri, standardizasyon, rakipler ve rekabetin yoğunluğu gibi faktörler de şirketleri küçük düşünme eğilimine iten unsurlardır (Orta Anadolu İhracatçılar Birlikleri, 2023). Bu başlığın tam anlamıyla *"yeni bir iş/ürün geliştirmede karşılaşılan zorlukları"* temsil etmediği, gerçeklik teknolojilerine yönelik çok daha ciddi bir zorluğu temsil ettiği görülmektedir. Daha önce de ifade edilmiş olduğu gibi gerçeklik teknolojileri ile oyun/uygulama geliştirme; mobil veya video oyun geliştirme ile aynı süreçleri ve materyalleri içerir. Dolayısı ile gerçeklik teknolojilerini içeren iyi bir fikir çok hızlı ve kaliteli bir şekilde kopyalanabilir.

Artırılmış ve Sanal Gerçeklik Girişimciliğinde Küçük Endüstriye Sahip Ülkelerin Zorlukları

Küçük endüstriye sahip veya dijital oyunlar sektöründe gelişim gösteremeyen bazı ülkelerde, artırılmış ve sanal gerçeklik teknolojilerine yönelik girişimcilik faaliyetleri durgunluk yaşanması muhtemeldir. Bu durum, farklı açılardan aşılması gereken zorlukları ortaya koymaktadır. Özellikle dijital oyunlar sektöründeki uygulama gelişme süreçleri, gerçeklik teknolojileriyle uygulama çıkarma aşamasında benzer materyaller içermektedir. Ancak Türkiye gibi dijital oyunlar endüstrisinde silikon vadisi konumunda olan ülkeler, artırılmış ve sanal gerçeklik uygulamaları geliştirme noktasında oldukça avantajlı bir pozisyondadır (Sensor Tower, 2022).

Artırılmış ve Sanal Gerçeklikte 3B Modellerin Önemi ve 3B Sanatçıların Karşılaştığı Zorluklar

Artırılmış ve sanal gerçeklik teknolojilerinde, 3B modellerin yeri doldurulamaz bir öneme sahiptir. Ancak 3B sanatçı sayısı, bu ihtiyacı karşılamaktan oldukça uzaktadır. Ayrıca, sentetik nesnelerin gerçek nesnelere ayırt edilemeyecek derecede benzemesi istenmektedir ve bir tasarımcının bu becerileri kazanması uzun yıllar gerektiren zorlu bir süreçtir. Bu durum, artırılmış ve sanal gerçeklik alanında 3B modellerin önemi ve 3B sanatçılarına olan ihtiyacı oraya koymaktadır (Kavak Gökçek, Ş. & Akbulut, D., 2022).

İnovasyonun Ekonomik Alanlara Uygulanması

İnovasyon, yeni fikirlerin veya buluşların ekonomik alanlara uygun hale getirilip tatbik edilmesiyle mümkün olmaktadır. Bu süreç, genellikle iki yol üzerinden ilerlemektedir: birincisi, şirketler aracılığıyla gerçekleştirilen inovasyon faaliyetleri; ikincisi ise üniversiteler ve araştırma enstitüleri tarafından sağlanan inovasyon çalışmalarıdır. Bilimsel araştırmalarla yeni teknolojilerin ortaya çıkması, büyük avantajlara sahip olmakla birlikte maliyetli ve zaman alıcı bir süreçtir. Bu nedenle, birçok ülke dışarıdan gelen donanım ve yazılımlara güvenmek zorunda kalmaktadır. Ülke dışı yazılım ve donanım kullanmak ise uzun vadede daha maliyetli olabilmektedir. Yerli yazılım endüstrisini geliştirmenin stratejik önemini fark eden Çin Hükümeti, Çin'in yazılım endüstrisinin ve genel olarak yüksek teknoloji endüstrisinin büyümesini teşvik etmek için ücretsiz alan, yüksek teknoloji kuluçka merkezleri ve diğer ekonomik sübvansiyonlar sunan teşvik programları başlatmıştır (Muhammet Damar, 2022).

Hikâye Anlatımı: Reklamcılık ve Turizm Sektöründe Gerçeklik Teknolojileri

Reklamcılık sektörü, eğitim ve turizm gibi alanlarda hikâye anlatımı önemli bir fırsat sunmaktadır. Reklamlarda, kullanıcıya ürün veya hizmetler hakkında doğrudan bilgi sunmak yerine bir olay örgüsü anlatılması, reklamın bir araç olmaktan çıkıp müşterilerin yaşamlarından kesitler bulduğu sorunlara çözümler sunan önermelere dönüşmesini sağlar (Emine Şahin, 2018). Ancak artırılmış ve sanal gerçeklik teknolojilerini kullanarak kullanıcı kabulünü artırmak, metotlar geliştirmek bir dizi zorluk içerir. Bazı sektörlerde ise sanal gerçeklik teknolojisi kullanmak, risklerin ortaya çıkmasına neden olabilir. Örneğin, turizm sektöründe sanal gerçeklik teknolojisi, fiziksel seyahat turlarını olumsuz etkileyebilir. Bununla birlikte, sanal evrenlerde ilgili turistik yerlerin görülmesi, gerçek dünyada da görme arzusunu pekiştirebilir fikri de mevcuttur. Turizm sektör temsilcileri arasında farklı yaklaşımlar içeren bu konu belirsizliğini korumaktadır.

Silo Zihniyeti

Silo zihniyeti, bilgi paylaşmak istemeyen ve iş birliği yapmaktan kaçınan bir tutumu ifade eder. Bu zihniyet, bir şirket veya bölüm içinde zararlı olabileceği

gibi, artırılmış ve sanal gerçeklik iş modelleri için de engel teşkil etmektedir. Bu yaygın sorun, artırılmış ve sanal gerçeklik içeriğinin uygulanabilir ve kârlı olmasını sağlamak için aşılması gereken bir davranış olarak tanımlanır. Silo zihniyeti, farklı ekipler ve departmanlar arasında iş birliğini de engellemektedir. Bu zihniyet bilgi ve deneyim paylaşımını sınırlamakta ve yeni fikirlerin ortaya çıkmasını önlemektedir. Daha önce de ifade edilmiş olduğu gibi artırılmış veya sanal gerçeklik teknolojileri video oyun veya mobil oyun geliştirme araçları ile kodlanır. Bu süreçler birbirine son derece yakındır. Tüm gerçeklik teknolojileri (artırılmış, sanal, karma ve genişletilmiş gerçeklik) birlikte düşünüldüğünde ise oldukça büyük bir iş birliğinin gerekliliği ortaya çıkmaktadır. Dolayısı ile bilgi ve deneyim paylaşımı, tam anlamıyla sağlanması noktasında konuşulması gereken bir zorluk olarak ortaya çıkmaktadır.

Akademik-Endüstri İşbirliğinin Güçlendirilmesi

Akademisyenler, okullar ve endüstri arasındaki bağlantının güçlendirilmesi ve devletlerarası hareketliliğin teşvik edilmesi, akademik bilginin organik bir şekilde endüstriye aktarılmasının zorluklarını ortadan kaldırmak için önemlidir. Bu iş birliği, akademik dünyanın endüstriyel uygulamaları daha iyi anlamasını sağlarken, endüstriyel sektörlerin de akademik araştırmaların sonuçlarından yararlanmasına olanak tanır. Devletlerarası hareketlilik, akademisyenlerin ve endüstri profesyonellerinin farklı ülkelerde deneyim kazanmasını ve farklı kültürlerin, iş pratiklerinin ve inovasyon yaklaşımlarının paylaşılmasını sağlar. Bu sayede, akademik bilginin gerçek dünya sorunlarına uygulanması kolaylaşır ve endüstriye daha hızlı bir şekilde entegre olur. Bu noktada doğru bir okuma yapıldığı taktirde artırılmış gerçeklik teknolojisi ile gerçek dünya sorunlarının çözüme kavuşturulduğu birçok örneğin "Gerçeklik Teknolojilerinin Kullanıldığı Sektörler" başlığı altında irdelendiği görülecektir. Devletlerin akademik- endüstri iş birliğini teşvik etmek için politikalar geliştirmesi, destekleyici programlar oluşturması ve hareketliliği kolaylaştırması gerekmektedir. Bu cümlenin bir tavsiye seti içermediği, kendi içinde majör zorluklar barındırdığı ve bu zorlukların ifade edildiği gözden kaçırılmamalıdır.

Veri Gizliliği ve Kullanıcı İzni Başlıklarında Farkındalığın Artırılması

Veri gizliliği sorunları, yenilikçi çözümlerin geliştirilmesini tetikleyebilecek önemli bir konudur. Uygulama ve oyunların kullanımı sırasında verilen izinler ve gerçek zamanlı veri işleme veya toplanan verilerin sahipleriyle ilgili endişeler, kullanıcıların bu teknolojileri benimsemesini olumsuz etkileyebilir. Bu nedenle, daha fazla farkındalık oluşturulması gerekmektedir. Kullanıcıların verilerinin nasıl toplandığı, işlendiği ve paylaşıldığı konusunda şeffaf ve anlaşılır bir şekilde bilgilendirilmeleri önemlidir. Ayrıca, kullanıcıların verileri üzerinde daha fazla kontrol ve güvenlik sağlayan yöntemlerin geliştirilmesi ve bu yöntemlerin aktif olarak kullanılması gerekmektedir. Bu şekilde, kullanıcıların veri gizliliği konusundaki endişeleri azaltılabilir ve yenilikçi çözümlerin benimsenmesi teşvik edilebilir. Veri gizliliği konusunda daha fazla farkındalık oluşturulması hem kullanıcıların hem de şirketlerin güvenini artırarak, yenilikçi teknolojilere ve çözümlere olan talebi artırabilir.

3.2 Yasal Zorluklar

Yasal zorluklar genellikle artırılmış gerçeklik teknolojisinin doğası gereği anlık olarak büyük ölçeklerde kullanıcı verisi toplamasıyla alakalıdır. Bu verilerin toplanması, verilerin kullanım amacı, verilerin nerede tutulacağı ve bu verilere kimlerin erişebileceği konuları yasal düzenlemeler gerektirmektir. Ayrıca finansal zorluklar başlığı altında da değinecek olan bir konu olan girişimcilerin girişimlerinin başarısız olması durumunda onları koruyacak bir takım yasal tedbirlerin alınması da yasal zorluklar arasındadır. Bu başlık özelinde tanımlanmış zorluklar aşağıda listelenmiştir;

Veri İşleme ve Ağ Güvenliği

Emniyet ve güvenlik, artırılmış ve sanal gerçeklik teknolojilerinin yaygınlaşması için önemli bir faktördür. Kişisel verilerin işlenmesi ve ağ güvenliği konuları, düzenlemeler açısından dikkate alınması gereken hususlardır. Bu nedenle, ilgili kurumların emniyet ve güvenlik standartlarını belirlemek ve uygulamak için çalışmalar yapması beklenmektedir. Ancak Kurumları bir araya getirerek onlara birtakım sorumluluk yüklemek kendi içinde zorluklar içermektedir.

Yönetim ve Mevzuat Uyumunun Önem

Yönetim ve mevzuat konularında uyum sağlanması için birden fazla paydaşın iş birliği yapması gerekmektedir. Artırılmış ve sanal gerçeklik teknolojilerinin geliştirilmesi ve kullanımıyla ilgili olarak, hükümetler, düzenleme rolü üstlenen kamu kurumları, şirketler ve sivil toplum kuruluşları arasında birlikte çalışma ve standartlar oluşturma ihtiyacı vardır. Bu hem teknolojinin potansiyelini açığa çıkarmak hem de kullanıcıların güvenliğini sağlamak için önemlidir.

Sanal Gerçeklikte Kullanıcı Deneyimini Güçlendirmek

Artırılmış ve sanal gerçeklik teknolojilerinin tanıtılması için veri erişim ara yüzlerine ihtiyaç vardır. Bu ara yüzler, kullanıcıların verilere erişimini kolaylaştırır ve deneyimlerini geliştirirken veri güvenliği standartlarının uygulanmasına yardımcı olur. Kullanıcı beklenti ve deneyimlerinin, veri güvenliği standartlarına uygun olarak geliştirilen ara yüzlerle desteklenmesi, teknolojinin kabulünü hızlandırabilir.

3.3 Sosyal Alan Zorlukları

Sosyal hayata dair zorluklar genellikle kullanıcı kabulü başlığı altında şekillenmektedir. Kullanıcı kabulü ise aslında iş dünyasına dair zorluklardan teknolojik zorlukları kadar tüm mevcut zorluklardan bir nebze etkilenmektedir. Sosyal alan için tanımlanmış zorluklar aşağıda listelenmiştir;

Ebeveynlerin Artırılmış ve Sanal Gerçeklik Teknolojilerine İlişkin Kaygıları

Artırılmış veya sanal gerçeklik teknolojilerinin benimsenmesi sürecinde, ebeveynler arasında yaygın bir şüphecilik hali bulunmaktadır. Araştırma bulguları ebeveynlerin kaygılarının temelsiz olmadığını ortaya koymaktadır (Theiet Apr, 2022). Ebeveynler, çocuklarının güvenliği, sağlıklı gelişimi ve teknolojinin etkileri konusunda endişeler taşımaktadır. Bu nedenle, artırılmış ve sanal gerçeklik teknolojilerinin benimsenmesi sürecinde, ebeveynlerin kaygılarını anlamak ve bu kaygıları gidermek için bilgilendirme, eğitim ve güvenlik önlemleri gibi yöntemlerin kullanılması önemlidir. Araştırma bulgularına dayanarak, ebeveynlerin kaygılarının ciddiye alınması ve onların da teknolojiye ilişkin endişelerini çöz-

meye yönelik çözümler üretilmesi gerekmektedir.

Güvenlik ve Gizlilik Endişeleri

Diğer zorluk başlıkları altında da irdelenmiş olan güvenlik ve gizlilik endişeleri sosyal alan zorlukları başlığı altında da önemli bir yer tutmaktadır. Yeni nesil haberleşme teknolojileriyle birlikte, daha fazla veri transferi ve daha geniş bir ağ bağlantısı söz konusu olacaktır. Bu da güvenlik ve gizlilik endişelerini artırmaktadır. Özellikle, AR uygulamalarında kullanıcıların kişisel verilerinin korunması, güvenlik açıklarının önlenmesi ve izinsiz erişimlerin engellenmesi gibi konular önem kazanmaktadır. Bu zorlukların üstesinden gelmek kullanıcı kabulünü olumlu yönde etkileyecektir.

3.4 Teknolojik Zorluklar

Bilindiği gibi donanım üretimi oldukça maliyetli bir süreçtir. Sistemin işleyebilmesi için doğru malzemenin icadı bu malzemenin uygun fiyatlar ile erişebilir olmasının sağlanması ve bu süreçlerin organizasyonu maliyet çıktısının parametrelerini oluşturmaktadır. Gözlük üretiminden sonra birtakım haberleşme teknolojileri ile veri iletiminin sağlanması ve toplanan büyük verinin tutulup organize edilmesi birçok zorluk barındırmaktadır. Faklı açılardan teknolojik zorluklar ise aşağıda listelenmiştir;

Yüksek Çözünürlüklü İçerik ve Ağ Altyapısının Artırılmış ve Sanal Gerçeklikte Önemi

Artırılmış ve sanal gerçeklik teknolojilerinde kullanıcı deneyimini en üst düzeye çıkarmak için yüksek çözünürlüklü içeriğin büyük bir önemi vardır. Ancak, bu teknolojilerde yüksek bant genişliğine ihtiyaç duyulması, içeriklerin doğru algoritmalarla sunuculara yüklenip indirilmesi gerektiğini ortaya koymaktadır. Ağ altyapısının sağlamlığı, yüksek çözünürlüklü içeriğin kesintisiz bir şekilde kullanıcılara iletilmesinde kritik bir rol oynamaktadır. Bu nedenle, artırılmış ve sanal gerçeklikte kullanılan içeriklerin doğru şekilde sunuculara yüklenmesi ve kullanıcılara hızlı bir şekilde indirilmesi için gelişmiş algoritmalar ve sağlam ağ altyapısı gerekmektedir.

Haptik Teknolojiler

Haptik teknoloji, kinestetik iletişimi veya 3B dokunma deneyimini ifade eden bir teknolojidir. Şu anda bazı üst düzey endüstri çözümlerinde mevcut olsa da haptik teknoloji henüz erken aşamadadır. Ancak, daha geniş bir kullanıcı kitlesine ulaşması için daha fazla araştırma ve geliştirme çalışmalarına ihtiyaç duyulmaktadır. Haptik teknolojinin ilerlemesi, etkileşimli oyunlar, sanal gerçeklik deneyimleri, cerrahi simülasyonlar, eğitim ve daha birçok alanda büyük potansiyel taşımaktadır. Ancak, mevcut zorlukların aşılması ve kullanıcı deneyimini iyileştirmek için daha fazla çalışma yapılması gerekmektedir.

Artırılmış Gerçeklikle Birlikte Kullanılan Teknolojilerin Tanımlanması

Sürükleyici teknolojiler, genellikle artırılmış ve sanal gerçeklik teknolojileriyle ilişkilendirilse de tam olarak tanımlanmamış soyut yapıda kavramlar olarak havada kalmıştır. Birlikte kullanılan teknolojiler, artırılmış gerçeklik deneyimini destekleyen ve zenginleştiren araçlar olarak kabul edilir. Bu teknolojiler, haptik geribildirim, görsel algılamalar, yapay zeka, giyilebilir cihazlar gibi çeşitli disiplinleri içerebilir. Bu bağlamda, sürükleyici teknolojilerle ilgili araştırma ve çok disiplinli bir yaklaşım gereklidir. Farklı alanlardan uzmanların bir araya gelerek, artırılmış gerçeklik deneyimini zenginleştirecek ve geliştirecek teknolojik çözümler üzerinde çalışmaları önemlidir.

Endüstri 4.0'dan 5.0'a Geçiş

Endüstri 4.0'dan 5.0'a geçiş süreci başlamıştır ve bu geçiş, kullanıcı merkezli bir yaklaşımın sağlanmasını gerektirmektedir. Geleceğin endüstrilerinde kullanılabilirlik, memnuniyet ve gerçeklik teknolojilerinin kullanıcılar üzerindeki etkileri büyük önem taşımaktadır. Endüstri 5.0, insanlar ve yapay zekâ arasındaki iş birliğini vurgulayan bir dönüşümü ifade eder. Bu dönüşüm sürecinde, üretim süreçlerinin daha insana odaklı ve kullanıcı dostu hale getirilmesi hedeflenmektedir. Gerçeklik teknolojileri, bu süreçte önemli bir rol oynamaktadır. Endüstri 5.0'a geçişte gerçeklik teknolojilerinin kullanımıyla birlikte, kullanıcıların güvenliği, veri gizliliği ve etik sorunlarının da göz önünde bulundurulması önemlidir.

Altyapı Yetersizliği

Yeni nesil haberleşme teknolojilerinin etkili bir şekilde uygulanması geniş bant, düşük gecikme süresi ve yüksek kapasite gibi avantajlar sağlayacaktır. Ancak, bu altyapıyı sağlamak altyapı maliyetlerini ve mevcut ağ altyapısının karmaşıklığını artıracaktır. Bu nedenle, mevcut altyapı yetersizliği, yeni nesil haberleşme teknolojilerinin hızlı bir şekilde benimsenmesini ve uygulanmasını zorlaştırıcı bir rol oynayacaktır. Yeni nesil haberleşme teknolojilerinin gecikmesi ise tüm özellikleri ile aktifleştirilmiş artırılmış ve sanal gerçeklik uygulamalarının benimsenmesini logaritmik olarak artıracaktır.

Standartlar ve Uyum

Yeni nesil haberleşme teknolojileri ve AR uygulamalarının yaygınlaşması için standartlar oluşturulmalı ve uyum sağlanmalıdır. Farklı cihazlar, ağlar ve uygulamalar arasında uyumlu bir şekilde çalışabilmek elzemdir. Ayrıca, veri paylaşımı, veri güvenliği ve etkileşim protokolleri gibi konularda standartlar belirlenmelidir. Bu, farklı platformlar arasında etkili bir şekilde haberleşmeyi sağlayacak ve AR uygulamalarının yaygınlaşmasını destekleyecektir.

3.5 Finansal Zorluklar

Finansal zorluklar genellikler yatırımcı bulma süreci etrafında şekillenen ve girişim maliyetlerini düşürme ile alakalı bir durumdur. Finansal zorluklara ilişkin liste şu şekildedir;

Yenilikçi KOBİ'ler İçin Risk Teşvikli Finansman ve Koruyucu Yasaların Önemi

Artırılmış ve sanal gerçeklik teknolojilerine yatırım yapan şirketlerin risklerini minimize etmek amacıyla, bu teknolojilere yatırım yapan şirketler için koruyucu yasaların oluşturulması gerekmektedir. Yenilikçi KOBİ'lerin büyüme potansiyelini desteklemek için risk teşvikli finansman sistemleri oluşturulmalı ve koruyucu yasalar geliştirilmelidir (Strategic Paper).

Özel Finansmanın Artırılmış ve Sanal Gerçeklik Firmalarına Etkisi

Özel finansman, artırılmış ve sanal gerçeklik teknolojisi üreten firmaların sektöre giriş kararları sonrasında dikkate alınması gereken bir faktördür. Bu firmaların yetişmiş kalifiye personel yeteneklerine sahip olmaları, gerçeklik teknolojileri üzerinde geliştirme yapabilme kabiliyetine sahip olmaları maliyetleri düşürebilir. Özel finansmanın sağlanması, artırılmış ve sanal gerçeklik teknolojisi üreten firmaların başarılı bir şekilde sektöre giriş yapabilmeleri için önemlidir. Ancak, bu finansman sağlandıktan sonra doğru sektöre giriş yapıldığından emin olmak adına analizlerinin yapılması gerekmektedir. Bu nedenle, artırılmış ve sanal gerçeklik teknolojisi üreten firmaların özel finansmanla ilgili stratejik bir yaklaşım benimsemeleri ve sektöre giriş analizlerini doğru bir şekilde gerçekleştirmeleri önemlidir (Strategic Paper). Ancak Özel finansman elde etmek, özellikle yeni girişimler için zor olabilir. Yatırımcıların ve finansman sağlayıcılarının ilgisini çekmek ve ikna etmek zaman gerektirebilmektedir. Özellikle artırılmış ve sanal gerçeklik gibi yenilikçi teknolojiler birtakım ortak riskler barındırdığından finansman sağlayıcılarının çekingen bir tavır sergilemesi muhtemeldir. Kalifiye personel bulmak, özellikle bu teknolojilere hakim olan uzmanları işe almak zor olabilir. Bu alanda deneyimli profesyonellerin sınırlı olması, rekabeti artırabilir ve maaş beklentilerini yükseltebilir. Bu durum girişimcilerin finansman kaynağı bulmasını elzem kılarken finansman sağlayıcıları çekingen davranmaya itmektedir.

SONUÇ VE ÖNERİLER

Artırılmış, sanal, karma ve genişletilmiş gerçeklik teknolojileri, her sektörde kullanılmak üzere tasarlanmış çok yönlü teknolojilerdir. Bu teknolojilerin kullanımı, sektörlerin verimliliğini artırma, deneyimleri zenginleştirme ve yenilikçi fırsatlar sunma potansiyeline sahiptir. Ancak, bu teknolojilerin benimsenmesi ve etkili bir şekilde kullanılabilmesi önünde çeşitli zorluklar bulunmaktadır.

Bu çalışmada, iş dünyası, sosyal faktörler, teknolojik engeller ve finansal zorluklar gibi çeşitli alanlarda karşılaşılan zorluklar ele alınmıştır. Acil çözüm gerektiren problemler olduğu gibi zaman içinde kendiliğinden çözülebilecek sorunlar da mevcuttur. Özellikle veri güvenliği, düzenlemeler, kullanıcı kabulü ve finansman gibi konularda acil önlemler alınması elzemdir. Ancak, zamanla teknolojinin gelişmesi ile birlikte yeni zorlukların ortaya çıkması da kaçınılmazdır. Bu nedenle, iş dünyası, hükümetler, düzenleyici kurumlar, şirketler ve sivil toplum kuruluşları arasında iş birliği ve ortak çalışma oldukça önemlidir.

Sosyal kabulün artırılması, artırılmış ve sanal gerçeklik teknolojilerinin toplum tarafından daha iyi anlaşılması, değerinin fark edilmesi ve yaygınlaşması için önemli bir faktördür. Bu nedenle, teknolojiyi kullanarak organizasyonlar oluşturmak ve bu teknolojileri daha geniş bir kitleye tanıtmak için çalışmalar yapılması gerekmektedir. Organizasyonlar, sanatsal etkinlikler, eğitim programları, topluluk etkinlikleri ve bilinçlendirme kampanyaları gibi faaliyetler düzenlenerek artırılmış ve sanal gerçeklik teknolojilerinin potansiyeli gösterilmeli ve insanların bu teknolojilere daha olumlu reaksiyon göstermeleri sağlanmalıdır. Böylece, sosyal kabulün artmasıyla birlikte teknolojinin gelişimi hızlanacak ve daha geniş bir kullanıcı kitlesi tarafından benimsenecektir.

Sonuç olarak; gerçeklik teknolojileri, potansiyel fırsatlar sunduğu, fırsatları zamanında yakalama noktasında ise birtakım zorlukların bulunduğu tespit edilmiştir. Bu zorlukları aşmak ve teknolojinin tam potansiyelini açığa çıkarmak için ilgili taraflar arasında iş birliğinin sağlanması gerekliliği, düzenlemelerin güncellenmesi ve sürekli yenilikçi yaklaşımlar gerektiği izhar olmuştur. Bu sayede gerçeklik teknolojileri, daha geniş bir kitleye ulaşarak gelecekte sektörel ve sosyal dönüşümlere öncülük edebilecektir.

KAYNAKLAR

Aisling Ní Chúláin (2022). New AR Glasses Allow Deaf People to 'See' Conversations by Turning Audio into Subtitles. https://www.euronews.com/next/2022/07/29/new-ar-glasses-allow-deaf-people-to-see-conversations-by-turning-audio-into-subtitles adresinden 20 Haziran 2023 tarihinde alınmıştır.

Ayda Ayoubı (2017). IKEA Launches Augmented Reality Application. https://www.architectmagazine.com/technology/ikea-launches-augmented-reality-application adresinden 20 Haziran 2023 tarihinde alınmıştır.

Aytekin&Handan (2016). Müzelerde artırılmış gerçeklik uygulamaları: Sakıp Sabancı müzesi örneği. https://acikbilim.yok.gov.tr/handle/20.500.12812/552531 adresinden 20 Haziran 2023 tarihinde alınmıştır.

Berfin Çipa (2023). Metaverse bir balon mu yoksa geleceğin kendisi mi? https://www.ekonomim.com/sektorler/teknoloji/metaverse-bir-balon-mu-yoksa-gelecegin-kendisi-mi-haberi-690389 adresinden 20 Haziran 2023 tarihinde alınmıştır.

Better Health Channel (2023). The dangers of sitting: why sitting is the new smoking, https://www.betterhealth.vic.gov.au/health/healthyliving/the-dangers-of-sitting adresinden 20 Haziran 2023 tarihinde alınmıştır.

Kırıkkaya, E. B. ve, Şentürk. M. (15.01.2018). The ımpact of using augmented reality technology in the solar system and beyond unit on the academic achievement of the students. Kastamonu Education Journal, 26(1), 181 - 189. https://doi.org/10.24106/kefdergi.375861

Cem Kaya (2023). Yükseklik Fobisi. https://l24.im/aHlim adresinden 19 Haziran 2023 tarihinde alınmıştır.

Çankaya, G., Boyacı, A. ve Yarkan, S. (01.07.2020). Kızılötesi damar görüntüsü işleme ve damar tespiti. Teknoloji ve Uygulamalı Bilimler Dergisi, 3(2), 1-6. https://doi: 10.1109/IC3I.2014.7019808.

Dalle Mura, M., Dini, G. (2021). Augmented Reality in Assembly Systems: State of the Art and Future Perspectives. In: Ratchev, S. (eds) Smart Technologies for Precision Assembly. IPAS 2020. IFIP Advances in Information and Commu-

nication Technology, vol 620. Springer, Cham. https://doi.org/10.1007/978-3-030-72632-4_1

Devpost (2015). Augmented Reality - Antipersonnel Mines. https://devpost.com/software/ar-apm-augmented-reality-antipersonnel-mines adresinden 18 Eylül 2022 tarihinde alınmıştır.

Dylan Malyasov (2022). US Army incorporates augmented reality goggles into combat vehicles. https://defence-blog.com/us-army-incorporates-augmented-reality-goggles-into-combat-vehicles/ adresinden 20 Haziran 2023 tarihinde alınmıştır.

Ebru Avcı (2020). Artırılmış Gerçeklik teknolojisi turizm için neden önemli? https://www.turizmgunlugu.com/2020/02/01/artirilmis-gerceklik-teknolojisi-turizm/ adresinden 18 Ocak 2023 tarihinde alınmıştır.

Emine Şahin (2018). Reklam Stratejileri Kapsamında Hikaye Anlatımı Kullanımı: Sanal Marka Topluluklarında Reklam Mesajlarının Aktarımı. https://l24.im/2Xpu6f adresinden 20 Haziran 2023 tarihinde alınmıştır.

Erer, S. & Atıcı, E. (2010). Selçuklu ve Osmanlılarda Müzikle Tedavi Yapılan Hastaneler. Uludağ Üniversitesi Tıp Fakültesi Dergisi, 36 (1), 29-32. Retrieved from https://dergipark.org.tr/tr/pub/uutfd/issue/35281/391528

Furkan Gençoğlu (2021). Türk Telekom'un 5G bağlantısı ile çevrim içi ameliyat gerçekleştirildi. https://www.aa.com.tr/tr/sirkethaberleri/bilisim/turk-telekomun-5g-baglantisi-ile-cevrim-ici-ameliyat-gerceklestirildi/668281 adresinden 20 Haziran 2023 tarihinde alınmıştır.

Hsu, T. (2017). Learning english with augmented reality: do learning styles matter?. Computers&Education, 106, 137-149. https://doi.org/10.1016/j.compedu.2016.12.007

Infodefensa (2018). Airbus presenta su cajón de arena militar de realidad aumentada. https://www.infodefensa.com/texto-diario/mostrar/3074662/airbus-presenta-cajon-arena-militar-realidad-aumentada adresinden 18 Ocak 2023 tarihinde alınmıştır.

James Şilin (2019). KLM Debuts "Try Before You Fly" Augmented Reality Campaign Ads. https://www.insidertravelreport.com/klm-debuts-try-befo-

re-you-fly-augmented-reality-campaign-ads adresinden 18 Ocak 2023 tarihinde alınmıştır.

Kavak Gökçek, Ş. & Akbulut, D. (2022). Bağımsız Video Oyunlarının Geliştirilme Sürecinde Oyun Tasarımına Yönelik İhtiyaçların, Problemlerin, Benzerliklerin ve Farklılıkların Keşfedilmesi İçin Bir Alan Çalışması . Sanat ve Tasarım Dergisi , - (30) , 187-207 . Retrieved from https://dergipark.org.tr/tr/pub/sanat-vetasarim/issue/73722/1215230

Kayadibi, F. (2001). Eğitim Kalitesine Etki Eden Faktörler ve Kaliteli Eğitimin Üretime Katkısı. Journal of Istanbul University Faculty of Theology, 0 (3). Retrieved from https://dergipark.org.tr/tr/pub/iuilah/issue/967/10911

Kinjoll Dey (2023). Global Augmented Reality in Healthcare Overview. https://l24.im/szkxj0f 20 Haziran 2023 tarihinde alınmıştır.

KKB Kliniği ve ARGE Merkezi (2023). Denge Sisteminin Anatomisi. https://kbbarge.com/kbb/denge-sisteminin-anatomisi/ adresinden 20 Haziran 2023 tarihinde alınmıştır.

Künüçen, H. H. & Samur, S. (2021). Dijital Çağın Gerçeklikleri Sanal, Artırılmış, Karma ve Genişletilmiş Gerçeklikler Üzerine Bir Değerlendirme. Yeni Medya, 2021 (11), 38-62. Retrieved from https://dergipark.org.tr/tr/pub/yenimedya/issue/67044/995540

Liu, H., Wang, Z., Musa, H. ve Kao, D. (2020, 12). Virtual reality racket sports: virtual drills for exercise and training [Bildiri sunumu]. Porto de galinhas, Brazil.

Motion Systems (2023). Motıon Platforms, https://motionsystems.eu/ adresinden 20 Haziran 2023 tarihinden alınmıştır. (20.06.2023)

Muhammet Damar (2022). Dijital Dünyanın Dünü, Bugünü Ve Yarını: Bilişim Sektörünün Gelişimi Üzerine Değerlendirme. https://dergipark.org.tr/en/download/article-file/2449247 adresinden 6 Temmuz 2023 tarihinde alınmıştır.

Mütem (2023). Müzik Terapi Uygulama ve Araştırma Merkezi. https://uskudar.edu.tr/mutem/tr/hakkinda adresinden 19 Haziran 2023 tarihinde alınmıştır.

Nilüfer Koca (2023). Eğitici Kartların Faydaları. https://welcomebaby.com.tr/blog/egitici-kartlarin-faydalari adresinden 20 Haziran 2023 tarihinde alınmıştır.

Octagon Studio (2022). Humanoid 4D+. https://play.google.com/store/apps/details?id=com.OctagonStudio.ARSkeletal&hl=tr&gl=US&pli=1 adresinden 20 Haziran 2023 tarihinde alınmıştır.

Orta Anadolu İhracatçılar Birlikleri (2023). Dış Pazarlara Açılırken Karşılaşılan Sorunlar Nelerdir? https://oaib.org.tr/tr/bilgi-merkezi-sikca-sorulan-sorular-dis-pazarlara-acilirken-karsilasilan-sorunlar-nelerdir.html adresinden 20 Haziran 2023 tarihinde alınmıştır.

Otel Satın Alma Müdürleri ve Eğitimi Derneği (2020). Turizm Nedir? https://www.osmed.com.tr/turizm-nedir/ adresinden 18 Ocak 2023 tarihinde alınmıştır.

Psikiyatri Hemşireliği (2019). Sosyal Anksiyeteye Müdahalede Teknolojik Bir Araç:

Sanal Gerçeklik. https://jag.journalagent.com/phd/pdfs/PHD-75010-REVIEW-OZER.pdf adresinden 19 Haziran 2023 tarihinde alınmıştır.

Radboud Universiteit (2021). A Whole New Customer Experience: The Use Of Augmented Reality İn The B2B Versus The B2C Sector. https://theses.ubn.ru.nl/server/api/core/bitstreams/c84f0570-6ccd-4e8d-aea2-686ec4e1fdb3/content adresinden 20 Haziran 2023 tarihinde alınmıştır.

Rangoli, (2023). Top Global Brands that are Going Big on Metaverse. https://www.analyticsinsight.net/top-global-brands-that-are-going-big-on-metaverse/ adresinden 20 Haziran 2023 tarihinde alınmıştır.

Savunma Haber (2021). ASELSAN Sivas ve BİTES, Yerli ve Milli Arttırılmış Gerçeklik Gözlüğü için El Sıkıştı. https://www.savunmahaber.com/bites-aselsan-sivas-yerli-arttirilmis-gerceklik-ar-gozlugu/ adresinden 19 Haziran 2023 tarihinde alınmıştır.

Savunma Haber (2022). BİTES'in Artırılmış Gerçeklik Tabanlı Zırh Ötesi Görüş Sistemi, Envantere Girmeye Hazırlanıyor, https://www.savunmahaber.com/bitesin-artirilmis-gerceklik-tabanli-zirh-otesi-gorus-sistemi-envantere-girmeye-hazirlaniyor/ adresinden 18 Eylül 2022 tarihinde alınmıştır.

Sensor Tower (2022). State of Mobile 2022. https://www.data.ai/en/go/state-of-mobile-2022/ adresinden 6 Temmuz 2023 tarihinde alınmıştır.

Sönmez, H. Ş. ve Zarbızade, V. (31.01.2022). Müzelerde deneyimsel pazarlama aracı olarak artırılmış gerçeklik uygulamalarının tüketiciler üzerindeki etkileri: seka kağıt müzesi örneği. Anadolu Üniversitesi İletişim Bilimleri Fakültesi Uluslararası Hakemli Dergisi, 30(1), 1-20. https://dergipark.org.tr/en/pub/kurgu/issue/68336/797765

Strategic Paper (2022). Publication Detail (s. 35-36). https://op.europa.eu/en/publication-detail/-/publication/9aaef6fd-28db-11ed-8fa0-01aa75ed71a1 adresinden 6 Temmuz 2023 tarihinde alınmıştır.

Theiet Apr (2022). Generation VR. https://www.theiet.org/media/press-releases/press-releases-2022/press-releases-2022-april-june/19-april-2022-generation-vr/ adresinden 20 Haziran 2023 tarihinde alınmıştır.

Tricia McKinnon (2022). 10 of the Best Augmented Reality (AR) Shopping Apps to Try Today. https://www.indigo9digital.com/blog/how-six-leading-retailers-use-augmented-reality-apps-to-disrupt-the-shopping-experience adresinden 20 Haziran 2023 tarihinde alınmıştır.

Vision Pro (2023). Vision Pro. https://www.apple.com/apple-vision-pro/ adresinden 20 Haziran 2023 tarihinde alınmıştır.

Zeynep Oğuzhan (2018). Antik Dönemden 16 Farklı Zar ve Masa Oyunu. https://arkeofili.com/antik-donemden-16-farkli-zar-ve-masa-oyunu/ adresinden 20 Haziran 2023 tarihinde alınmıştır.

BİLGİSAYAR TEMELLİ UYGULAMALAR İLE SPORCULARDA DİKKAT VE ALT BİLEŞENLERİNİN TESPİT EDİLMESİ: BİR LABORATUVAR ÇALIŞMASI

Merve ERDOĞDU[1]

Gizem AYTAÇ[2]

Gökhan DELİCEOĞLU[3]

Özet

Amaç: Sporcularda dikkat ve alt bileşenlerine ilişkin problemlerle sıklıkla karşılaşılmaktadır. İlgili literatür incelendiğinde, özgül yöntemlere ihtiyaç duyulduğu düşünülmektedir. Bu bağlamda şimdiye dek genellikle tercih edilmiş olan yöntem ve kullanılan ölçütlerin çoğunun, geleneksel uygulamalar ile kısıtlı bir içeriğe sahip olduğu ve yeniden test edilebilir ve somut değerlendirmeler için elverişli olmadığı gözlemlenmiştir. Bu çalışmada, milli sporcularda dikkat ve alt bileşenleri, bilgisayar temelli uygulamalar ile araştırılmıştır. Çalışmanın amacı, sporcuların dikkat düzeylerinin; zamanlama, planlama ve performansı sürdürme gibi beceriler üzerinde etkisinin olup olmadığını deneysel yöntemlerle incelemektir. **Gereç ve Yöntem:** Araştırmanın örneklemi Ankara ilindeki 143 kadın, 229 erkek olmak üzere toplam 327 sporcudan oluşmaktadır. Araştırmada gönüllük esas alınıp rastgele örneklem yöntemi ile uygun örnekleme Psikoloji Araştırmaları Laboratuvarı'nda (PAL) uygulanmıştır. Ölçüm, bilgisayar ortamında simule edilmiş, çoklu karıştırıcı ve çeldiricilerin bulunduğu görsel, işitsel ve nötr uyarılarla tasarlanmış bilgisayar temelli uygulama ile sporcularda dikkat ve alt bileşenleri değerlendirilerek tamamlamıştır. Psikolojik yorgunluğun etkisini ölçmek için, Bilgisayar Tabanlı Çeldiricili Sürekli Performans Testi uygulanmıştır. Katılımcılara test boyunca değişen uyarıcılara karşın beklenen reaksiyonu vermesi görevi verilmiştir. Değişen çeşitli koşullar günlük yaşamın dijital bir taklidi ve simule edilmiş versiyonu olarak tasarlanmıştır. Böylece, katılımcıların farklı durumlardaki performansı hakkında bilgiler elde edilmiştir. Bunlara ek olarak bilgisayar ortamında uygulanan deneyler ile Web tabanlı ortamlarda gerçekleştirilen araştırmaların avantajları/dezavantajları ve dezavantajlarının hangi yöntemlerle giderilebileceğinden bahsedilmiştir. **Bulgular:** Yapılan analizler sonucunda, dikkat ile zamanlama arasındaki pozitif ilişki ve dürtüsellik ile hata puanları toplamı arasındaki negatif ilişki yer almaktadır. **Sonuç:** Bu çalışmanın, dikkate ilişkin psikoloji uygulamaları alan yazınına katkı sağlayacağı düşünülmektedir. Dikkat çalışmaları bilgisayar tabanlı ölçümler perspektifinden analiz edildiğinde, elde edilen sonuçların uygulamalı psikoloji alanlarındaki çalışmalara destek olacağı ileri sürülebilir.

Anahtar Kelimeler: *Çevrimiçi deneyler, dikkat, performans, psikoloji, spor.*

1 Doktorant, Hacettepe Üniversitesi Adli Bilimler A.B.D. Adli Psikoloji, merve.erdogdu@hacettepe.edu.tr ORCID: 0000-0002-3745-2639

2 Uzm. Psk., Ankara Üniversitesi, Sağlık Bilimleri Enstitüsü, gizem.aytac@gsb.gov.tr ORCID: 0000-0002-7251-2318

3 Doç. Dr. Gazi Üniversitesi, Spor Bilimleri Fakültesi, deliceoglugokhan@gmail.com ORCID:0000-0003-2459-920

DETECTION OF ATTENTION AND ITS SUB-COMPONENTS IN ATHLETES WITH COMPUTER-BASED APPLICATIONS: A LABORATORY STUDY

Abstract

Aim: Problems related to attention and its sub-components are frequently encountered in athletes. When the relevant literature is examined, it is thought that specific methods are needed. In this context, it has been observed that most of the methods and criteria used so far have a limited content with traditional applications and are not suitable for retestable and concrete evaluations. In this study, attention and its subcomponents in national athletes were investigated with computer-based applications. The aim of the study is to experimentally examine whether the attention levels of athletes have an effect on timing, planning and performance maintenance skills. Materials and Methods: The sample of the study consists of a total of 327 athletes, 143 women and 229 men, in Ankara. The study was conducted on a voluntary basis and with the random sampling method, convenient sampling was applied in the Psychology Research Laboratory (PAL). The measurement was completed by evaluating the attention and sub-components of the athletes with a computer-based application simulated in the computer environment, designed with visual, auditory and neutral stimuli with multiple mixers and distractors. In order to measure the effect of psychological fatigue, the Computer-Based Continuous Performance Test with Distractor was applied. The participants were given the task of giving the expected reaction to the changing stimuli throughout the test. It is designed as a digital imitation and simulated version of daily life in various changing conditions. Thus, information was obtained about the performance of the participants in different situations. In addition to these, the advantages/disadvantages and disadvantages of the experiments carried out in the computer environment and the researches carried out in the Web-based environments are mentioned. **Results:** As a result of the analysis, there is a positive relationship between attention and timing, and a negative relationship between impulsivity and the sum of error scores. **Conclusion:** It is thought that this study will contribute to the literature on psychology practices related to attention. When attention studies are analyzed from the perspective of computer-based measurements, it can be argued that the results obtained will support studies in the fields of applied psychology.

GİRİŞ

Dikkat, belirli bir konu, olay veya durum üzerine zihinsel bir gayret sarf ederek yoğunlaşıldığında/odaklanıldığında ortaya çıkan, zihnin açık ve alarmda olduğu durumdur. Dikkat, öğrenilmek istenen konuya odaklanmayı sağlayan bir olgu olduğu için öğrenmenin önemli bir şartıdır. Dikkatin pek çok tanımı bulunmaktadır ancak genel anlamda zihnin konuyla alakasız uyaranları eleyerek hedef konuya, duruma veya nesneye odaklanması şeklinde tanımlamak mümkündür. Dikkatin 6 alt çeşidi vardır. Bunlardan ilki olan seçici dikkat, kişinin alakalı duruma odaklanıp reaksiyon gösterirken alakasız durumlara karşı herhangi bir tepki vermemesidir. Bir diğer alt tür olan yoğunlaşmış dikkat, ortamda birden fazla uyaran bulunduğunda gözlenir ve bu dikkat türünde kişi ortamdaki belirli bir uyaranı seçer ve dikkatinin kaynağını değiştirmeden ona odaklanır. Üçüncü tür olan sürekli dikkatte kişi dikkatini belli bir duruma/konuya odaklar ve uzun süre bu odağı sürdürür. Bölünmüş dikkat ise aynı zaman diliminde birden fazla harekette bulunulması gerektiğinde, kişi bu görevlere ayrı ayrı dikkatini verebildiği zaman oluşur. Bu dikkat türünde, dikkatin yönlendirildiği çoğul uyaran vardır ve dikkat bu uyaranlara bilinçli bir şekilde dağıtılır. Bir diğer tür olan değişken dikkat, kişi bir duruma dikkatini odaklamışken dikkat hedefinin birden değişmesiyle ortaya çıkar. Son alt tür olan dağınık dikkat ise kişinin herhangi bir konuya, duruma veya nesneye dikkatini odaklayamaması durumudur. Bu durumun temel nedeni kişinin zihninde başka problemlerle uğraşıyor olmasıdır. Zihnin sürekli alarm halinde olması ve sakinleşememesi, yetersiz motivasyon ve stres bu durumun bazı kaynaklarındandır (van Ede ve Nobre, 2022).

Dikkati etkileyen faktörler; psikolojik, zihinsel, çevresel ve fiziksel olabilmektedir. Bilişsel fonksiyonlar ve kabiliyetler zihinsel faktörlere; motivasyon ve amaç eksikliği, kaygı, fazla heyecan ve diğer ruhsal sıkıntılar psikolojik faktörlere; gürültü, ışık, yüksek/düşük sıcaklık çevresel faktörlere; uyku ve beslenme problemleri ise fiziksel faktörlere örnek olarak gösterilmektedir. Dikkat unsuru spor faaliyetlerinde oldukça önemlidir çünkü sporda ilgili uyaranı dikkatin hedefi olarak almak ve dikkat odağını bu uyaran üzerinde sabitlemek başarı getirir. Bundan dolayı sporcuların dikkat seviyelerini ölçmek ve dikkatin hangi unsurlarla ilişkili olduğunu, performansı nasıl etkilediğini ve nasıl artırılabileceğini belirlemenin sporcularımıza fayda getireceği düşünülmektedir (Erdoğdu, Aytaç ve Aydın, 2023; Ulukan, 2020). Sporda hedeflenen yüksek performansa ulaşabilmekte dik-

kat son derece önemli bir etkendir. Sporcuların ve antrenörlerinin hedeflenen performans seviyesine erişebilmeleri için özellikle karar verme ve dikkat stratejilerinin yüksekliği önem arz etmektedir. Spor ve egzersiz çalışmalarına paralel olarak dikkate yönelik çalışmaların da antrenman rutinlerine eklenmesi hem zihinsel hem fiziksel performansa katkı sağlayacak, odaklanmayı üst seviyelere taşıyacaktır. Tüm bu süreçler göz önüne alındığında, dikkatin kontrol edilebilmesi ve dikkatin yoğunlaştırılabilmesinde herhangi bir problem olup olmadığına ilişkin ölçümler yapılması gerektiği ve ihtiyaç duyulan durumlarda, sporcunun değişkenlerine uygun olduğu uzmanlarca karar verilen, dikkatini geliştirmeye katkı sağlayacak eğitimler düzenlenmesi gerektiği saptanmıştır. Alanyazın tarandığında dikkatin çeşitli alt boyutlarını ve düzeyini tespit etmeye yönelik pek çok farklı ölçeğe rastlanmaktadır. Bu ölçeklere örnek vermek gerekirse; "Burdon Dikkat Testi", "Benton Görsel Bellek Testi", "Frostig Görsel Algılama Testi", "MOXO Sürekli Performans Testi"," Bender Gestalt Görsel Motor Algı Testi" ve "D2 Dikkat Testi" gibi örnekler, bu testlere örnek olarak düşünülebilir (Woo, Rajagopalan ve Andamon, 2022).

Dikkat eksikliği hiperaktivite bozukluğu (DEHB), nörogelişimsel bir bozukluk olup çoğunlukla ilk belirtilerini erken çocukluk döneminde göstermektedir ve bu belirtiler yetişkinlikte de devam edebilmektedir. DEHB çoğunlukla kendini, dikkatin dağılması ve dikkati toparlayamama, dürtü kontörlünde zorlanma, aşırı hareketlilik gibi olgularla gösterir.

Diğer canlıların beyin gelişimi ve sinir hücrelerindeki esneklik göz önüne alındığında insanlardaki benzer süreçler daha uzun sürmektedir. Bu özellik, insanoğluna yüksek düzeyde öğrenme kapasitesi sağlamakla birlikte henüz gelişim sürecinde olan beyni, dışsal etkilere karşı incinebilir hale de getirmektedir. Dikkat eksikliği hiperaktivite bozukluğu, öğrenme ve dil bozuklukları gibi başta nörogelişimsel bozukluklar olmak üzere pek çok psikiyatrik bozukluğun incelenmesi neticesinde, bu bozuklukların, erken çocukluk dönemindeki genetik ve çevresel sapma ya da aksamalarla ilişkisinin olabileceği bulunmuştur (Berger, Lev, Braw, Elbaum, Wagner ve Rassovsky, 2021).

Bireylerin hayatın ileriki dönemlerinde dikkat performansında düşüklük, uzun vadeli takip edildiğinde ise gelişimsel bozukluklar, yeme ve uyku bozuklukları, dikkat, öğrenme, hafıza ve bilişsel bozukluklara rastlanmıştır ve daha

fazla antisosyal ve depresif davranışlar sergiledikleri fark edilmiştir (Karabekiroğlu, 2007). Seslerin işlenip beyne iletilmesinden sorumlu olan stapes vetensör timpani kaslarındaki eşgüdüm problemi, dikkat eksikliği ve hiperaktivite bozukluğunun oluşmasında rol oynamaktadır. Stapes vetensör timpani kasları, gelen sesi işledikten sonra anlamlandırarak beyne iletir. Bahsi geçen kas grubundaki tembellik ise dışarıdan gelen seslerin yeterince etkili işlenmemesine sebep olur ve bilgiler yanlış olarak beyne veya eksik şekilde iletilir. İletilmek istenen bilgi ya da uyaranın beyne yanlış ya da eksik şekilde iletilmesi de bu kişilerdeki dikkat eksikliği ve hiperaktivite bozukluğu ile ilişkilendirilmektedir (Slobodin, Blankers, Kapitány-Fövény, Kaye, Berger, Johnson, Demetrovics, van den Brink ve van de Glind, 2020). Benzer şekilde işitme engelli sporcuların davranışlarında da bu durum sıklıkla gözlenebilmektedir. Dikkat eksikliği ve hiperaktivite bozukluğu, sporcuların profesyonel spor hayatlarında çeşitli problemlerin yaşanmasına sebep olmaktadır ve tedavi edilmesi gerekmektedir (Berger ve Cassuto, 2014; Erdoğdu, Artuner, Demirbaş ve Aytaç, 2022).

DİKKAT- PERFORMANS İLİŞKİSİ

Sporcularda gözlenen dikkat-performans ilişkisini etkileyen faktörlerden birinin imgeleme olduğu gözlemlenmiştir. İmgeleme, bir eylemin harekete geçmeden, yalnızca zihinden hayal edilerek, mental ortamda gerçekleşmesi durumudur. Sporcuların performans bilgileri, Burdon Dikkat Testi ve Sporda İmgeleme Envanteri kullanılarak yapılan bu çalışmada, sporcuların dikkat testi sonuçları ve performans seviyeleri ile imgeleme envanterinden gelen sonuçların ilişkisi incelenmiştir. Araştırmanın sonucunda, dikkat seviyesinin sporcuların performansıyla pozitif yönde bağlantılı olduğu gözlemlenmiştir. Bunlara ek olarak, destekleyici ailelerde yetişen ve destekleyici antrenörlere sahip olan okçuların dikkat düzeylerinin; engelleyici, eleştirel ve umursamaz ailelerde yetişenlere ve bu tarz antrenörlere sahip olanlara göre daha yüksek olduğu görülmüştür. Ayrıca, algılanan antrenör desteğinin de sporcunun dikkatinde anlamlı bir etki yarattığı bulunmuştur. Dikkatin performansla pozitif yönde ilişkili olduğu düşünülecek olursa, bu faktörlerin iyileştirilmesinin, dikkati etkileyerek dolaylı yoldan performans gelişimine de katkı sağlayabileceği bildirilmiştir (Erdoğdu, Artuner, Demirbaş ve Aytaç, 2022; Ulukan, 2020).

Atletik uzmanlığın dikkat, işleyen bellek kontrolü-kapasitesi ve motor beceri-

lerle ilişkisi ile işleyen bellek kontrolü-kapasitesinin dikkat-performans ilişkisine etkisini inceleyen bir çalışma da Birleşik Krallıktaki basketbol akademisindeki atletler üzerinde yürütülmüştür. Bu çalışmadaki atletler, ortalama 18-19 yaşlarında olup %54'ü erkektir. Katılımcılar acemi, amatör, deneyimli ve çok deneyimli olmak üzere kategorilere ayrılmış ve bu katılımcılara sürekli görsel dikkati, hız/doğruluk değişimi ile görsel aramayı, işleyen bellek kapasitesini ve işleyen bellek kontrolünü ölçen testler uygulanmıştır. Sürekli görsel dikkat, The Rapid Visual Information Task (Hızlı Görsel Bilgi Testi) kullanılarak ölçülmüştür. Bu testte ekranın ortasında 2'den 9'a kadar olan sayıları gelişigüzel bir şekilde gösteren beyaz bir kutucuk bulunmaktadır ve katılımcılar kutucuğun yanında verilen belirli bir sayı sıralamasına (ör. 3-5-7) göre kutucukta o sayılar belirdikçe bir tuşa basmaktadır. Bu testte yüksek skorlar almak iyi performansın göstergesi olarak gösterilmektedir. Katılımcılar, belirtilen değişkenlerle alakalı testleri çözmüş ve yapılan analizler sonucunda işleyen bellek kontrolünün ve kapasitesinin performans-dikkat ilişkisi üzerinde pozitif bir aracı etkisi yarattığı gözlenmiştir. Başka bir deyişle, işleyen bellek kapasitesi ve kontrolü, dikkatin motor becerilerdeki performansı etkilemesinde aracı görevi görmektedir. Aynı zamanda, literatürdeki diğer çalışmaları doğrulayacak şekilde, bu çalışmada da işleyen bellekle alakalı ölçümlerin dikkatle alakalı ölçümlerle pozitif bir ilişkisi olduğu gözlenmiştir (Gupta, Kar ve Srinivasan, 2011; Vaughan ve Laborde, 2020; Garaizar, Vadillo, López-de-Ipiña ve Matute, 2014). Bu sonuçlar, sporcularda işleyen belleğin geliştirilmesinin dikkati ve dolayısıyla performansı iyileştirmeye yardımcı olabileceğini işaret edebilmektedir.

BİLGİSAYAR TABANLI DİKKAT ÖLÇÜMÜ

Yukarıdaki araştırma sonuçlarında da belirtildiği üzere, dikkatin sporcuların performansı üzerindeki etkisi azımsanamayacak boyuttadır. Bireylerin başarısını etkileyen önemli faktörlerden biri olan dikkat, DEHB gibi bozukluklar sonucu zarar görmektedir. Bu nedenle DEHB ve buna benzer bozuklukların tanısının mümkün olan en doğru biçimde yapılması önem arz etmektedir. DEHB'nin bilişsel bileşenlerinden dikkat, dürtüsellik, zamanlama ve hiperaktivitenin ölçüldüğü testlerden biri olan MOXO-d-CPT (Distracter – Continuous Performance Test), dijital ortamda gerçekleştirilen bir uygulamadır ve kişinin hedef uyaranı gördüğünde belirtilen klavye tuşuna basması şeklinde yapılmaktadır. Uygulama

esnasında kişi sesli ve görüntülü (bazen tek, bazen bir arada), çeldirici uyaranlara maruz kalır ve bu uyaranların etkisi altındayken ve değilken performansı ölçülmektedir. MOXO Dikkat Performans Testinin, teşhislerde doğruluk ve tutarlılık seviyesiyle ilgili araştırmalar yürütülmektedir.

MOXO-CPT testinin DEHB konusundaki tespit doğruluğunun anlaşılabileceği bir çalışma DEHB ve madde kullanım bozukluğu hastaları üzerinde yürütülmüştür. Çalışmaya 18-65 yaş arası ve Avustralya'dan (n=106), İsrail'den (n=56), Bulgaristan'dan (n=146), ve Amerika'dan (n=178); yalnızca DEHB'ye sahip (n=56), yalnızca madde kullanım bozukluğuna sahip (n=150), hem DEHB hem madde kullanım bozukluğuna sahip (n=108), hastalar ve kontrol grubu olarak sağlıklı bireyler (n=172) kullanılmıştır. Katılımcıların demografik bilgileri edinildikten ve hastalıkların tanısı konulduktan sonra MOXO-CPT uygulanmıştır. Bu araştırmada bütün çok değişkenli analizler çoklu karşılaştırmalar için Tukey doğrulamasıyla yapılmış, Cohen etki büyüklüğü hesaplanmış ve araştırmanın sonucunda Tukey ile doğrulanmış post hoc testlerde sağlıklı bireylerin MOXO-CPT sonuçlarının, üç klinik grubun da sonuçlarından, "zamanlama" kategorisi hariç anlamlı boyutta farklılaştığı görülmüştür. Buna ek olarak, DEHB hastaları, madde kullanım bozukluğuna sahip olsalar da olmasalar da "hiperaktivite" kategorisinde, yalnız madde kullanım bozukluğuna sahip olanlardan anlamlı boyutta farklı sonuçlar almışlardır. Cohen d değeri bütün anlamlı farklılıklar için orta-büyük etki büyüklüğü (0.35-0.74) göstermiştir. Ayrıca, en büyük anlamlı grup farklılığı, sağlıklı kontrol grubu ve DEHB grubu arasında, "hiperaktivite" ve "dürtüsellik" kategorisinde görülürken (d=0.74 ve d=0.66), bu farkı, "dikkat" kategorisinde madde bozukluğu grubunun kontrol grubuyla farkı (d=0.62) ve ardından, kontrol grubu ile hem DEHB hem madde bozukluğundan müzdarip hastaların farkı (d=0.58) izlemiştir (Lev, Elbaum, Berger ve Braw, 2022). Bütünüyle bakıldığında bu sonuçlar, MOXO-CPT testinin DEHB hastalarını sağlıklı bireylerden ayırabildiğini göstermekte ve DEHB tanısı için kullanılabilir olduğunu ifade etmektedir (Slobodin vd., 2020; Miguel, Martins, Moleda vd., 2016; Liebrenz vd., 2015; Tamm vd., 2013; Berger ve Goldzweig, 2010). Bu araştırmadan ve bahsedilen diğer çalışmalardan elde edilen sonuçlar, dikkat ile sporun çift yönlü, karşılıklı bir etkileşim içinde olduğunu göstermektedir (İnce ve Yıldırım, 2018; Zwierko, Florkiewicz, Fogtman ve Kszak-Krzyżanowska, 2014; Ziereis ve Jansen, 2015; Wulf ve Prinz, 2001).

GEREÇ VE YÖNTEM

Bu bölümde, araştırmada kullanılan örneklemin ölçütleri, katılımcıların demografik özellikleriyle ilgili bilgiler, veri toplama araçlarının psikometrik özellikleri ve veri analizi ile ilgili bilgilere yer verilmiştir. Nicel analizler içinde betimsel analizler, t testi ve regresyon analizleri yer almaktadır.

ÇALIŞMA POPÜLASYONU

Bu araştırmanın evrenini Ankara'ya sağlık ölçümlerine gelen sporcular oluşturmaktadır. Örneklem için bazı dahil edilme ölçütleri belirlenmiştir. Araştırma, GSB'ye ait Ankara-Etimesgut ilçesinde bulunan Sporcu Sağlığı, Performansı ve Hizmet Kalite Standartları Daire Başkanlığı Psikolojik Değerlendirme ve Müdahale Birimi Psikoloji Araştırmaları Laboratuvarı (PAL)'nda yapılmıştır. Araştırmanın örneklem sayısının belirlenmesi hususunda sezon içerisinde birime başvuru yapan kayıt verileri dikkate alınmıştır. Dahil edilme ölçütleri, test performansını etkileyebilecek görme ya da işitme kusuru olmayan, renk körlüğü tanısı almamış, yani normal görsel keskinliğe ve normal işitme yetisine sahip, psikiyatrik ve/veya nörolojik hastalık tanısı almamış olan bireylerden oluşmaktadır. Çalışma 18-30 yaş arasındaki Atıcılık, Atletizm, Buz Pateni, Curling, Eskrim, Hentbol, Judo, Modern Pentatlon, Sutopu, Tenis ve Voleybol branşlardaki 143 kadın, 229 erkek, toplam 327 milli sporcu ile bilgisayar üzerinden Psikoloji Araştırmaları Laboratuvarında (PAL) uygulanmıştır.

ÇALIŞMA DİZAYNI VE PROTOKOLÜ

Verilerin Toplanması: Bu çalışma, T.C. Gençlik ve Spor Bakanlığı (GSB) Türkiye Olimpiyatlara Hazırlama Merkezi (TOHM) bünyesinde yarışmalara hazırlanan ve Sporcu Sağlığı, Performansı ve Hizmet Kalite Standartları Daire Başkanlığı Psikolojik Değerlendirme ve Müdahale Birimine sağlık kontrolleri için başvuru yapan 18-30 yaş arasındaki milli sporcuları kapsamaktadır. Ayrıca çalışma, sporcuların dikkate düzeylerini incelemek MOXO d-CPT DEHB (Dikkat Eksikliği ve Hiperaktivite Bozukluğu) Yetişkinlere Yönelik Çeldiricili Sürekli Performans Testi'nden (N=327) yararlanılmıştır. Sporcu Sağlığı, Performansı ve Hizmet Kalite Standartları Daire Başkanlığı Psikolojik Değerlendirme ve Müdahale Birimi bünyesinde yapılan sağlık taramaları öncesinde bütün sporculara "Genel Onam Formu" imzalatılmıştır. Genel Onam Formu ile birimde yapılacak bütün uygula-

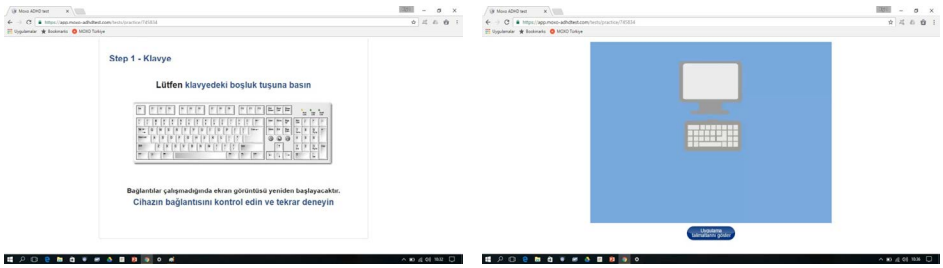
maların sadece eğitim ve bilimsel amaçla olmak üzere çeşitli çalışmalarda kullanılabileceği konusunda katılımcılardan onay alınmıştır. Ayrıca katılımcılara, hazırlanmış olan "Araştırma Amaçlı Çalışma İçin Bilgilendirilmiş Onam Formu" ve "Araştırma Amaçlı Çalışma İçin Gönüllü Katılım Formu" imzalatılmıştır. Araştırma uygulamasına katılım tamamen gönüllülük esasına dayalı planlanmıştır. Çalışmada kimlik belirleyici hiçbir bilgi istenmemiştir. Uygulanan anket formları tamamen gizli tutulmuş, yalnızca araştırmacılar tarafından değerlendirilmiştir. Veriler yalnızca araştırmada kullanılacak ve üçüncü kişilerle paylaşılmayacaktır. Katılımcılara onam belgesi imzalatılıp, anket konusunda sözlü bilgilendirme yapılmıştır. Katılımcılardan isimlerini belirtmeden formu doldurmaları istenmiş ve verilerin sadece bilimsel amaçlı kullanılacağı açıklanmıştır. Ankette ve anket uygulama sürecinde, kişisel rahatsızlık verecek sorulara ve durumlara yer verilmemiştir. Katılımcılar, süreç esnasında sorulardan ya da herhangi bir nedenle rahatsızlık hissederse anketten çekilme konusunda özgür bırakılmıştır. Katılımcıların aklına gelebilecek ya da merak ettikleri soruların yanıtları verilecektir. Onaylamadan önce sormak istedikleri herhangi bir soru varsa çekinmeden sormaları gerektiği vurgulanmıştır. Ek olarak, çalışma bittiğinde mail ya da telefon aracılığıyla ulaşarak yine sürece ilişkin istedikleri soruları sorabilecekleri ve sonuçlara ilişkin bilgi isteyebilecekleri katılımcılara belirtilmiştir. Sporcu Sağlığı, Performansı Hizmet Kalite Standartları Daire Başkanlığı ile birebir görüşülüp gerekli izinler alındıktan sonra, sporcular çalışmaya gönüllü katıldıklarını belirten onam formunu imzalamışlardır. Araştırmacılar tarafından, sporculara ilgili ölçüm uygulanmıştır. Ölçüm, Psikoloji Araştırma Laboratuvarı'nda bilgisayar üzerinden, araştırmacıların kontrolü altında yaklaşık 20 dakikada yapılmıştır. Deneye başlamadan önce, ölçümlerin sessiz ve kapalı bir odada uygulanması gerektiğinden uygun koşullar sağlanmaya çalışılmıştır. Ölçüm süresince telefon sesi başta olmak üzere ortam gürültüsü dahil hiçbir dikkat dağıtıcı unsurun olmaması için önlemler alınmıştır. Ölçüm yapılan mekânın ışığı uygun düzeyde ayarlanıp, ışığın göz kamaştırıcı ya da ekranda parlamaya neden olacak düzeyde olmaması sağlanmıştır. Ortam ısısı sporcunun rahat edeceği seviyede korunmuştur. Ölçüm pratiğinin öncesinde sporcuya yaklaşık 20 dakika boyunca rahat pozisyonda ve uygulama esaslarının gerektirdiği şekilde oturmaya hazır olması gerektiği bilgisi hatırlatılmıştır. Ölçüm, gün içinde sporcunun en uyanık (alert) olduğu zaman seçilerek, kahvaltısını yaptıktan yaklaşık 1 saat sonra yapılması için programlanmıştır. Sporculardan işitsel ya da görsel bir bozukluğu olanlar için uygulama

esnasında uygun gereçleri (lens, gözlük, işitme cihazı vs.) kullanabilmesi için yönlendirme yapılmış ve yardımcı olunmuştur. Sporcunun bilgisayar karşısında konforlu bir şekilde, sabit bir sandalyede ve ekran ile arasındaki gereken mesafeyi koruyarak ölçüme katılabilmesi için laboratuvar ortamı hazırlanmıştır. Sporcular dörderli olarak laboratuvar ortamına alınmıştır. Her denek başına All-In-One PC konumlandırılmıştır. Akış istasyonu dışındaki bilgisayarlardan WEB tabanlı görüntüleme kapatılmış ve veriler yalnızca kurum içinde olacak şekilde saklanmıştır. Ölçüm sporcularda dikkat ve alt bileşenlerin değerlendirildiği çoklu karıştırıcı ve çeldiricilerin bulunduğu görsel, işitsel ve nötr uyarılarla tasarlanmış ruhsatlı bilgisayar temelli uygulamalar ile tamamlanmıştır. Test her bir sporcuya bir kez uygulanmıştır. Veriler Sporcu Sağlığı, Performansı ve Hizmet Kalite Standartları Daire Başkanlığı Psikolojik Değerlendirme ve Müdahale Birimi Gözlem Odasında Covid-19 önlemleri alınmış bir şekilde her bir katılımcı ile birebir ve yüz yüze olarak toplanmıştır. Her bir katılımcının uygulamayı yaklaşık 20 dakikada tamamlaması planlanmıştır.

MOXO

MOXO Sürekli Performans Testi, bilgisayar ortamında yapılan ve çeldiricilerin bulunduğu bir çeşit görsel-işitsel dikkat ölçme testidir. Bu test hem çocuklar hem de yetişkinler için geliştirilmiştir. Bu testin diğer sürekli performans testlerinden farkı, test içinde ölçülebilir dikkat dağıtıcıların bulunmasıdır. Bu testin uygulanması esnasında katılımcıdan beklenen, dikkat dağıtıcı uyaranlara rağmen dikkati sürdürmeleri ve uygulamanın başında kendisine aktarılan hedef görseli gördüğünde, en kısa sürede klavyedeki boşluk tuşuna basmalarıdır. Testin 8 seviyesi bulunmaktadır ve her seviyede 53 deneme mevcuttur. Ölçüm esnasındaki uyaranlar ve uyaranların ekrana gelme süreleri bütün seviyelerde aynı olmakla birlikte denemelerdeki görsel ve işitsel çeldiriciler her seviyede farklılık göstermektedir. 1. ve 8. seviyelerde herhangi bir çeldirici yoktur. 2. ve 3. seviyelerde görsel uyarıcılar vardır. 4. ve 5. seviyelerde işitsel uyarıcılar vardır. 6. ve 7. seviyelerde görsel ve işitsel uyaranların bir kombinasyonunu bulunmaktadır. Test, kişinin 4 performansını kontrol etmektedir. Dikkat alt boyutunda; tüm test boyunca, hedefe kaç kez cevap verildiğini göstermektedir. Zamanlama alt boyutunda; yalnızca hedef uyaran ekrandayken verilen doğru cevap sayısı dikkate alınmıştır. Dürtüsellik alt boyutu; tüm test boyunca, hedef olmayan görüntüye hedefe vermesi gereken tepkiyi verilmesidir. Hiperaktivite alt boyutu; çoklu ya-

nıtlar, rastgele tuş ya da tuşlara basmak, boşluk tuşundan başka klavyede herhangi bir düğmeye basmak gibi yanlış basılan tüm tuşların sayısıdır.



Şekil 1. Moxo Dikkat Testi uygulamasına ait örnek ekran görüntüsü

Not: Uygulama örneği 2023 yılında Moxo resmi sitesinden alınmıştır.

Ulusal literatür incelendiğinde 2013-2023 yılları arasında dikkat ve aktivite (spor, hareket, fiziksel aktivite) ilişkisini inceleyen çalışmalarda MOXO Sürekli Performans Testinin kullanılmadığı görülmektedir. Literatürdeki bu eksikliğin tamamlanması adına, Gençlik ve Spor Bakanlığı, Sporcu Sağlığı, Performansı ve Hizmet Kalite Standartları Daire Başkanlığı, Psikolojik Destek ve Müdahale Birimi'nde, MOXO Sürekli Performans Testi çok sayıda milli ve elit sporcuya uygulanmakta ve böylece dikkat ile aktivite arasındaki ilişki incelenmektedir. MOXO testinin dikkati ölçmedeki yeterliliğini incelemek amacıyla tarafımızca literatür taraması yapılmıştır.

VERİLERİN ANALİZİ

Bilgisayar üzerinden uygulama yapılmıştır, uygulama esnasında katılımcıların cevapları ve tepkileri kaydedilmiştir. Test uygulanacak kişinin hedef uyarı ekranı belirdikten sonra bilgisayar klavyesinin space tuşuna sadece bir kez ve en kısa zamanda basması gerekmektedir. Sonra hedef uyarı ekranında görünür ve 0,5, 1 ya da 4 saniye ekranda kalmaktadır. Hedef ekrandan kalktıktan sonra hedefin ekranda kaldığı süre boyunca boş zaman verilmektedir. Verilen bu boş zaman, dikkati bozuk olmayan fakat zamanlama sorunu yaşayan kişilerin doğru şekilde değerlendirilmesini sağlamaktadır. ADHD teşhisinde ve tedavisinde yeni yaklaşımlar hastalığın gelişimsel, bilişsel ve davranışsal olduğunu vurgulamaktadırlar. Bilgisayar Tabanlı Çeldiricili Sürekli Performans Testi Analytics ADHD bu patolojinin gelişimsel, bilişsel ve davranışsal üç bileşeni için kapsayıcı ve ölçülebi-

lir göstergeler sağlamaktadır (Neurotech, 2013; NeuroTechnology Solutions Ltd., 2014, s.20). Çalışma sonucunda elde edilen verilerin analizi, "SPSS (Statistical Packagefor Social Sciences) for Windows 25.0" istatistik paket programı ile analiz edilecektir. Veriler ortalama, standart sapma, minimum-maksimum değerler olarak sunulacaktır. Sonuçlar %95 güven aralığında p değeri 0.05 altında olduğunda anlamlı sayılacaktır. Araştırma grubundan elde edilen verilerin branşlara göre farklılığını bulmak için Kay-kare istatistiği uygulanmıştır. A (Attention-Dikkat), T(Timing-Zamanlama), I(Impulsiveness-Dürtüsellik) ve H(Hyperactivity-Hiperaktivite) parametreleri arasındaki ilişkiyi bulmak için Kendall's Tau istatistiksel analizi uygulanmıştır. Verilerin analizi için SPSS 23.00 paket programı kullanılmıştır. Anlamlılık düzeyi için $p<0,05$ kabul edilmiştir.

ETİK BEYANI

Anket Bilgilendirme Formunda; araştırmanın neden yapıldığı, bilgilerin gizli tutulacağı, tamamen araştırma amacı ile kullanılacağı ve **çalışmaya katılımda gönüllülüğün esas alındığı bilgilendirmeler**i yer almaktadır. Örneklem için veri toplama işlemi 6 Temmuz-25 Kasım 2022 tarihleri arasında Psikoloji Araştırmaları Laboratuvarı'nda yüz yüze yapılmıştır. Araştırmanın uygulama aşamasından önce Gazi **Üniversitesi** Etik Kurulu'ndan 21 Haziran 2022 tarih ve E-77082166-604.01.02-393603 Sayı ve 826 Karar No ile etik onay alınmıştır. **İlgili** birimin koordinatörü aracılığı ile uygulama yapabilmek için izin alınmıştır.

BULGULAR

Araştırma grubunda elde edilen verilere ait istatistiksel analizler, yorumları ile birlikte tablo halinde verilmiştir. Araştırma grubunu oluşturan farklı branşlardaki sporcuların A, T, I ve H alt boyutları bakımından, arasındaki farklılığa ilişkin Kay-kare test sonuçları tablo 1'de verilmiştir.

Tablo 1. Farklı branşlardaki sporcuların A (Attention-Dikkat), parametresi bakımından arasındaki farklılığa ilişkin Kay-kare testi sonuçları

Parametre	N	x̄	SS	1	2	3	4	Toplam	X2	p	Anlamlı Fark
Artistik Buz Pateni	9	1,89	1,17	5	1	2	1	9	70,972	,000	Judo-Atıcılık Judo-Eskrim Judo-Hentbol Judo-Su Topu Judo-Voleybol
Atıcılık	41	1,54	0,95	28	8	1	4	41			
Atletizm	35	2,11	1,08	12	13	4	6	35			
Buz Pateni	9	1,89	1,17	5	1	2	1	9			
Curling	23	1,96	1,11	10	8	1	4	23			
Eskrim	12	1,50	0,80	8	2	2	0	12			
Hentbol	40	1,95	1,18	21	7	5	7	40			
Judo	63	2,73	1,27	17	10	9	27	63			
Modern Pentatlon	15	2,00	1,20	7	4	1	3	15			
Sutopu	58	1,53	0,88	38	13	3	4	58			
Tenis	26	1,46	0,65	16	8	2	0	26			
Voleybol	41	1,88	1,12	22	8	5	6	41			
Toplam	372	1,93	1,13	189	83	37	63	372			

Tablo incelendiğinde A (Attention-Dikkat) parametresi bakımından branşlar arasında farklılık görülmektedir (X^2=70,972, p<0,05). Bu farklılığın hangi gruplardan kaynaklandığını bulmak amacıyla yapılan ikili karşılaştırma istatistiğine göre judo branşı atıcılık, eskrim, hentbol, su topu ve voleybol branşlarından daha yüksek puanlara sahip olduğu belirlenmiştir.

Tablo 2. Farklı branşlardaki sporcuların T (Timing-Zamanlama), parametresi bakımından arasındaki farklılığa ilişkin Kay-kare testi sonuçları

Parametre	N	x̄	SS	1	2	3	4	Toplam	X2	p	Anlamlı Fark
Artistik Buz Pateni	9	3,00	1,12	1	2	2	4	9	67,558	,000	Atıcılık ve Tenis-Diğer Branşlar
Atıcılık	41	1,80	1,17	25	6	3	7	41			
Atletizm	35	2,49	1,29	13	3	8	11	35			
Buz Pateni	9	3,00	1,12	1	2	2	4	9			
Curling	23	2,39	1,31	8	6	1	8	23			
Eskrim	12	2,58	1,08	3	1	6	2	12			
Hentbol	40	2,55	1,30	13	7	5	15	40			
Judo	63	2,98	1,18	12	8	12	31	63			
Modern Pentatlon	15	2,73	1,28	4	2	3	6	15			
Sutopu	58	2,00	1,12	27	13	9	9	58			
Tenis	26	1,85	1,16	14	7	0	5	26			
Voleybol	41	2,46	1,36	16	6	3	16	41			
Toplam	372	2,41	1,27	137	63	54	118	372			

Tablo incelendiğinde T (Timing-Zamanlama), parametresi bakımından branşlar arasında farklılık görülmektedir (X^2=67,558, p<0,05). Bu farklılığın hangi gruplardan kaynaklandığını bulmak amacıyla yapılan ikili karşılaştırma istatistiğine göre atıcılık branşının, diğer branşlardan daha düşük puanlara sahip olduğu belirlenmiştir.

Tablo 3. Farklı branşlardaki sporcuların I (Impulsiveness-Dürtüsellik) parametresi bakımından arasındaki farklılığa ilişkin Kay-kare testi sonuçları

Parametre	N	x̄	SS	1	2	3	4	Toplam	X2	p	Anlamlı fark
Artistik Buz Pateni	9	2,33	1,41	4	1	1	3	9			
Atıcılık	41	2,71	1,42	15	3	2	21	41			
Atletizm	35	2,71	1,27	10	4	7	14	35			
Buz Pateni	9	2,33	1,41	4	1	1	3	9			
Curling	23	2,57	1,41	9	2	2	10	23			Su topu-Atıcılık
Eskrim	12	1,92	1,38	8	0	1	3	12			Su Topu-Atletizm
Hentbol	40	2,35	1,35	18	3	6	13	40	117,521	,000	Su Topu-Judo
Judo	63	3,03	1,26	12	12	1	38	63			Su Topu-Pentatlon
Modern Pentatlon	15	3,20	1,15	2	2	2	9	15			
Sutopu	58	1,78	0,90	27	21	6	4	58			
Tenis	26	2,38	0,80	1	18	3	4	26			
Voleybol	41	2,49	1,33	14	9	2	16	41			
Toplam	372	2,50	1,29	124	76	34	138	372			

Tablo incelendiğinde I (Impulsiveness-Dürtüsellik) parametresi bakımından branşlar arasında farklılık görülmektedir (X^2=117,521, p<0,05). Bu farklılığın hangi gruplardan kaynaklandığını bulmak amacıyla yapılan ikili karşılaştırma istatistiğine göre Su topu branşının; atıcılık, atletizm, judo ve modern pentatlon branşlarından daha düşük puanlara sahip olduğu belirlenmiştir.

Tablo 4. Farklı branşlardaki sporcuların H (Hyperactivity-Hiperaktivite) parametresi bakımından arasındaki farklılığa ilişkin Kay-kare testi sonuçları

Parametre	N	x̄	SS	1	2	3	4	Toplam	X2	p	Anlamlı Fark
Artistik Buz Pateni	9	1,78	0,97	4	4	0	1	9	74,472	,000	Judo-Atıcılık Judo-Eskrim Judo-Hentbol Judo-Voleybol Judo-Tenis
Atıcılık	41	1,56	1,05	30	4	2	5	41			
Atletizm	35	2,03	1,22	17	8	2	8	35			
Buz Pateni	9	1,78	0,97	4	4	0	1	9			
Curling	23	1,74	1,21	16	1	2	4	23			
Eskrim	12	1,25	0,87	11	0	0	1	12			
Hentbol	40	1,65	1,03	26	6	4	4	40			
Judo	63	2,44	1,38	27	5	7	24	63			
Modern Pentatlon	15	2,00	1,25	8	2	2	3	15			
Sutopu	58	1,62	0,88	34	15	6	3	58			
Tenis	26	1,12	0,33	23	3	0	0	26			
Voleybol	41	1,56	0,98	28	7	2	4	41			
Toplam	372	1,77	1,12	228	59	27	58	372			

Tablo incelendiğinde H (Hyperactivity-Hiperaktivite) parametresi bakımından branşlar arasında farklılık görülmektedir (X2=74,472, p<0,05). Bu farklılığın hangi gruplardan kaynaklandığını bulmak amacıyla yapılan ikili karşılaştırma istatistiğine göre judo branşının; atıcılık, eskrim, hentbol, voleybol ve tenis branşlarından daha yüksek puanlara sahip olduğu belirlenmiştir.

Tablo 5. Erkek sporculardan elde edilen veriler arasındaki ilişkiye ait Kendall's Tau istatistiği sonuçları

Parametreler	Kendall's Tau	A	T	I	H
a	Korelasyon Katsayısı	1,000	,476**	,098	,262**
	P	.	,000	,083	,000
t	Korelasyon Katsayısı	,476**	1,000	-,005	,208**
	P	,000	.	,929	,000
ı	Korelasyon Katsayısı	,098	-,005	1,000	,144*
	P	,083	,929	.	,012
h	Korelasyon Katsayısı	,262**	,208**	,144*	1,000
	P	,000	,000	,012	.

*** P<0,01 * p<0,05*

Tablo incelendiğinde erkek sporculardan elde edilen A (Attention-Dikkat) parametresi ile T (Timing-Zamanlama) arasında orta düzeyde, H (Hyperactivity-Hiperaktivite) parametresi ile düşük düzeyde, H (Hyperactivity-Hiperaktivite) ile T (Timing-Zamanlama) ve I (Impulsiveness-Dürtüsellik) arasında ise düşük düzeyde istatistiksel olarak anlamlı ilişki görülmektedir.

Tablo 5. Kadın sporculardan elde edilen veriler arasındaki ilişkiye ait Kendall's Tau istatistiği sonuçları

Parametreler	Kendall's Tau	A	T	I	H
A	Korelasyon Katsayısı	1,000	,488**	,126	,494**
	P	.	,000	,090	,000
T	Korelasyon Katsayısı	,488**	1,000	-,006	,238**
	P	,000	.	,938	,001
I	Korelasyon Katsayısı	,126	-,006	1,000	,293**
	P	,090	,938	.	,000
H	Korelasyon Katsayısı	,494**	,238**	,293**	1,000
	P	,000	,001	,000	.

*** P<0,01 * p<0,05*

Tablo incelendiğinde kadın sporculardan elde edilen A parametresi ile T ve H parametresi orta düzeyde, H ile T ve I arasında düşük düzeyde, istatistiksel olarak anlamlı ilişki görülmektedir. Sonuç olarak bazı branşlar, elde edilen A, T, I ve H parametrelerinde farklılaşmaya neden olmakta özellikle branşın bahsedilen parametrelerdeki değişimi etkilediği gözlemlenmiştir. Diğer bir sonuç ise A, T, I ve H parametrelerinin birbirlerini düşük düzeyde etkilediği ve cinsiyete göre ise bahsi geçen 4 değerde (A, T, I, H) erkek sporcular kadın sporculara göre daha yüksek puanlar almışlardır. Erkek sporcuların kadın sporculara göre dikkat ve zamanlama puanları daha düşüktür. Dürtüsellik ve hiperaktivite eğilim puanları ise daha yüksek olarak belirlenmiştir.

TARTIŞMA VE SONUÇ

Dikkat, sporcuların performansını etkileyen en önemli faktörlerden biridir. Sporcunun, içinde bulunduğu ana ve bu andaki doğru uyarana dikkat kesilmesi, hareketlerinin doğruluğunu artıracağı gibi performansını da pozitif yönde etkilemektedir. Bu nedenle sporcularda dikkatin uygun ölçekler ve testler kullanılarak ölçülmesi ve zamanında alınan önlemlerle desteğe ihtiyaç duyan sporcuların dikkatlerini yükseltmek için çalışmalar yürütülmesi önem taşımaktadır.

Bugüne kadar sporcularda dikkati ölçen pek çok araştırma yürütülmüştür. Bu çalışmalar, dikkat ve spor performansının çift yönlü ilişkisini belirgin bir şekilde ortaya koymuştur. Örneğin Ulukan'ın (2020) yürüttüğü çalışma, okçuların dikkat seviyeleri ve performansları arasındaki pozitif ilişkiyi göstermiştir. Aynı zamanda destekleyici antrenörlere ve ailelere sahip olan sporcuların dikkat seviyesinin de eleştirel aile ve antrenörlere sahip olanlara kıyasla daha yüksek olduğunu belirtilmiştir. Bu sonuçlar, sporcuların dikkatinin nasıl geliştirilebileceğine dair bir yol göstermektedir. Bu sonuçlara göre, sporcuların ailelerine ve antrenörlerine pozitif yaklaşım, empati ve desteğin önemini çeşitli yollarla belirtmek, onlara bu konularda seminer ve eğitimler vermek sporcuların dikkatini artırarak performanslarını geliştirmelerine de yardımcı olacaktır.

Dikkatin performansa olan etkisi, yapılan çalışmalar sonucu net bir şekilde gösterilmiştir. Dikkati ve dolayısıyla performansı etkileyen faktörlerden bir diğeri olan işleyen bellek kapasitesi ve kontrolü de Vaughan ve Laborde'nin (2020) çalışmasında incelenmiştir. Bu çalışmada, sporcularda dikkatin performansla olan ilişkisinin işleyen bellek kapasitesinden etkilendiği ortaya koyulmuştur. İşleyen bellek kapasitesinin dikkat üzerinde de etkisi olduğu düşünülecek olursa, sporcularda işleyen bellek kapasitesi ve kontrolünün geliştirilmesine yönelik çalışmalar yapılması dikkati geliştirerek performansı da olumlu yönde etkileyecektir.

Dikkatin spor performansı üzerindeki etkisinin yanı sıra, sporun da dikkat üzerinde yadsınamaz bir etkisi bulunmaktadır. İnce ve Yıldırım'ın (2018) çalışmasında, vaktinin büyük kısmını oturarak geçiren ve egzersiz yapmayan öğrencilerin hokey ve hentbol ile uğraşan öğrencilerden daha düşük dikkat seviyesine sahip olduğu gözlemlenmiştir. Bu sonuçlar, spor ve dikkat ilişkisinin yalnızca tek yönlü değil, çift yönlü de hareket ettiğini göstermektedir. Bu sonuçlardan hareketle, dikkat konusunda problem yaşayan öğrencilerin spor faaliyetlerine katıl-

malarının dikkatlerini geliştirme alanında onlara fayda sağlayacağı söylenebilir. Ailelerin bu konuda bilinçlendirilmeleri ve okullarda sedanter öğrencilerin belirlenerek ilgilerine göre bir spor dalına yönlendirilmeleri, dikkatlerinin gelişmesine yardım ederek genel performanslarına katkı sağlayacaktır.

Hem sporda hem de genel anlamda önem arz eden dikkat faktörünü ölçmek için çeşitli yöntemler bulunmaktadır. Bunların arasında İşaretleme Testi, Stroop Testi TBAG Formu, d2 Testi gibi direkt uygulayıcı tarafından canlı ortamda yapılan testlerin yanı sıra, MOXO-CPT gibi dijital ortamda uygulanan testler de bulunmaktadır. MOXO-CPT testinden bahsedilecek olursa, bu testin DEHB tanısındaki başarısı, Slobodin ve arkadaşları (2020) tarafından çeşitli milletler üzerinde yürütülen bir çalışmayla gösterilmiştir. Bu çalışmada, MOXO'nun DEHB tanısı almış bireylerdeki hiperaktivite ve dürtüsellik seviyelerini sağlıklı bireylerinkinden ayırt edebildiği görülmüştür. Bu sonuçlar, MOXO-CPT'nin DEHB tanısında kullanılmasının faydalı olabileceğini göstermiştir. Bu konuya sporcular açısından bakıldığında, sporculara MOXO-CPT testi uygulanılarak dikkat ölçümlerinin gerçekleştirilmesinin ve çıkan sonuçlara göre erken zamanda uygun önlemlerin alınmasının performanslarını geliştirmeye katkı sağlayabileceği anlaşılmaktadır.

Günümüzde MOXO-CPT testi gibi dijital ve çevrimiçi platformlarda uygulanan pek çok test bulunmaktadır. Laboratuvar ortamında direkt olarak araştırmacı tarafından uygulanan testlerden çevrimiçi ve dijital testlere geçiş aşaması COVID-19'dan kaynaklanan salgın dönemi sonucu giderek hız kazanmıştır (De Man vd., 2021). Bilgisayar ortamında uygulanan bu testlerin çeşitli avantajları ve dezavantajları bulunmaktadır. Bu testler, araştırmacıların çeşitli demografik özelliklere sahip çok sayıda katılımcıya zaman ve imkân tasarrufu ederek ulaşabilmesini sağlamaktadır. Aynı zamanda, araştırmacı etkisini ve araştırmacının tepkilerinden doğabilecek katılımcı etkisini azaltmaktadır (Oktay, 2022). Bu testlerin etkinliğini azaltan en önemli dezavantaj, bilgisayar ortamında yürütülen testlerin tepki zamanı hassaslığı ve doğruluğunun düşmesidir. Çeşitli işletim sistemleri, çoklu görev ortamları sebebiyle veri kaydı sırasında zaman kaybına sebep olur. Bu sorun, bilgisayarı gereksiz yüklerden arındırarak çözülebilmektedir. Fare ve klavye gibi harici donanım aygıtları zamanlama kaydının doğruluğunu olumsuz yönde etkilemektedir. Aynı zamanda fareler, imlecin lokasyonunu bilgisayara bildirirken ayrı bir zaman kaybına yol açar. Bu sorunlar, işlevsel olduğu takdirde

tepki kutuları ve paralel portlar veya oyun portları kullanarak, işlevsel olmadığı takdirde ise kullanılan harici donanım cihazlarının zamanlama doğruluğunu ek bir düzenek kullanarak ölçerek çözülebilir. Aynı zamanda, farenin imlecin yerini iletme fonksiyonunu devre dışı bırakmak da bu konuda yardımcı olabilmektedir (Li vd., 2010; Stewart, 2006; Voss, Leonhart ve Stahl, 2007; Erdoğdu, Karar ve Aytaç, 2023).

Uygun programlama tekniğinin kullanılmaması zamanlama hassasiyetini düşürmektedir. Bu sorunu gidermek için eğer araştırmacı yeterli programlama becerisinden yoksunsa ücretli ve uygun bir programlama yazılımı tercih etmeli, yeterli programlama bilgisine sahipse seçeceği programlama dilini hassas zamanlamaya uygun olacak şekilde belirlemelidir. Bunun mümkün olmadığı durumlarda, işletim sisteminde bulunan zamanlayıcı işlevlerinden faydalanılmalıdır (Chambers ve Brown, 2003).

Bilgisayar ortamında uygulanan deneylerin yanı sıra, Web deneyleri de günümüzde oldukça yaygınlaşmış durumdadır. Web deneylerini laboratuvarlarda bilgisayar ortamında uygulanan deneylerden farklı kılan faktör, katılımcıların farklı tarayıcılara, işletim sistemlerine ve donanımlara sahip olan farklı bilgisayarlardan deneylere katılım sağlamasıdır. Bu durum beraberinde yeni sorunlar ve daha farklı çözümler getirmektedir. Bu soruna ilişkin, katılımcıların bilgisayarları ve kullandıkları tarayıcılar öğrenilerek uygulanacak deneyin o bilgisayara uygun versiyonunun gönderilebildiği gibi, yalnızca belirli işletim sistemleri, donanımlar veya tarayıcılardan gelen veriler analize dahil edilebilmektedir. Ayrıca, deneylerde kullanılan animasyonların zaman aralıkları, deneyin tasarlandığı platforma uygun olacak şekilde tutulabilmektedir (Garaizar, Vadillo ve López-de-Ipiña, 2014). Ek olarak, daha geniş örneklem kullanılalarak veya katılımcılara sunulan deneme sayıları artırılarak çözümlerin üretilebileceği düşünülmektedir (Chetverikov ve Upravitelev, 2016).

Bilgisayar ortamında ve Web'de uygulanan deneylerin doğruluğunun artırılması ve kullanıma elverişli hale gelmesi yukarıda belirtilen çözüm yollarının uygulanmasıyla sağlanabilmektedir. Bu yöntemler kullanıldığında, bilgisayar ve Web ortamındaki deneylerin avantajlarından verimli bir şekilde faydalanmak mümkündür. Bütün bunlara ek olarak, 21 katılımcıya laboratuvar ortamında, 21 katılımcıya ise çevrimiçi ortamda aynı testin uygulandığı bir çalışmada, bilişsel

ve davranışsal faktörleri ölçen çevrimiçi deneylerin çevrimiçi ortamda uygulandığında performans veriminde ve yeterliliğinde herhangi anlamlı bir fark yaratmadığı görülmüştür (Brimmell ve Vaughan, 2022). Bu bilgilere bakıldığında, çevrimiçi ve bilgisayar ortamında uygulanan testlerin, gerekli yapılandırmalar sağlandığında ve yeterli önlem alındığında kullanışlı olduğu anlaşılmaktadır. Örneğin, BART uygulaması incelendiğinde, bu çevrimiçi bilgisayar temelli uygulamanın, geleneksel dürtüsellik anketleriyle paralel sonuçlar verdiği, yeterli derecede güvenilirlik ve tutarlılığa sahip olduğu gözlemlenmiştir (Hunt vd., 2005; Lejuez vd., 2002). Bu örnekten de yola çıkarak, Web tabanlı ve çevrimiçi testlerin avantajlarından, sporcularda dikkati ölçerken de yararlanılabilir. Çevrimiçi ve bilgisayar ortamında uygulanan testler, daha kısa zamanda daha fazla sporcuya daha etkili bir şekilde dikkat ve ilgili faktörlerin ölçümünün yapılmasını sağlayabilir.

Sporcularda dikkatin önemi yalnızca performans gelişimi konusunda değil, dikkatsizlikten kaynaklanan olası sakatlıkların önüne geçme konusunda da büyük önem taşımaktadır. Sakatlanma ve yaralanma risklerinin önüne geçmek için, Williams ve Andersen'in Stres ve Atletik Sakatlık Modeline göre hem fiziksel hem de psikolojik önlemler alınmalıdır. Fiziksel önlemler kas gerilimine odaklanırken psikolojik önlemler daha çok bireyin bilişsel kabiliyetleri ve dikkatini kontrol ederken kullandığı stratejiler üzerine yoğunlaşmalıdır. Bireyin yaşadığı strese verdiği tepkilerden olan dikkat dağınıklığı ve bilişsel kaygı, görüş alanının daralması ve vücuttaki kasların genel olarak gerilmesi sakatlık riskini oluşturan sebeplerden sayılabilir (Ivarsson vd., 2015) ve bunlardan, stresin kontrol edilmesi, dikkat dağınıklığının önüne geçerek sakatlanma riskinin düşmesine katkıda bulunabilir. Bu da stresi yönetmek için etkili bir yöntem bulmayı gerektirmektedir.

Bireylerin günlük hayatta yaşadıkları stresi kontrol altında tutabilmelerine yardımcı olan yöntemlerden biri sayılan bilinçli farkındalık, kişinin geçmiş ve geleceğin yükünden sıyrılarak içinde bulunduğu anı yargılamadan, açık yüreklilikle fark etmesi ve anın içinde kalmasıdır. Bu alanda kullanılan en yaygın uygulamalardan biri, Ivarsson ve arkadaşlarının makalelerinde bahsettiği üzere, araştırmalar/teoriler ile temellenmiş ve kabullenmeyi odak alan MAC ("Mindfulness" =Farkındalık, "Acceptance" =Kabullenme, "Commitment" =Bağlılık) isimli bir programdır. Bu program, atletlerin psikolojik ve performans anlamında gelişmesini hedef alan bir yaklaşımdır ve genel anlamda, sporcuların içinde

bulundukları ana olan farkındalıklarının artmasının, dikkat vermeleri gereken uyarana odaklanmalarını kolaylaştırarak performanslarını artıracağı tahmini üzerinde durmaktadır. Bilinçli Farkındalık odaklı programlar genel olarak bireyin dikkatini şu ana yönlendirmesini amaçlamaktadır ve bu alanda yapılan bir çalışma, farkındalık uygulamalarının sporcuların sakatlık dereceleri ve sayılarını nasıl etkilediğini ortaya koymuştur. Bu çalışmada 16-19 yaşları arasındaki kadın (n = 10) ve erkek (n = 31) futbol oyuncuları kullanılmıştır ve bu katılımcılar iki gruba ayrılmış, deney grubu 7 seanslık MAC odaklı farkındalık eğitimi alırken kontrol grubu 7 seans boyunca takım psikolojisi ve yoğunlukla futbolla alakalı seminerler dinlemiştir. Bilinçli farkındalık eğitimi alan gruba seanslar haftada bir 45'er dakikalık seanslar halinde verilmiştir ve bütün bu seanslarda öğrencilere farkındalık egzersizleri yaptırılmış, seans sonlarında sporculara haftada en az 3 kere dinleyecekleri bir ses kaydı (egzersiz) verilmiştir. Araştırmanın sonucunda, 6 ay içinde, deney grubundaki sporculardan %67'sinin sakatlık geçirmediği görülürken, bu oran kontrol grubunda %40 olmuştur ve bunlara ek olarak, deney grubu sakatlıklardan kaynaklı 4-33 gün arası zaman kaybederken kontrol grubunda bu sayı 4-89 gün arasında kalmıştır. Bu sonuçlardan yola çıkılarak dikkati yaşanılan andaki belirli bir duruma/hedefe getirebilme yetisini artıran bilinçli farkındalık eğitimlerinin sporcuların sakatlık riskini azalttığı söylenebilir (Ivarsson vd., 2015).

Son olarak, dikkatin sporda önemi, nasıl ölçülebileceği ve güncel ölçüm tekniklerinden sonra, dikkati artırmaya yönelik çözümlerden bahsedilmiştir. Bu çözümlerin arasında bilinçli farkındalık gösterilebilir. Kişinin geçmişten ve alakasız düşüncelerden sıyrılarak ana odaklanmasını sağlayan farkındalık yöntemi, sporcuların içinde bulundukları ana yoğunlaşmalarını sağlayarak dikkatlerini hedef uyarana vermelerini kolaylaştırabilir. Yapılan bir araştırmada, farkındalık eğitimi alan sporcuların yaralanma sayıları ve yaralanmalarının ciddiyet seviyesinde, kontrol grubuyla karşılaştırıldığında, belirgin bir azalma görülmüştür (Ivarsson vd., 2015). Bu araştırmadan da anlaşılabileceği üzere, farkındalık eğitimi sporcuların dikkatini artırarak yaralanma/sakatlanma riskini düşürmekte ve dolaylı yoldan performanslarını da artırmaktadır. Bu sebeple, geleneksel yöntemlere ek olarak, sporculara verilecek basit farkındalık ve ruh sağlığının önemi hakkında farkındalık eğitimlerinin, dikkat seviyelerinde gözle görülür farklar yaratacağı düşünülmektedir.

Sonuç olarak, tarafımızca yapılan literatür taramasında, dikkatin ölçülmesinde ve sahte DEHB tespitinde MOXO-d-CPT'nin faydalı olabileceği anlaşılmıştır. Ancak literatürde, özellikle sağlıklı yetişkinlerin dikkat ölçümü hususunda MOXO d-CPT uygulanması ile ilgili büyük bir boşluk olduğu fark edilmiştir. Dikkat ve aktivite arasındaki ilişkinin kurumumuzda tarafımızca çeşitli branşlardan elit ve milli sporculara MOXO d-CPT uygulanarak incelenmesinin literatürdeki boşluğu dolduracağı ve gelecek araştırmacılara çalışmalarında yol gösterebileceği sonucuna ulaşılmıştır.

KAYNAKLAR

Arnsten, A.F. (2009). Toward a new understanding of attention-deficit hyperactivity disorder pathophysiology pathophysiology: an important rolefor prefrontal cortex dysfunction. CNS Drugs;23 Suppl 1:33-41

Barkley, R. A., Edwards, G.,Laneri, M.,Fletcher, K., Metevia,L. (2001). Executivefunctioning, temporal discounting,and sense of time in adolescents with attention deficit hyperactivity disorder (ADHD) and oppositional defiant disorder (ODD). J Abnorm Child Psychol ;29(6): 541- 56.

Barkley, R.A., Fischer, M., Smallish, L., Fletcher, K. (2002).The persistence of attention-deficit/hyperactivity disorders into young adulthood as a function of reporting sourceand definition of disorder. J Abnorm Psychol;111(2):2

Berger, C., Lev, A., Braw, Y., Elbaum, T., Wagner, M., & Rassovsky, Y. (2021). Detection of Feigned ADHD Using the MOXO-d-CPT. Journal of Attention Disorders, 25(7), 1032–1047. https://doi.org/10.1177/1087054719864656

Berinsky, A.J., Huber, G.A., Lenz, G.S. (2012). Evaluating online labor markets for experimental research: Amazon.com's mechanical turk. *Political Anal.*, 20, 351–368.

Brimmell, J., Vaughan, R. (2022). Moving online: Comparing executive function and visual attention performance online and in the laboratory – A brief report. https://doi.org/10.31234/osf.io/4kg8b

Buhrmester, M., Kwang, T., Gosling, S.D. (2011). Amazon's mechanical turk: A new source of inexpensive, yet high-quality, data? *Perspect. Psychol. Sci.* 6, 3–5.

Chambers, C. D., Brown, M. (2003).Timing accuracy under Microsoft Windows revealed through external chronometry. *Behavior Research Methods, Instruments, & Computers, 35*, 96–108.

Chetverikov, A., Upravitelev, P. (2016). Online versus offline: The Web as a medium for response time data collection. Behavior Research Methods, 48, 1086–1099.

Clifford, S., Jerit, J. (2014). Is There a cost to convenience? An experimental comparison of data quality in laboratory and online studies. *J. Exp. Political Sci*, 1, 120–131.

Costa, A.,La Fougére, C., Pogarell, O.etal. (2013). Impulsivity is Related to aStriatal DopamineTransporter Availability in Healthy Males. Psychiatry Research. 211, 251-256.

Çağlar, E., Koruç, Z. (2006). D2 Dikkat Testinin Sporcularda Güvenilirliği ve Geçerliği. *Hacettepe Journal of Sport Sciences, 17*(2), 58-80.

De Man, J., Campbell, L., Tabana, H., Wouters, E. (2021). The pandemic of online research in times of COVID-19. *BMJ open*, *11*(2), e043866.

Erdoğdu, M., Aytaç, G. & Aydın, İ. (2023). Web Tabanlı Oyun Aracılığıyla Sporda Dürtüsel Davranış Ölçümleri. Spormetre Beden Eğitimi ve Spor Bilimleri Dergisi, 21 (2) , 162-177. DOI: 10.33689/spormetre.1173219

Erdoğdu, Artuner, Demirbaş ve Aytaç, (2022). Sporcu Sağlığında Güncel Yaklaşım: Bilgisayar Tabanlı Psikolojik Ölçümler . Türkiye Sağlık Enstitüleri Başkanlığı Dergisi, 5 (3) , 43-55. DOI: 10.54537/tusebdergisi.1173181

Erdoğdu, M., Karar, E. N. & Aytaç, G. (2023). Web Tabanlı Psikoloji Deneylerinin Çevrimiçi Tasarımı Ve Uygulamaları. Türkiye Sağlık Enstitüleri Başkanlığı Dergisi, 6 (1) , 38-53. DOI: 10.54537/tusebdergisi.1177366

Garaizar, P., Vadillo, M. A. (2014). Accuracy and precision of visual stimulus timing in PsychoPy: No timing errors in standard usage. *PLoS ONE, 9*, e112033

Garaizar, P., Vadillo, M. A., López-de-Ipiña, D., Matute, H. (2014). Measuring software timing errors in the presentation of visual stimuli in cognitive neuroscience experiments. *PLoS One, 9*, e85108.

Gupta, R., Kar, B. R.,Srinivasan, N. (2011). Cognitivemotivational deficits in ADHD: development of a classification system. Child Neuropsychology;17(1):67-81.

Hoff, H. (2002). Lehrbuch der Psychiatric,vol II. Basel: Benno Schwabe; 1956; p 554. Aktaran Sandberg S,

Barton J. Historical development. In:Sandberg S,ed.

Hunt, M. K., Hopko, D. R., Bare, R., Lejuez, C. W., Robinson, E. V. (2005). Construct validity of the Balloon Analog Risk Task (BART). *Assessment*, *12*(4), 416–428. https://doi.org/10.1177/1073191105278740

Ivarsson, A., Johnson, U., Andersen, M. B., Fallby, J., Altemyr, M. (2015). It pays to pay attention: A mindfulness-based program for injury prevention with soccer players. *Journal of Applied Sport Psychology*, *27*(3), 319–334. https://doi.org/10.1080/10413200.2015.1008072

İnce, G., Yıldırım, A. (2018). The effect of apparatus use on athletes' attention performance in sports branches playing with Ball: Pilot Study. *International Journal of Sport, Exercise & Training Sciences*, 122–130. https://doi.org/10.18826/useeabd.445340

İyilikci, O. (2019). Davranışsal Deneyler Tasarlanırken, Uyaran Sunumu ve Tepki Zamanı Kaydında Yaşanan Zamanlama sorunları. *Türk Psikoloji Yazıları*, *22*(43), 14–24. https://doi.org/10.31828/tpy1301996120180414m000002

Laufer, M.W., Denhoff,E.,Solomons, G. (2011). Hyperkinetic impulse disorder in children's behavior problems. J Atten Disord;15(8):620-5.

Lejuez, C. W., Read, J. P., Kahler, C. W., Richards, J. B., Ramsey, S. E., Stuart, G. L., Strong, D. R., Brown, R. A. (2002). Evaluation of a behavioral measure of risk taking: The Balloon Analogue Risk Task (BART). *Journal of Experimental Psychology: Applied*, *8*(2), 75–84. https://doi.org/10.1037/1076-898x.8.2.75

Lev, A., Elbaum, T., Berger, C., & Braw, Y. (2022). Feigned ADHD Associated Cognitive Impairment: Utility of Integrating an Eye-tracker and the MOXO-dCPT. Journal of Attention Disorders, 26(9), 1212–1222. https://doi.org/10.1177/10870547211063643

Li, X., Liang, Z., Kleiner, M., Lu, Z. L. (2010). RT-box: A device for highly accurate response time measurements. *Behavior Research Methods, 42*, 212–225.

Liebrenz, M., Gamma, A., Ivanov, I., Buadze, A., Eich, D. (2015). Adult attention-deficit/hyperactivity disorder: Associations between subtype and lifetime substance use – a clinical study. *F1000Research*, *4*, 407. https://doi.org/10.12688/f1000research.6780.1

MOXO ADHD Analytics PerformanceExcellence. (2023). https://www.moxoadhdtest.com

MOXO Türkiye. http://www.moxoturkiye.com

Neurotech (2013). 8th annual The Neorotech Investing & Partnering Con-

ference. Advances in Drugs, Devices & Diagnostics fort he Brain and Nervous System. May 23-24.

NeuroTechnology Solutions. (2014). MOXO ADHD analytics Professional guide(Version EU 1.00). Israel.

Miguel CS, Martins PA, Moleda N, Klein M, Chaim-Avancini T, Gobbo MA ve ark. (2016). Cognition and impulsivity in adults with attention deficit hyperactivity disorder with and without cocaine and/or crack dependence. *Drug Alcohol Depend*, 160, 97–104.

Neath, I., Earle, A., Hallett, D., Surprenant, A. M. (2011). Response time accuracy in Apple Macintosh computers. *Behavior Research Methods, 43*, 353–362.

Oktay, B. (2022). Deneysel psikolojide çevrimiçi veri toplama: Avantajları, dezavantajları, Etik Konular ve uygulamaları. *Celal Bayar Üniversitesi Sosyal Bilimler Dergisi*, *20*(1), 65–76. https://doi.org/10.18026/cbayarsos.874942

Plant, R. R., Hammond, N., Whitehouse, T. (2002). Toward an experimental timing standards lab: Benchmarking precision in the real world. *Behavior Research Methods, Instruments, & Computers, 34*, 218–226.

Sauter, M., Draschkow, D., Mack, W. (2020). Building, hosting and recruiting: A brief introduction to running behavioral experiments online. *Brain Sciences*, *10*(4), 251. https://doi.org/10.3390/brainsci10040251

Stewart, N. (2006). A PC parallel port button box provides millisecond response time accuracy under Linux. *Behavior Research Methods*, *38*, 170–173.

Slobodin, O., Blankers, M., Kapitány-Fövény, M., Kaye, S., Berger, I., Johnson, B., Demetrovics, Z., van den Brink, W., van de Glind, G. (2020). Differential diagnosis in patients with substance use disorder and/or attention-deficit/hyperactivity disorder using continuous performance test. *European Addiction Research*, *26*(3), 151–162. https://doi.org/10.1159/000506334

Slobodin, O., Cassuto, H.ve Berger, I. (2015). Age-Related changes in distractibility: developmental trajectory of sustained attention in ADHD. Journal of Attention Disorders, 1-11.

Tamm, L., Trello-Rishel, K., Riggs, P., Nakonezny, P.A., Acosta, M., Bailey G. ve ark., (2013). Predictors of treatment response in adolescents with comorbid

substance use disorder and attention deficit/hyperactivity disorder. *J Subst Abuse Treat*, *44*(2), 224–30.

Ulukan, M., Tekin, M. (2020). Okçuların imgeleme becerileri ile dikkat düzeyleri arasındaki ilişkinin incelenmesi. *Turkish Studies-Educational Sciences*, *15*(4), 3099–3110. https://doi.org/10.47423/turkishstudies.43631

Vaughan, R. S., Laborde, S. (2020). Attention, working-memory control, working-memory capacity, and sport performance: The moderating role of athletic expertise. *European Journal of Sport Science*, *21*(2), 240–249. https://doi.org/10.1080/17461391.2020.1739143

Valera, E.M., Faraone,S., Murray, K.E. etal. (2007). Meta-analysis of Structural Imaging Findings in Attention-Deficit/Hyperactivity Disorder. Biological Psychiatry. 61, 1369.

van Ede, F., & Nobre, A. C. (2022). Turning attention inside out: how working memory serves behavior. *Annual Review of Psychology, Forthcoming*.

Volkow, N.D.,Wang, G.J., Kollins,S.H.etal. (2009). Evaluating Dopamine Reward Pathway in ADHD: Clinical Implications.The Journal of the American Medical Association. 302, 1084-1091.

Voss, A., Leonhart, R., Stahl, C. (2007). How to make your own response boxes: A step-by-step guide for the construction of reliable and inexpensive parallel-port response pads from computer mice. *Behavior Research Methods*, *39*, 797–801.

Woo, J., Rajagopalan, P., & Andamon, M. M. (2022). An evaluation of measured indoor conditions and student performance using d2 Test of Attention. *Building and Environment*, *214*, 108940.

Wulf, G., Prinz, W. (2001). Directing attention to movement effects enhances learning: A review. *Psychonomic Bulletin & Review*, 8, 648-660

Zhou, H., Fishbach, A. (2016). The pitfall of experimenting on the web: How unattended selective attrition leads to surprising (yet false) research conclusions. *J. Personal. Soc. Psychol*, 111, 493–504.

Ziereis, S., Jansen, P. (2015). Effects of physical activity on executive function and motor performance in children with ADHD, *Research in Developmental Dis-*

abilities, 38, 181–91. doi: 10.1016/j.ridd.2014.12.005

Zwierko, T., Florkiewicz, B., Fogtman, S., Kszak-Krzyżanowska, A. (2014). The ability to maintain attention during visuomotor task performance in handball players and non-athletes, *Central European Journal of Sport Sciences and Medicine*, *7*(3), 99–106.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ (BTK DERGİ)
CİLT: 1 SAYI: 1 TARİH: TEMMUZ - EYLÜL 2023 ISSN: 2980-1311

BİLGİ VE İLETİŞİM TEKNOLOJİLERİNİN GELİŞMESİYLE DEĞİŞEN SİBER SUÇ TANIMI VE YAKLAŞIMLAR

Burak YAĞCI[1]

Özet

Bilgi ve iletişim teknolojilerinin günden güne gelişip değişmesiyle birlikte bireyler ve toplum açısından olumlu etkilerinin yanı sıra olumsuz etkileri de ortaya çıkmaktadır. Öyle ki suçlular için yeni bir faaliyet sahası oluşarak suça ilişkin yeni yöntemlerde ve suç çeşitliliğinde büyük bir artış söz konusu olmuştur. Kara, hava, deniz ve uzay ortamında meydana gelen klasik suç tiplerine ek olarak siber uzay adı verilen muğlak alanda meydana gelen suç tipleri, bilgi ve iletişim teknolojilerinin ilerlemesiyle farklı bir yöne evrilerek karmaşık bir yapıya ulaşmıştır. Bunun sonucunda siber suçların farklı teknolojilerle olan birleşiminde yeni dinamikler ortaya çıkmıştır. Öyle ki bu dinamikler devletlerin suça olan bakış açısını, mevzuatlarını ve buna ilişkin politikalarını değiştirmelerini gerekli kılmıştır. Bu ortamda karşılaşılan suçların uluslararası hukuk literatüründe kendisine henüz yer bulamadığı ve hukuki karşılığının olmadığı düşünüldüğünde, devletlerin karşılaştırmalı hukuk ve mütekabiliyet açısından yeknesak ve ortak bir siber suç tanımına sahip olması önem kazanmaktadır. Bu çalışmada siber suçun tanımı üzerine ulusal ve uluslararası literatür taranarak söz konusu alanda yer alan hukuki ve teknik boşluğun doldurulması amacıyla Birleşmiş Milletler (BM) nezdinde halihazırda çalışmaları devam eden taslak sözleşme çalışması detaylı şekilde incelenmiştir. Bu çerçevede literatür taramasıyla bilgi ve iletişim teknolojilerinin gelişmesi doğrultusunda devletlerin siber suça olan yaklaşımları ele alınmış, siber suçun değişen tanımına ilişkin hususlara değinilmiştir.

Anahtar Kelimeler: *siber suç, bilişim suçları, bilgi ve iletişim teknolojileri, siber güvenlik, siber uzay*

[1] Bilgi Teknolojileri ve İletişim Kurumu, burak.yagci@btk.gov.tr, ORCİD: 0009-0003-9787-8791

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ (BTK DERGİ)
CİLT: 1 SAYI: 1 TARİH: TEMMUZ - EYLÜL 2023

DEFINITION AND APPROACHES OF CYBERCRIME CHANGING WITH THE DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Abstract

As a fast evolving technology, ICTs (Information and Communication Technologies) generated benefits as well as drawbacks for individuals and society. Thus, a new field of activity has been created for criminals, and there has been a tremendous increase in new methods and crime diversity. In addition to the conventional types of crimes that occur in land, air, sea and space environments, the types of crimes that occur in the area called cyberspace have evolved into a different direction with the advancement of information and communication technologies and reached a complex structure. New dynamics, therefore, have emerged in the combination of cybercrime with different technologies. These dynamics made it necessary for states to change their perspective on crime, their legislation and their policies. Considering that the crimes encountered in this environment have not yet found a place in the international law literature and have no legal equivalent, it has become important for states to have a uniform and common definition of cybercrime in terms of comparative law and reciprocity. In this study, the national and international literature on the definition of cybercrime has been reviewed and the draft contract, which is currently in progress at the United Nations, has been examined in detail in order to fill the gap in this field. In this context, with the literature review, the approaches of states to cybercrime in line with the development of information and communication technologies were discussed and the issues related to the changing definition of cybercrime were mentioned.

Keywords: *cybercrime, ICT crime, informatıon and communication technologies, cyber security, cyberspace.*

GİRİŞ

Siber uzayın ülkesel sınırları aşan, özerk ve suç işlenmesini kolaylaştıran yapısı itibariyle bu alanda işlenen siber suçlar günden güne artış göstermektedir (AAG IT Services, 2023). Özellikle uluslararası mevzuat eksikliği ve cezai yaptırımlara ilişkin belirsizlikler siber suç faillerinin suç işleme motivasyonunu artırarak siber suç sayısındaki artışı etkilemiştir. Öyle ki bu faillerin siber alanın muğlaklığından faydalanmasıyla internet ortamındaki kullanıcıların hak kayıpları ve menfaat ihlalleri oluşmaya başlamıştır. Bunun yanı sıra kullanıcıların maddi ve manevi zararına neden olan siber tehditlerle, olumsuz sonuçların oluşturulmasına zemin hazırlanmıştır. Kullanıcıların bireysel olarak uğradığı zararlar sonrası devletler, söz konusu alanda vatandaşlarını korumak ve suçluları yakalayarak cezai yaptırıma tabi tutmak üzere koruyucu bir rol üstlenmek durumunda kalmıştır. Devletlerin hukuki sorumluluk alanında klasik suçlara ilişkin uyguladıkları yerel ve uluslararası mevzuatlar siber suçlara uygulanırken büyük sorunlarla karşılaşılmaktadır. Siyasi ve coğrafi sınırları aşan yapıdaki siber suçların faillerinin soruşturma ve kovuşturmaya tabi tutulması uluslararası alanda ortak bir mevzuat, siber suç tanımı ve müşterek yaklaşımı gerekli kılmıştır. Ancak devletlerin suça yaklaşımındaki farklılıklar müşterek bir uygulama tekniğinin önüne geçmektedir. Buradaki problem devletlerin diğer devletlerce suç sayılan hukuka aykırı fiilleri suç olarak tanımlamamış olmasından kaynaklanmaktadır. Devletler arası siyasi kutuplaşmalar ve ulusal politikaya bağlı oluşan fikir ayrılıkları, siber suçun tüm devletler tarafından kabul edilen küresel bir tanımının ve bu tanım etrafında oluşacak keskin bir çerçevesinin çizilmesine engel olmaktadır. Diğer taraftan gelişen teknolojilerin cezai suçların ölçeği, hızı ve kapsamı üzerindeki etkisi dikkate alındığında siber suçun hangi çerçevede ele alınacağı problemi ortaya çıkmaktadır. Devletlerin siber suça ilişkin yaptıkları tanımlamalar ulusal mevzuatlarındaki lafzi ve kanuni yorumları etkileyerek uygulamada farklılıklara yol açmaktadır. Söz konusu farklılıklar, birden fazla devleti etkileyen müşterek olaylarda siber suçun mülki sınırlara sığmayan yapısı itibariyle hukuki ve siyasi ihtilafların ortaya çıkmasına yol açmaktadır. Bu kapsamda siber suça ilişkin toplumu korumayı amaçlayan ve uluslararası iş birliğini destekleyen ortak bir siber suç tanımı ve politikasının oluşturulması önem arz etmektedir. Öyle ki ulusal ve uluslararası mevzuatlar çerçevesinde devletlerin karşılıklı olarak siber suça yaklaşımlarının aynı eksende olması, bu suçların faillerinin yakalanarak cezai yaptırım uygulan-

masına hizmet edecektir. Cezai yaptırım, suçluların iadesi, teknik yardım ve adli yardım gibi alanlarda devletler arası iş birliğinin hayata geçirilmesi söz konusu ortamda siber suça ilişkin ortak bir tanım üzerinde uzlaşılmasını sağlayacaktır.

Bu çalışmada siber uzay içerisinde işlenen siber saldırılar ve onların yol açtığı siber suçlara ilişkin tanımsal literatür ortaya koyularak siber suçların gelişen ve değişen teknolojilerle birlikte hangi kapsamda yorumlanması gerektiğine dair bir değerlendirme ortaya konulacaktır. Çalışmanın ilk bölümünde siber uzay ve siber suç kavramlarına dair ilgili akademik yazın ele alınacaktır. İkinci bölümde Türkiye'de siber suça olan yaklaşımlar üzerinde durulurken, üçüncü bölümde kavramın küresel ölçekte nasıl ele alındığına dair yaklaşımlara yer verilecektir. Dördüncü bölümde çalışmaları hala devam eden "Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Bilgi ve İletişim Teknolojilerinin Suç Amaçlı Kullanımıyla Mücadele Konusunda Kapsamlı Uluslararası Sözleşme)" isimli taslak çalışma detaylı şekilde incelenecektir. Son bölümde ise çalışmanın sonuçları tartışılarak çözüm önerilerine yer verilecektir.

I. SİBER SUÇ VE SİBER UZAY

Siber suç ifadesinin tam olarak anlaşılabilmesi, bu ifadeyi oluşturan terimlerin analiz edilmesi ile doğrudan bağlantılıdır. Siber ile suçun kesişimi zamanla gelişerek değişime uğrayan bilgi ve iletişim teknolojileri vasıtasıyla olmuştur. Bu kesişim yeni bir terim olan siber suçu ortaya çıkarmıştır. Suç terimi "törelere, ahlak kurallarına hukuki olarak da yasalara aykırı davranış, cürüm" şeklinde tanımlanmıştır (Türk Dil Kurumu, 2023). Bu tanımdan görüleceği üzere hem kanunda suç sayılan fiiller hem de toplum nezdinde suç olarak kabul edilen eylemler suç tanımına girebilmektedir. Ancak kanunsuz suç ve ceza olmaz ilkesi gereğince (kanunilik ilkesi) bu çalışmada kanunda suç sayılan ve uluslararası sözleşmelerde geçen siber suçlar üzerinden bir inceleme yapılacaktır. Diğer taraftan siber terimi ise BM tarafından yapılan tanımda "internete bağlı bilgisayarların, iletişim altyapılarının, çevrim içi iletişim yapan kişilerin, veri tabanı ve bilgi sistem araçlarının oluşturduğu küresel bir sistem" olarak ifade edilmiştir (Andress ve Winterfeld, 2013). Siber terimi bu tanıma göre bilgi ve iletişim ağlarını hatta internet kullanıcılarını da kapsayan genel bir kavram olarak ortaya çıkmaktadır. Siber suçlara ilişkin dünya üzerinde birçok farklı tanım yapılmış ancak çeşitli sebeplerle

ortak bir tanıma ulaşılamamıştır. Siber suç tanımının kesin ve yeknesak şekilde yapılamamasında belirleyici faktörler, siber uzayın genişliği ve siber suçlarla ilgili kriminolojik çalışmaların yetersizliğidir (Holt ve Bossler, 2020, s. 5-13). Siber uzay ya da diğer bir deyişle siber uzam, yapısı gereği fiziksel olmayan ve coğrafi olarak sınırları bulunmayan bir alandır. Lasky tarafından yapılan tanımda siber uzay "bilgisayarlar, bilgisayar ağları, internet ve internet ağına dahil diğer cihazlar ile bileşenler arasındaki bağlantıların neticesinde ortaya çıkan, teorik olarak var olan ve fiziksel bir şekli olmayan alan" şeklinde ifade edilmiştir (Lasky, 2022). Bu tanımdan hareketle siber uzayın geniş yapısı içerisinde birçok farklı teknolojinin kapsam dahilinde olduğu, ağa bağlanabilen cihazların internet ve internet ortamındaki içeriklerle ilişkili olarak çeşitli suçların işlenilmesinde araç olarak kullanılabileceği değerlendirilmektedir. Siber uzayın genişliğinden anlaşılması gereken bir diğer husus ise suç işlemek için esnek bir zaman aralığına sahip olunması ve faillerin bu alanda hareket edebilme kabiliyetlerinin yüksek olmasıdır. Siber suçlara ilişkin faaliyetlerde bulunan kişiler, kendilerini bu uzam içerisinde rahatlıkla gizleyerek devletlerin kolluk kuvvetlerinden ve siber güvenlikle ilgili otoritelerinden kaçabilmektedir.

Siber suça ilişkin literatürde birçok farklı tanım olmasına rağmen en sık karşılaşılan tanım "On The Definition And Classification Of Cybercrime" isimli makalelerinde Gordon ve Ford tarafından yapılan "bilgisayar veya bilgisayar ağları ve donanımları kullanılarak işlenen suç" şeklindedir. Bu ikili yaptıkları tanımı diğer yapılan tanımlamalardan ayrı tutarak kavramsal bir tabana oturtmak istemişlerdir. Siber suçlara ilişkin bir sınıflandırma yaparak iki tip siber suç üzerinden incelemelerde bulunmuşlardır. Bu sınıflandırmada belirleyici unsur, suçun oluşmasında ana faktörün insan etkisini içermesi ya da insan etkisinden uzak şekilde yazılımsal kodlar olmasındaki farklılıktır. Birinci tip suçları, siber suç tanımının insan unsurunu ön planda tuttuğu ve suçun oluşmasında insan faaliyetlerinin yeterli olduğu siber suçlar oluşturmaktadır. Bunlara ilişkin sosyal mühendislik faaliyetleri ve oltalama (phishing) gibi siber saldırı türleri örnek olarak verilebilecektir. İkinci tip siber suçları ise virüs, solucan veya kötücül yazılım saldırıları gibi yazılımsal kodlamaların söz konusu saldırılarda araç olarak kullanıldığı suçlar meydana getirmektedir (Gordon ve Ford, 2006, s. 13-20). Bu kapsamda değerlendirme yapıldığında farklı kategorilere ayrılan siber suçlara ilişkin yaklaşım farklılıklarının olduğu görülecektir. Kavramsal olarak beşeri veya yapay unsurlar

siber suç sınıflandırmasında etkili olmuştur. Bunun yanı sıra siber suçlarla ilgili tanımlar arasında mihenk taşı olarak kabul edilen Thomas ve Loader tarafından yapılan tanıma göre siber suç "yasa dışı olan veya belirli taraflarca yasa dışı kabul edilen ve küresel elektronik ağlar aracılığıyla gerçekleştirilebilen bilgisayar aracılı faaliyetler" şeklinde yorumlanmıştır (Thomas ve Loader, 2000). Burada meşru olmayan davranışlar söz konusu olmakla birlikte bunların yazılı veya yazısız hukuk kurallarının ihlal edilmesine yönelik bir ayrımı getirmediği görülmektedir. Öyle ki söz konusu tanımda belirli kesimlerce yasa dışı kabul edilen ifadesi toplumsal normları ifade etmektedir. Bir diğer dikkat edilecek nokta ise küresel ağlar kullanılarak yapılan ve araç olarak bilgisayarın kullanıldığı saldırıların bulunmasıdır. Burada araç bazlı yaklaşım ön planda tutularak bilgisayarın amaç olarak kullanıldığı veya bir geçiş vasıtası şeklinde yararlanıldığı diğer kategoriler tasnif dışı bırakılmıştır (Thomas ve Loader, 2000). Siber suçlara ilişkin bir diğer tanım da Brenner tarafından *"klasik suçtan farklı olarak siber ortamda bilgisayar sistemleriyle gerçekleştirilen suçlar"* şeklinde ifade edilmiştir. Brenner, klasik suç tipleri ile bilgisayar ortamında işlenen suç ayrımından yola çıkarak bir tanımlamada bulunmuştur. Bunun yanı sıra siber suçların kamu düzenini tehdit altına alan saldırılar vasıtasıyla işlenmesinden dolayı meşru olmayan davranışlar bütünü olduğunu dile getirmiştir. Geleneksel şekilde işlenen suçların bir dönüşüm içerisinde siber suçlara evrildiğini belirterek söz konusu bağlamın siber uzay olduğunu vurgulamıştır. Bu tanım etrafında siber suçlar üç farklı kategoride incelenmiştir. Bunların ilkini araç olarak bilgisayarın kullanımı oluşturmaktadır. Siber suçlar bilgisayarlar aracılığıyla gizlilik ön planda tutularak işlenebilmektedir. İkinci kategoride suçun işlenilmesinde bilgisayarın doğrudan değil dolaylı olarak tesadüfi şekilde etkisi olabileceğini değerlendirmiştir. Son kategoride ise bilgisayar hedef alınarak yapılan saldırılar kapsamında sınıflandırma yapılmıştır (Brenner, 2010, s.115). Brenner tarafından yapılan sınıflandırma bu çalışmanın uluslararası sözleşme çalışmaları kısmında incelenen taslak sözleşmede tartışma konusu olan sibere bağımlı suç *(cyber dependant),* siberle kolaylaşan *(cyber enabled)* veya siberle ilgili *(cyber related)* suçlar ayrımının kaynağını da oluşturmaktadır.

Siber suça ilişkin devletlerin genel olarak yaklaşımları da sibere bağımlı ve siberle kolaylaşan suçlar şeklindeki ayrım çerçevesinde ele alınmaktadır. Buna ilişkin devlet örneklerine bakıldığında Singapur Polis Gücü (SPF) ve Singapur Siber Güvenlik Ajansı tarafından yapılan ayrım önemli bir emsal teşkil etmekte-

dir. Öyle ki Singapur'da bu iki büyük güvenlik otoritesi siber suçları ikiye ayırarak belirgin bir ayrım yapmışlardır. İlk suç tipi olan sibere bağımlı suçlar kategorisinde, bilgisayar korsanlığı ve fidye yazılımı gibi siber saldırı türlerinin olduğu bilgisayarın hedef alındığı suçlar bulunmaktadır. Siberle kolaylaşan suç tipinde ise bilgisayarın araç olarak kullanıldığı çevrim içi dolandırıcılık, çevrim içi taciz, siber gasp ve diğer çevrim içi suçların olduğu siber özellikli suçlar yer almaktadır (SPF, 2023). Yine bunun gibi İngiltere tarafından benzer bir ayrım yapılarak siber suçlar kategorize edilmiştir. İlk tipteki suçlar, sadece çevrim içi cihazların kullanılması yoluyla işlenebilen ve bu cihazların hem suçun işlenmesinde araç hem de suçun hedefi konumunda olduğu suçlardır. İkinci tipteki suçları ise bilgisayar kullanılarak ölçeği artırılabilen geleneksel suçlar oluşturmaktadır. Söz konusu siber suçların içeriğinde bilgisayar korsanlığı, *dark web (*karanlık ağ), sosyal medyada *trolleme*, kimlik avı ve kimlik hırsızlığı, dağıtılmış hizmet reddi (DDOS) saldırıları, çevrim içi tehdit ve taciz, cinsel görüntülerin izinsiz ifşası gibi suçlar bulunmaktadır (The Crown Prosecution Service, 2022). Diğer taraftan siber güvenlikle ilgili hususlarda dünyada öncü olarak gösterilen Amerika Birleşik Devleti'nin (ABD) teknoloji ve standart enstitüsü olarak görev yapan National Institute of Standards and Technology (NIST) tarafından yapılan tanım "internet üzerinden veya bilgisayar teknolojisinin kullanılmasıyla işlenen suçlar" şeklindedir. Söz konusu suçlar ağ üzerinde de rahatlıkla işlenebilen suçlar olması nedeniyle tanımda internet vurgusu da yapılmaktadır. (NIST, 2023) Yine ABD'de federal bir kurum olarak görev yapan U.S Department of Justice (ABD Adalet Bakanlığı) nezdinde bilgisayar suçlarına ve siber suça ilişkin yaklaşım geniş bir perspektiften bakış açısı sağlamaktadır. Bakanlık nezdinde yapılan tanım "suçlanması, soruşturulması veya kovuşturulması için bilgisayar teknolojisi bilgisini içeren her türlü ceza hukuku ihlali" şeklindedir. Söz konusu tanım etrafında yapılan sınıflandırmada ilk olarak bilgisayarın suçun nesnesi konumunda olduğu, donanım ve yazılımlarının çalınması ifade edilmektedir. İkinci sınıfta bilgisayarın suçun maddesi konumunda olduğu bilgisayarlar ve sunucuları aracılığıyla mümkün kılınan meşru hizmet ve faaliyetlere kötücül şekilde müdahalelere ilişkin her türlü girişim ifade edilir. Son sınıfta ise bilgisayar bağlantılı suçlar bulunmaktadır. Burada klasik suçların işlenişinde bilgisayarın sağladığı kolaylıkla vasıta olarak kullanılması esas alınmaktadır (US Department Justice Office, 2023). Görüldüğü üzere siber güvenlik konusunda dünyada öncü olan devletler tarafından klasik siber suça yaklaşım içeren sibere bağımlı suçlar *(cyber dependant)* bir kenara bırakılarak

gelişen teknolojiyle farklı şekillerde ortaya çıkan suç tiplerini barındıran siberle kolaylaşan *(cyber enabled)* ve siberle ilgili *(cyber related)* siber suç tanımları tercih edilmektedir.

II. TÜRKİYE'DE SİBER SUÇA YAKLAŞIM

Ülkemizde siber suçlara ilişkin farklı tanımlar yapılmış olmakla birlikte, resmi olarak en son yapılan tanımlardan birisine 2020-2023 Ulusal Siber Güvenlik Strateji ve Eylem Planı'nda yer verilmiştir. Planın *"Tanımlar" kısmında siber suç; "bir bilişim sisteminin güvenliğini ve/veya buna bağlı verileri ve/veya kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlar"* olarak nitelendirilmiştir (Ulaştırma ve Altyapı Bakanlığı, 2023). Söz konusu tanım siber suça ilişkin Ülkemizin bakış açısını ve stratejik hedeflerini ortaya koymaktadır. Ulusal literatürde Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı bünyesinde oluşturulan "SiberAy" tarafından yapılan tanıma göre siber suç; "bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzay kaynaklı olarak çeşitli tehdit odaklarından gelen ve kanunlara göre suç kabul edilen eylemler" şeklindedir (Emniyet Genel Müdürlüğü, 2023).

Diğer taraftan, 5237 sayılı Türk Ceza Kanunu'nda (TCK) bilişim suçları düzenlenmekle birlikte resmi olmayan ikili bir ayrıma gidildiği söylenebilir. Bu ayrım Yargıtay içtihatlarında sıklıkla yer almakla birlikte uygulamada da teamül haline gelmiştir. Ayrımda bilişim suçlarına ilişkin fiillerin doğrudan ve dolaylı olarak işlenebilecek yapıda olması etkili olmuştur. Suçun ağırlaştırıcı unsuru konumunda bulunan ve suçun işleniş şeklini değiştiren durumlarda dolaylı bilişim suçlarından bahsedilebilir. İnternet ortamında bir kişiye karşı hakarette bulunmak fiziksel olarak da işlenebilen bir suç iken sanal ortamın getirdiği kolaylıktan yararlanılarak yapılan hakaret fiili dolaylı bilişim suçuna girmektedir. Söz konusu fiil sadece bilgisayar vasıtasıyla değil diğer teknolojik aygıtlar sayesinde de işlenebilmektedir. Bu yüzden klasik olarak kullanılan "bilgisayar suçları" ifadesi yerine "bilişim suçu" ifadesi ulusal mevzuatımızda tercih edilmektedir. TCK'nın üçüncü kısım onuncu bölümünde düzenlenen "Bilişim Alanında Suçlar", mezkûr Kanun'un 243, 244 ve 245. maddelerinde yer verilen bilişim suçları ile detaylandırılmıştır. 243.maddede "Bilişim Sistemine Girme (Yetkisiz Erişim) Suçu", 243. maddenin dördüncü fıkrasında "Sisteme Girmeksizin Verileri İzleme Suçu", 244. maddede "Bilişim Sistemine ve Verilere Müdahale Suçu", 245/A'da "Yasak Cihaz

veya Programlar", yine 245. maddede "Banka veya Kredi Kartlarının Kötüye Kullanılması" düzenlenmektedir (Türk Ceza Kanunu, 2004). Bu maddelerde suçun gerçekleştiği ortam olarak yer verilen bağlam bilişim sistemleridir.

Siber suçlara ilişkin ulusal mevzuatımızda 5237 sayılı TCK'da bilişim suçları başlığı altındaki suçlara ek olarak, bilişim sistemleri kullanılarak işlenen suçlara Kanun'un "Mal varlığına Karşı Suçlar" kısmında da yer verilmiştir. TCK'nın 142. maddesinde "Bilişim Sistemlerinin Kullanılması Suretiyle Hırsızlık" suçu tarif edilmiştir. Buna benzer olarak yine 158.maddede "Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık" düzenlenmektedir. TCK'nın 132 ile 138. maddeleri arasında "Özel Hayata ve Hayatın Gizliliğine Karşı Suçlar" kısmında "Haberleşmenin Gizliliğini İhlal", "Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması", "Özel Hayatın Gizliliğini İhlal", "Kişisel Verilerin Kaydedilmesi", "Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme", "Verileri Yok Etmeme" suçlarına yer verilmiştir. Sayılan suçlar bilişim suçları olarak nitelendirilerek yapıları itibariyle siber suçlar kategorisindedir. Özellikle de 135 ile 138. maddeler arasında düzenlenen kişisel verilerin korunmasına ilişkin hükümler, siber saldırı sırasında bilgisayar veya bilişim sistemlerindeki kişisel verilerin hukuka aykırı olarak ele geçirilmesi veya kullanılması gibi suç oluşturan fiillerin işlenmesinde gündeme gelecektir. TCK'nın 124 ve 125. maddelerinde "Haberleşmenin Engellenmesi" ve "Hakaret" suçları bilişim suçu olarak siber suç kategorisinde sayılmıştır. İlaveten, TCK'nın 286. maddesinde "Adliyeye Karşı Suçlar" kısmında "Ses veya Görüntülerin Kayda Alınması" suç tanımına yer verilmiştir (Türk Ceza Kanunu, 2004).

Bu kanun dışında 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda yer alan siber suçlar 71 ve 72. maddelerde "Manevi, Mali ve Bağlantılı Haklara Tecavüz" ile "Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri" şeklinde düzenlenmiştir (Fikir ve Sanat Eserleri Kanunu, 1951). Usul hukuku kapsamında 5271 sayılı Ceza Muhakemeleri Kanunu'nun (CMK) 134 ve 135. maddelerinde de yine bu alanda düzenlemede bulunulmuştur. Söz konusu maddelerde "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" ile "İletişimin tespiti, dinlenmesi ve kayda alınması" başlıkları altında gerekli düzenlemeler yapılmıştır (CMK, 2004). İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da (5651 sayılı Kanun) da yine bilişim suçlarına ilişkin hükümlere

yer verilmiştir. Bu Kanun'da içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı, toplu kullanım sağlayıcı ve sosyal ağ sağlayıcı gibi kavramlar üzerinde durularak uygulamaya yönelik olarak "içeriğin çıkarılması ve erişimin engellenmesi" düzenlenmiştir. Diğer taraftan bahsi geçen Kanunun 10. maddesinin altıncı fıkrasında Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) görevleri arasında siber saldırılara ilişkin tespit fonksiyonunun yerine getirilmesinde yukarıda sayılan internet süjeleri ile bağlantı kurarak kullanıcı mağduriyetlerinin giderilmesi konusunda koordinasyon ve gerekli tedbirlerin alınması hususu düzenlenmiştir (5651 Sayılı Kanun, 2007). Söz konusu yasada yer verilen ve sorumlu tutulan internet özneleri 2001 tarihli Avrupa Konseyi Siber Suçlar Sözleşmesi'nin (Budapeşte Sözleşmesi) 1. maddesinde yer verilen hizmet sağlayıcı tanımı içerisinde kendine karşılık bulabilmektedir. Öyle ki bu Sözleşme'de hizmet sağlayıcı "kamu veya özel tüzel kişilerinin dışında iletişim hizmeti sunan tüzel kişiler adına veya böyle bir hizmetin kullanıcıları adına bilgisayar verisini işleyen ve depolayan her türlü kişilik" olarak nitelendirilmiştir. Bu tanıma uyarlandığında 5651 sayılı Kanun'un internet özneleri olarak yukarıda sayılan sağlayıcıların da Sözleşme kapsamında hizmet sağlayıcı olarak kabul edilmesi mümkündür (Akpek, 2015, s. 64-65). 5651 Sayılı Kanun'da yer verilen maddelere bakıldığında söz konusu internet süjelerinin siber suçlarla bağlı bir ilişkisinin olduğu görülmektedir. Avrupa Konseyi Siber Suçlar Sözleşmesi kapsamında hizmet sağlayıcı olarak karşılık bulan bu süjeler yerel mevzuatlarda da yer almaktadır. Suçların sadece siber saldırı yöntemleri değil aynı zamanda hukuka aykırı içerik oluşturma, hukuka aykırı erişim, sosyal ağlar yoluyla işlenen suçları da içermesi nedeniyle söz konusu hükümlerin de işlerlik kazandığı bir kapsam alanı oluşmaktadır. Bu kapsamda söz konusu süjeler etkiledikleri alanlar çerçevesinde sadece sibere dayalı olan klasik suç türlerini değil aynı zamanda siberle alakalı olan ve siberin kolaylaştırdığı suç tiplerini de içerisine almaktadır. Özellikle de TCK kapsamında bilişim suçları olarak Kanun'un üçüncü kısım onuncu bölümünde düzenlenen suç tipleri "bilişim sistemleri" ifadesiyle bilgisayar sistemlerini de içerisine almaktadır. Söz konusu siber suçların kapsamına aldığı hususlara bakıldığında bilgisayar ve bilgisayar teknolojilerinin araç ve amaç olarak kullanımı asli önem arz etmektedir. Siber suçlar bu teknolojiler vasıtasıyla işlenebileceği gibi bu teknolojilere karşı da işlenebilmektedir. Diğer taraftan söz konusu teknolojilerin kullanımı suçların işlenmesinde önemli bir işlevsellik görerek farklı suçların oluşmasına yol açabilmektedir (Smith, Grabosky ve Urbas, 2004, s. 5-7). Söz konusu farklılıklar tanımlamaların da dar veya geniş

yorumlanarak değişik şekillerde ifade edilmesine sebebiyet vermektedir. Bu çerçeveden bakıldığında oluşturulan tanımlarda dar yorumlu tanımıyla siber suç; "bilişim sistemlerine, verilerine, gizliliğine, bütünlüğüne ya da sistemlerin veya verilerin fonksiyonuna karşı işlenen suçlar" iken geniş yorumlu olan tanımı "bilişim sistemleri ya da verileri aracılığıyla, bilişim sistemlerine veya verilerine karşı işlenen her çeşit suçlar" şeklinde ifade edilebilecektir (Aldoori, 2020, s. 20-21).

5070 sayılı Elektronik İmza Kanunu (EİK) kapsamında da adli ve idari suçlar şeklinde düzenlemeler bulunmaktadır. EİK'nın 16. maddesi elektronik imzaların kullanımına dair imza sahiplerinin rızasını şart koşmaktadır. Öyle ki bu madde kapsamında rıza dışı imzaya ait bilgiye veya imza oluşturma aracına erişim adli para cezası ile cezalandırılmıştır. Bunun yanı sıra imzaya ilişkin bilgiyi veren, kopyalayan ve uygunsuz şekilde e-imzayı tekrar oluşturanlar da aynı cezaya tabi olmaktadır. EİK'nın 17. maddesinde elektronik sertifikada sahtekârlık düzenlenerek söz konusu e-sertifikaları oluşturan, taklit eden, tahrif eden, haberi olmasına rağmen kullanan kişiler hapis ve adli para cezası ile cezalandırılacağı düzenleme altına alınmıştır. Aynı Kanun'un 18. maddesi kapsamında e-sertifika hizmet sağlayıcılarının yükümlülüklerini yerine getirmemesi durumunda idari para cezası öngörülmüştür. 19. maddede tüzel kişilere özgü güvenlik tedbiri düzenlenmekle birlikte gerekli şartların sağlanması durumunda tüzel kişiliğin etkinliğine ilişkin iznin iptali söz konusu olabilmektedir (Elektronik İmza Kanunu, 2004).

Bununla birlikte, yapılan ikincil düzenlemelerle siber suçların düzenlendiği kanunlar desteklenmektedir. Öyle ki siber suçlara karşı mücadele hususunda siber güvenliğin sağlanması büyük önem arz etmektedir. 5809 sayılı Elektronik Haberleşme Kanunu'nda (EHK) BTK'nın yetkileri ve idari yaptırımlara ilişkin icrai kuvveti hakkında bu Kanunun 60. maddesinde çeşitli hükümlere yer verilmiştir. Mezkûr maddenin on birinci fıkrasında "Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır" ifadesine yer verilmiştir. Yine aynı maddenin on ikinci fıkrasında BTK'nın bilgi ve belge taleplerinin herhangi bir gerekçeyle geri çevrilemeyeceği belirtilirken, on üçüncü fıkrada yükümlülüklerin yerine getirilmemesi durumunda idari yaptırım yetkisinin bulunduğu hüküm altına alınmıştır (EHK, 2008). BTK tarafından düzenlenen Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği bu alanda siber suçlara ilişkin düzenleme yapılan bir başka ikincil kaynak konumundadır.

Bu Yönetmelik'te siber suçların işlenmesinde araç olarak kullanılan bazı siber saldırı unsurları düzenleme içerisinde geçirilerek şebeke ve bilgi güvenliğinin sağlanmasına ilişkin işletmecilerin sağlamakla yükümlü oluğu hususlara yer verilmiştir. Yönetmeliğin 21. maddesinde şebeke güvenliğinin sağlanması amacıyla gerekli önlemlerin işletmeciler tarafından alınması yükümlülüğü getirilmiştir. Aynı Yönetmeliğin 35. maddesinde Dos/Ddos saldırıları, zararlı yazılımların yayılması ve benzeri siber saldırı yöntemlerine karşı korunmaya ilişkin yükümlülüklerden bahsedilmiştir. Diğer taraftan kritik altyapı sektörlerine ilişkin Enerji Piyasası Düzenleme Kurumu tarafından Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği ve Bankacılık Düzenleme ve Denetleme Kurumu tarafından Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik bu alanda ikincil düzenlemelere örnek olarak verilebilecektir. Yine Sermaye Piyasası Kurumu tarafından çıkarılan Bilgi Sistemleri Yönetimi Tebliğleri ve farklı versiyonları da siber güvenliğin sağlanmasında ulusal literatürde yer alan düzenlemeler arasında yer almaktadır.

III. ULUSLARARASI KURULUŞLARIN SİBER SUÇA YAKLAŞIMLARI

Siber suç için uluslararası kuruluşlar tarafından yapılan çeşitli tanımlar siber suça olan yaklaşımın ortaya konulması açısından önem arz etmektedir. Ekonomik Kalkınma ve İş birliği Örgütü (OECD) tarafından yapılan siber suç tanımı "otomatik işleme tabi tutulan verilere karşı veya verileri nakil etme işlemlerinde yasaya, ahlaki değerlere aykırı veya yetkisiz bir şekilde gerçekleştirilen her türlü eylemler" şeklindedir (Çolak, 2016, s. 4). Söz konusu tanımdan anlaşılan suça ilişkin eylemlerin sadece yasayla belirlenen sınırlı alanla kalmadığı aynı zamanda etik değerlere ve toplum ahlakına yönelik saldırılar da içerdiğidir. Bunun yanı sıra verilerin nakil sürecine ilişkin hususlara da bu tanımda değinilmiştir. Öyle ki yasa dışı erişim sağlanan sistemler üzerinden verilere müdahale edilerek verilerin silinmesi, değişikliğe uğratılması ve kullanılamayacak hale gelmesine zemin hazırlanabilmektedir. Söz konusu ifade, ileride daha ayrıntılı şekilde değinilecek olan siberle kolaylaşan ve siberle ilgili suçların ulusal ve uluslararası metinlerde kendisine yer bulmasına hizmet edebilecek bir tanım konumunda bulunmaktadır. OECD tarafından 1996 yılında kurulan ve siber saldırılarla ilgili kriptolojik politikaları yürüten Committe on Information, Communications and Computer

Policy (ICCP) söz konusu alanda önemli bir komite görevindedir (ICCP, 2010). Bunun yanı sıra "OECD Policy Guidance on Online Identity Theft" isimli rapor internette kimlik avı hırsızlığına ilişkin rapor siber saldırıların suça bakan yönüne ilişkin önemli bir kaynaktır (OECD, 2008).

Avrupa Konseyi nezdinde insan hakları ve suçların önlenmesine dair tedbirlere ilişkin yapılan birçok çalışmanın yanı sıra siber suçlar alanında da çeşitli sözleşme çalışmaları yapılmıştır. Bu kapsamda hazırlanan "Programme on Cybercrime" çerçevesinde küresel anlamda teknik ve hukuki destek sağlanmaktadır. İnternet ortamında işlenen suçların önlenmesine dair saik doğrultusunda 2005 yılında "The Convention on the Prevention of Terrorism" ile birlikte terörizmin önlenmesine dair çok önemli bir sözleşme oluşturulmuş ve bu çalışma tüm ülkelere bir atıf kaynağı teşkil etmiştir. 2007 yılında Konsey tarafından "The Lanzarote Convention" hazırlanarak internet ortamında çocukların cinsel istismarını konu edinen önemli bir sözleşme daha literatüre girmiştir. Bu kapsamda çocuk haklarının korunması ve çocukların çevrim içi yollarla suça karışmasını önlemek adına önemli bir adım atılmıştır (Council Of Europe, 2023). 2001 yılında siber suçlarla mücadele alanında tek bağlayıcı uluslararası belge olarak ortaya çıkan "Avrupa Konseyi Siber Suçlar Sözleşmesi" siber suçlarla ilgili hazırlanan mevzuatın temelini oluşturan sözleşme konumundadır. Söz konusu Sözleşme 2003 yılında kabul edilen bilgisayar sistemleri aracılığıyla işlenen ırkçılık suçlarına ilişkin ek protokol ile zenginleştirilmiştir. Avrupa Konseyi Siber Suçlar Sözleşmesi'nde yapılmış olan siber suç tanımına bakıldığında suçların tasnif edilerek tanıma işlendiği görülmektedir. Bu tanım dört kategorinin birleştirilmesiyle "bilgisayar veri ve sistemlerinin gizlilik, bütünlük ve erişilebilirliğine, dolandırıcılık ve sahteciliğe, çocuk pornografisine, telif ve benzeri haklara yönelik bilgisayarla ilgili her türlü kötü niyetli eylemler" olarak nitelendirilmiştir (Council Of Europe, 2001). Yine bu tanımda da OECD tarafından yapılan tanıma benzer olarak siber suçların klasik şekilde sibere dayalı suçlar etrafında sınırlanamayacağı aynı zamanda çocuk pornografisi, dolandırıcılık, sahtecilik ve fikri mülkiyet gibi geniş bir alanı da içine alan siberle ilgili ve siberin kolaylaştırdığı suç tiplerini kapsayan yapıda olması gerektiği anlaşılmaktadır. Diğer taraftan, söz konusu Sözleşmenin 2001 tarihli olması nedeniyle teknolojik gelişmelerin henüz zirveye ulaşmadığı, temel seviyede sadece bilgisayar üzerinden işlemlerin yapılabilir olduğu bir dönemde yürürlüğe girmesinden dolayı bilişim sistemleri ifadesi metinde kendine

yer bulamamıştır. Bu ifade yerine tanımlarda ve içerikte bilgisayar sistemi ifadesi kullanılmıştır. Bu da gelişen ve ilerleyen teknolojinin beraberinde getirdiği çeşitli cihazların karşılık bulabileceği daha kapsamlı bir ifadenin mevzuatlarda ve uluslararası sözleşme metinlerinde kendisine yer bulması ihtiyacını gerektirmiştir.

Interpol tarafından yapılan tanıma bakıldığında söz konusu alanda evrensel olarak bir niteleme yapılamayacağı görüşüne varılmıştır. Interpol, siber suçları ikili bir ayrıma tabi tutmaktadır. İlk siber suç tipi, yüksek teknoloji suçu olarak nitelenen ve teknolojinin gelişmesiyle yazılımsal olarak bilgisayarlara karşı işlenen suçlardır. İkinci tip siber suçları ise siber uzay bağlamında işlenen suçlar oluşturmaktadır (Lin ve Masys, 2018, s. 65-66). İkinci tip suçların OECD ve Interpol tanımlarına paralel şekilde daha geniş yorumlanarak siber suç tiplerinin sayıca artırıldığı gözlemlenmektedir. Tanımlamalarda farklı şekillerde ele alınan siber suç, bazı metinlerde bilgisayar ortamı ile sınırlandırılmış, bazı yerlerde ise bilişim sistemleri ile genişletilerek daha büyük çerçevede ele alınmıştır. Siber suç kavramı söz konusu tanımlardan anlaşılacağı üzere farklı yorumlamalara açık bir konumda bulunmaktadır. 2017'de Interpol tarafından hazırlanarak yayınlanan strateji siber suçlarla mücadelede siber saldırıları gerçekleştiren kişi veya grupların tespiti hakkında önemli bilgiler içermektedir. Dijital delillerin elde edilmesinden uluslararası iş birliğine kadar birçok farklı etken söz konusu strateji belgesinde yer almaktadır (Interpol, 2017).

Uluslararası Telekomünikasyon Birliği (ITU) tarafından yapılan siber suçlara ilişkin sınıflandırma dört kategori altında detaylandırılmıştır (ITU, 2009). Bunların ilki "bilgisayardaki veri ve sistemlerin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı işlenen suçlardır (yasa dışı erişim, verileri çalma, veriye müdahale vb.)". Bu kısımda klasik olarak siber suçların sibere bağımlı olarak işlendiği şekilde suçların tasnifi yöntemine gidilmiştir. İkinci kategori "bilgisayar ile ilgili suçlar (online kumar, kimlik hırsızlığı, ücret sahteciliği vb.)" kapsamında ayrıntılı şekilde düzenlenmiştir. Bu gruptaki suçlar da daha önce belirtildiği şekilde siberle ilişkili olarak nitelendirilebilir. Üçüncü kategoride "içerikle ilgili suçlar (ırkçılık, nefret söylemi, şiddeti övme, yanlış bilgi vb.)" düzenlenmiştir. Söz konusu kategorideki suçlar internet ortamında kolaylıkla işlenebilen, halkı kışkırtmaya yönelik fiillerle beraber seyredebilen bir yapıdadır. Öyle ki kimliğini gizleyerek internette dezenformasyon çalışmaları yapabilen birçok bot hesap bulunmakta hatta *deepfake* uygulamaları ile gerçekte söylenmemiş sözler, hedef alınan kişi-

lerin ağzından çıkar şekilde kurgulanabilmektedir. Son olarak "Telif hakkıyla ilgili suçlar (telif ve fikri mülkiyet haklarına saldırı)" dördüncü kategori olarak detaylandırılmıştır. Özellikle internet ortamında yayınların artmasıyla beraber fikri mülkiyet haklarını ihlal edecek nitelikte siber saldırılar meydana getirilebilmektedir (BTK, 2022, s. 24). ITU tarafından 2007 yılında siber suçlarla mücadele konusunda temel hedeflerin belirlendiği "Global Cybersecurity Agenda (GCA)" önemli bir strateji eylem planı konumundadır. GCA kapsamında siber suçlara yönelik teknik ve hukuki kapasitenin artırılması, iş birliği ve koordinasyonun sağlanması konuları üzerinde çalışmalar ve raporlar yayınlanmıştır (GCA, 2007).

Avrupa Birliği nezdinde 2013 yılında yayınlanan ve siber saldırılara karşı korunma, siber tehditlerin tespiti ve önlenmesi, siber dayanıklılık ve üye ülkelerdeki gerçek ve tüzel kişilerin güvenilir dijital teknolojilere ulaşmasını hedefleyen "The EU Cybersecurity Strategy" kapsamında yapılan siber suç tanımı "bilgisayarların ve bilgi sistemlerinin birincil araç ya da birincil hedef olarak nazara alındığı geniş bir yelpazede farklı suç faaliyetleri" şeklindedir. Burada hem bilgisayar hem bilgi sistemleri tanım kapsamına alınmıştır. Ayrıca araç ve hedef bazlı iki türlü yaklaşımın da mümkün olabileceği değerlendirilmiştir. Söz konusu strateji 2020 yılında geliştirilerek fiziksel ve kritik varlıkların siber dayanıklılık derecesinin artırılması hedeflenmiştir (European Commission, 2022). Diğer taraftan ağ ve bilgi sistemlerinin güvenliğine ilişkin kuralların toplandığı, kritik altyapı ve sistemlerin korunmasının amaçlandığı "Ağ ve Bilgi Sistemleri Direktifi" olarak Türkçeye çevrilen "The Directive On Security Of Network And Information Systems (NIS Directive)" 2020 yılı içinde "Directive On Measures For A High Common Level Of Cybersecurity Across The Union (NIS2 Directive)" ismiyle revize edilmiş, (AB) 2022/2555 sayılı karar ile onaylanarak 16 Ocak 2023 tarihinde yürürlüğe girmiştir (European Commission, 2023a). Direktif kapsamında Avrupa Siber Kriz İrtibat Organizasyonu Ağı (EU-CyCLONe) hayata geçirilerek siber suçlara ilişkin bir koordinasyon ve iş birliği ağı kurulmaktadır. Bu kapsamda bahsi geçen direktif aynı zamanda siber suçlarla mücadele noktasında siber suçluların önünde bir engel konumunda bulunmaktadır. Aynı zamanda temel ve önemli kuruluşlar tarafından sağlanan hizmetlerin yüksek düzeyde siber güvenliğinin sağlanması bu hizmetlere yönelik siber saldırılar sonucunda oluşabilecek siber suçların sayısında büyük bir azalma sağlayacaktır. EU-CyCLONe kapsamında siber suç ve suçlulara ilişkin bilgi alışverişi artarak üye ülkeler arası siber suçlarla

mücadele hususu pekiştirilecektir (ENISA, 2023). Söz konusu yeniliklere ek olarak Avrupa Birliği genelinde dijital unsurlar içeren ürünlerin siber güvenliğinin arttırılması ve halihazırda bulunan siber güvenlik tüzüklerindeki açıkların kapatılması amacıyla 15 Eylül 2022 tarihinde Avrupa Komisyonu tarafından "Cyber Resilience Act (CRA)" adlı tüzük taslağı yayınlanmıştır. Söz konusu tüzük Internet of Things (IoT) ile ilgili yapılan ilk kanuni çalışma olmakla birlikte ağa bağlanabilen ve dijital unsur içeren tüm ürünler bu çerçevede düzenleme altında olacaktır. Siber suçların sadece bilgisayarlar değil çeşitli teknolojik aygıtlar kullanılarak da işlenebildiği dikkate alındığında söz konusu çalışmanın siber suçların ve suçluların önüne bir diğer engel olduğu söylenebilecektir. Öyle ki piyasaya sunulan dijital ürünler ve cihazlar, Avrupa Siber Güvenlik Ajansı (ENISA) bünyesinde oluşturulan European Cybersecurity Certification Framework (ECCF) kapsamında belirli bir denetleme sürecinden geçtikten sonra güvenilir damgalı etiketlerle son kullanıcıya sunulması siber güvenlik açısından kritik öneme sahip olacaktır (European Commission, 2023b). Diğer taraftan 2019 yılında AB Parlamentosu tarafından çıkarılan Avrupa Birliği Siber Güvenlik Kanunu (CSA) kapsamında ENISA kendisine verilen yetkiler çerçevesinde siber saldırılara karşı etkin mücadele yetisine sahip olmuştur. Bununla birlikte siber güvenliğe ilişkin sertifikasyon süreçlerinin yönetimi kapsamında ürün güvenliğine ilişkin bir sistem oluşturulmuştur. Söz konusu yasa dolaylı olarak siber suçların işlenmesini zorlaştıran ve siber saldırılara karşı savunma yönünü güçlendiren bir çerçeve çizmiştir (European Commission, 2023c). 18 Nisan 2023 tarihinde Komisyon tarafından önerilen değişikliklerle birlikte söz konusu siber tehdit içeren olayların tespit edilmesi, önlenmesi, sızma testleri ve güvenlik denetimleri gibi "managed security services" olarak nitelendirilen sertifikasyon uygulamasının benimseneceği değerlendirilmiştir. Kritik siber güvenlik hizmetlerinin güvenilirliğinin sağlanması hususu geliştirilerek "The EU Cyber Solidarity Act" yasa teklifi kapsamında "European Cybersecurity Shield" programının hayata geçirilmesi gündeme gelmiştir. Bu kapsamda uluslararası boyutta iş birliği ve koordinasyon sağlayacak bir sistem hayata geçirilmek istenmiştir. 2024 yılından itibaren öngörülen "Security Operations Centres (SOCs)" faaliyete başlayacak olup siber saldırılara karşı acil müdahale planları uygulanacaktır (European Commission, 2023d). Bu kapsamda söz konusu öncül tedbirler siber suçluların saldırı yapmasındaki motivasyonlarını azaltan, sonraki süreçlerde üye ülkeler arasındaki iş birliği kapsamında suçluların yakalanma riskinin artmasından dolayı suça yönelik caydırıcı

bir etki sağlamaktadır. Bunun yanı sıra 2013 yılında Europol tarafından kurulan ve bir görevi de AB kapsamında siber suçlara karşı adli makam ve kolluk kuvvetlerinin (LEAs) siber saldırılarla mücadelesini güçlendirmek olan "Europol's European Cybercrime Centre (EC3)" aynı zamanda çevrim içi suçlara karşı tüm paydaşları koruyucu bir yapıdadır. Bu merkez, "EU Law Enforcement Emergency Response Protocol (EU LE ERP)" vasıtasıyla kolluk kuvvetlerine operasyonel destek sağlayarak sibere bağımlı suçlar, çocuğun cinsel istismarı, ödeme dolandırıcılığı, dark web ve diğer platformlardaki suç tiplerine yönelik mücadelede büyük katkı sağlamaktadır. Kritik altyapı ve bilgi sistemlerini etkileyen siber suçlarla mücadelede öncü olmaktadır (Europol, 2023a). Yine Joint Cybercrime Action Taskforce (J-CAT) birimi EC3 bünyesinde siber suçlara karşı sınır ötesi soruşturma ve operasyon planlamalarında icrai rol alarak istihbarat odaklı eylemleri koordine etmektedir (Europol, 2023b). Bununla birlikte 2010 yılında bu yana çalışmalarına devam eden European Union Cybercrime Task Force siber suçların ve siber destekli suçların işlenmesini önleyici tedbirler alarak suça ilişkin altyapıları ortadan kaldırma amacını taşımaktadır (Europol, 2023). Avrupa Birliği bünyesinde oluşturulan direktif ve düzenlemelerin de siber suçlar alanında bağlayıcılık taşıyan hukuki metinler olarak bu suçlara karşı mücadelede önem arz ettiği varsayılabilir. Avrupa Birliği bünyesinde söz konusu direktifler elektronik ticarete ilişkin işlenen suçlarla birlikte kişisel verilerin ihlaline ilişkin suçları ve rıza dışı erişim sağlanan bilgisayar ve bilişim sistemlerini de içine almaktadır. Yine bu alanda pos cihazı ödemeleri ve internet yoluyla güvenli ödemelere ilişkin düzenlemeler de bulunmaktadır. Çocukların cinsel istismarı, fuhşa yönlendirme ve çocuk pornografisine yönelik çalışmalar Avrupa Birliği dahilinde yürütülen direktif çalışmalarında mevcut olan düzenlemeler arasındadır. Söz konusu uluslararası düzenlemeler, Sözleşme oluşturulurken ana atıf metni görevi görmektedir. Bu düzenlemeler dikkate alınarak hazırlanacak Sözleşme dilinin yeknesak şekilde oluşturularak metin düzeyinde birlik ve bütünlük sağlanması önem arz etmektedir (EUR-Lex, 2023).

Birleşmiş Milletler'in (BM) siber suçlara ilişkin yaptığı sınıflandırmada üç kategoriye yer verilmiştir. Bunların ilki "Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim" başlığı altında "Yetkisiz Erişim", "Yetkisiz Dinleme" ve "Hesap İhlali"dir. Yetkisiz erişimde bilgisayar sistem veya ağlarına kişi veya kişilerce rıza dışı erişilmesi söz konusudur. Dinleme ise yetkisiz şekilde erişilen bilgisayar

sistemlerindeki iletişimlere yönelik bir davranıştır. İletişim kanalıyla aktarılan veri transferleri bu şekilde takip edilmektedir. Hesabın ihlal edilmesinde amaç ödeme yapılmasından kaçınmak gayesiyle üçüncü kişilerin hesaplarını yasa dışı kullanmaktır. İkinci kategori suç sınıfına "Bilgisayar Sabotajı" girmektedir. Öyle ki bilgisayar sabotajı bu sınıflandırma içerisinde çeşitlendirilerek "mantıksal", "fiziksel", "bilgisayar yoluyla" şeklinde isimlendirilerek alt kategorilere ayrılmıştır. Bilgisayar sistemlerinin fonksiyonlarını önleyerek veri ve programlarda "truva atı", "virüs", "solucanlar" ve "zaman bombası" gibi siber saldırı türleri ile yazılımsal olarak tahribat yaratmak amaçlanmaktadır. Bu veriler söz konusu yazılımlar vasıtasıyla silinebilmekte, değiştirilebilmekte ve yok edilebilmektedir. Hedefleri doğrultusunda kişisel çıkarlar gözetilerek (örneğin ekonomik kazanç) veriler üzerinde değişiklik de yapılabilmektedir. Ekonomik kazanç kapsamında "Banka Kartı Dolandırıcılığı" suçu ön plana çıkmaktadır ki BM tarafından buna ikinci kategori suçlarda yer verilmiştir. Özellikle "Automated Teller Machine (ATM)" olarak adlandırılan kartlı ödeme sistemlerine yönelik işlenen suçlar söz konusu kartların çalınarak kopyalanması şeklinde vuku bulmaktadır. Aynı zamanda bu suçlar kurban olarak seçilen kişilerin dinlenilmesi veya haberleşme hatlarının engellenmesi yoluyla da ortaya çıkabilmektedir. Bilgisayar sistemlerine kasti olarak hatalı veri girişi yapılarak ortaya çıkan "Girdi/Çıktı/Program Hileleri" ikinci kategoride düzenlenen suçlar sınıfındadır. "İletişim Servislerini Haksız ve Yetkisiz Olarak Kullanma", "Bilgisayar Yoluyla Sahtecilik", "Bilgisayar Yazılımının İzinsiz Kullanımı", "Lisans Sözleşmesine Aykırı Kullanım" ve "Lisans Haklarına Aykırı Kiralama" bu kapsamda düzenlenen diğer suçlardır. Üçüncü kategoride ise "Diğer Suçlar" şeklinde belirli suç tipleri sıralanmıştır. Bu suçlar; "Kişisel Verilerin Suistimali", "Sahte Kişilik Oluşturma ve Kişilik Taklidi" ve "Yasa dışı Yayınlar" olarak verilmiştir. Özellikle kişisel verilerin ihlali, siber saldırılar yoluyla kurumların veri tabanlarında devletlerin vatandaşlarına ait bilgilerin alınması yoluyla ortaya çıkmaktadır. Sahte kişilikler oluşturma suçunda ise; gerçek kişilere ait kimlik bilgilerinin suçlular tarafından kendi özelliklerine haiz kimlikler gibi kamuoyuna sunulması temel hareket fiili olarak ortaya çıkmaktadır. Bunun yanı sıra hayali karakterler oluşturularak menfaat sağlama şeklinde de bu suçun görünümü bulunmaktadır (BTK, 2022, s. 18-22). BM nezdinde siber suçlarla ilgili birçok karar alınmasının yanı sıra 1995 yılında "Group of Seven (G7)" kapsamında sınır aşan organize suçlarla mücadele hususu ciddi şekilde ele alınmaya başlamıştır. 1995 yılından itibaren ekonomik suçların yanı sıra terörizm ve uyuşturucuyla

ilgili suçlar temelinde faaliyetler yürüten G7 grubu bünyesinde, "Lyon Grubu" adında yeni bir alt komisyon kurulmuştur. 1996 yılında sınır aşan organize suçların yanına siber suçlarla mücadele görevini de üstlenen bu grup devletler arası siber suçlara karşı iş birliğinde öncü bir konuma gelmiştir (Council of Europe, 2023). 1997 yılında kurulan alt komisyon "High Technology Crime Subgroup" bünyesinde "International 24/7 Point of Contact Network" ağ yapısı kurularak 7/24 esaslı çalışma hayata geçirilmiştir. Söz konusu gruplar bahsi geçen tarihlerden günümüze kadar belirli periyotlarda toplanarak siber güvenlik ve siber suçlarla ilgili küresel stratejilerin belirlenmesinde büyük rol oynamıştır (Euromed Justice Program, 2021).

IV. BİLGİ VE İLETİŞİM TEKNOLOJİLERİNİN SUÇ AMAÇLI KULLANIMIYLA MÜCADELE KONUSUNDA KAPSAMLI ULUSLARARASI SÖZLEŞME ÇALIŞMASI

Avrupa Konseyi Bakanlar Komitesi onayı ile 08.11.2001 tarihinde kabul edilen ve 01.07.2004 tarihinde yürürlüğe giren Avrupa Konseyi Siber Suçlar Sözleşmesi siber suçlarla mücadele alanında yapılmış olan en önemli sözleşme hükmünde yer almaktadır. Türkiye ise söz konusu Konsey'in kurucu üyesi olarak 10.11.2010 tarihinde sözleşmeyi imzalamıştır. Bu sözleşme Ülkemizde 29.09.2014 tarihinde yürürlük kazanmıştır. Avrupa Konseyi Siber Suçlar Sözleşmesi Ülkemizde "Sanal Ortamda İşlenen Suçlar Sözleşmesi" şeklinde resmi şekilde tercüme edilmiştir. Sanal Ortamda İşlenen Suçlar Sözleşmesi 37. maddesi gereğince Konsey'e üyelik durumuna bakılmaksızın tüm ülkelere uygulanabilmektedir (Usta ve Benzer, 2018, s. 35-42). Mezkûr Sözleşme kılavuz olarak değerlendirilerek son zamanlarda siber suça ilişkin yapılan ayrımlara bakıldığında mevzuat çalışmaları içerisinde sibere bağımlı *(cyber dependant)* başlığı altında bilgisayarla ilişkili (computer system) ve siberle ilişkili *(cyber related)* başlığı altında bilgi ve iletişim teknolojileriyle ilişkili *(information and communications technology system/device)* siber suç sınıflandırması yapıldığı görülmektedir. Bu seçeneklerin ülke mevzuatlarına uygulanmasında belirleyici faktör daha önce de değinildiği üzere devletlerin siber suça ilişkin tanımlamaları, yaklaşımları ve ulusal politikalarıdır. Söz konusu düzenleme temel alınarak Birleşmiş Milletler Genel Kurulu tarafından alınan 74/247 sayılı kararla (United Nations General Assembly [UNGA], 2020) bilgi ve iletişim teknolojilerinin suç amaçlı kullanımına karşı kapsamlı şekilde uluslarara-

sı bir sözleşmenin yapılması için açık uçlu, hükûmetler arası, geniş temsil bölgesine sahip ve uzmanlardan oluşan "Bilgi ve İletişim Teknolojilerinin Suç Amaçlı Kullanımıyla Mücadele Konusunda Kapsamlı Uluslararası Sözleşme" (Sözleşme) hazırlanması amacıyla Ad Hoc Komite kurulmuştur. Siber andaki boşlukların doldurulması ve yeni teknolojik gelişmeler ışığında siber suçların kapsamının genişlemesi ile ilgili bir sözleşme hazırlanması gereği öngörülmüştür. Ulusal, bölgesel ve uluslararası düzeylerde uzmanlar grubu ile ülkeler arasında istişareler yapılarak bahsi geçen Sözleşme metninin oluşturulması amaçlanmıştır. 74/247 sayılı Genel Kurul kararı gereğince oluşturulan Ad Hoc Komite tarafından 2021 Mayıs ayında Newyork'ta organizasyonel bir oturum (United Nations Office on Drugs and Crime [UNODC], 2021) gerçekleştirmiştir. Söz konusu organizasyonel oturumda sözleşme kapsamındaki faaliyetler ve oluşturulacak metin üzerinde tematik görüşmelerde bulunulmuştur. Mayıs ayı içerisinde yapılan Genel Kurul toplantısında 75/282 sayılı karar (UNGA, 2021a) kabul edilmiştir. Bu kararda bilgi ve iletişim teknolojilerinin cezai amaçlarla kullanılmasına karşı koymak ana amaç olarak belirlenmiştir. Söz konusu ifade aynı zamanda ilgili kararın başlığını oluşturmuştur. Kararda en az altı oturum şeklinde Newyork ve Viyana'da düzenlenecek şekilde organizasyon yapılması hususu karara bağlanmıştır. Genel Kurulun 76/552 sayılı kararı (UNGA 2021b) üzerine, 2022 Şubat ve Mart ayları arasında toplanılarak Komite için oturumlarda gerçekleştirilecek çalışma şekli, izlenecek yol haritası ve çalışmalar (UNODC, 2021) üzerinde mutabık kalınmıştır (UNODC, 2022a).

Bilgi ve iletişim teknolojileriyle (ICT) işlenen klasik suçların *(cyber dependent)* yanı sıra bilgisayar sistemlerinin yapısı itibariyle suçun işleniş şeklini, sonuçlarını, yapılış anını ve süresini değiştirdiği çocuk istismarı, sahtecilik, hırsızlık ve dolandırıcılık gibi siberle kolaylaşan *(cyber-enabled)* ve terörizm, soykırım, uyuşturucu kaçakçılığı gibi diğer anlaşmalarda mevcut olan ICT'lerin kolaylaştırdığı suçlar Sözleşme kapsamında gerçekleştirilen oturumlarda tartışılmıştır. Bu suçların Sözleşme metninde yer alıp almaması üzerine süregelen oturumlarda gündeme getirilen tartışmalarda söz konusu suçlar için hangi terimlerin tercih edileceği de devletler arasında görüş ayrılığına sebep olan konular olmuştur (UNODC, 2023a). Sözleşme kapsamında ülkelerin taslak metne ilişkin verdikleri görüşlerde sibere bağımlı *(cyber dependent)* veya siberle kolaylaşan *(cyber enabled)* şeklinde iki farklı yaklaşımın olduğu görülmektedir (UNODC, 2023b). Bu Sözleşme'nin

hazırlanmasında devletler tarafından kabul olunan ortak kanı, içeriğin belirli bir alana yönelerek uluslararası ortamdaki diğer düzenlemelerin uygulama alanlarını ihlal etmemesi ve söz konusu düzenlemelerle yeknesaklığa sahip olmasıdır. Aynı zamanda Birleşmiş Milletler Sınır Aşan Suçlarla Mücadele Sözleşmesi (UNTOC) ve Birleşmiş Milletler Yolsuzlukla Mücadele Sözleşmesi (UNCAC) gibi metinlerde yer alan suç türlerinin tekrar Sözleşme'de ele alınmasının tekerrüre düşüleceği anlamına gelebileceği vurgusu yapılmıştır. Bunun aksi durumda sözleşmelerin birbiriyle uyumsuzluğu gündeme gelerek çeşitli ihtilafların ortaya çıkması sonucunu doğurabileceği belirtilmiştir. Bu kapsamda, siber suçların işleniş şekilleri gereği birçok alanı etkileyen ve gelişen teknolojilerle karmaşık bir yapıda bulunması sebebiyle sözleşme hükümlerinin geniş yorumlanmasından uzak durulması gündeme gelmiştir. Buradaki amaç sınırlı olarak tutulan hüküm yorumu vasıtasıyla iç mevzuata uyum sağlama ve uygulamaya yönelik kolaylıklar sağlamaktır (UNODC, 2022b).

Sözleşme kapsamında Ad Hoc Komite'nin konsolide şekilde oluşturduğu ve devletlerin görüşlerine açılan taslağın son haline ilişkin metinde ikinci bölümde yer verilen "Suçlaştırma (*Criminalization*)" başlıklı kısımda oldukça kapsamlı düzenlemeler bulunmakla birlikte burada tanzim edilen suçlar sibere bağımlı (*cyber dependant) ve* siberle alakalı olarak *(cyber relatd)* tasnif edilmiştir. Bilgisayar sistemlerine veya bilgi ve iletişim teknolojileri sistem veya aygıtlarında *"illegal access (*yasa dışı erişim)*", "illegal interception* (yasa dışı müdahale)*", "misuse of devices* (cihazların kötüye kullanılması)*", "forgery* (sahtecilik)*", "fraud* (dolandırıcılık)*", ve "theft* (hırsızlık)*"* gibi suçları içeren bölüm, yukarıda daha önce değinilen ve ülkelerin kendi mevzuat ve politikalarına göre görüş vermeleri beklenen bilgisayar ya da bilgi ve iletişim teknolojileri ayrımı ile birlikte 2001 tarihli Avrupa Konseyi Siber Suçlar Sözleşmesi'ne paralel olarak düzenlenmiştir. Diğer taraftan metinde yer alan bazı suçlar siberle alakalı (*cyber related)* olarak düzenlemeye tabi tutulmuştur (UNODC, 2023a). Bu bölümdeki suçlara "çevrim içi çocuk cinsel istismarıyla veya istismara yönelik materyallerle ilgili suçlar" örnek olarak verilebilir. Taslak metnin bu kısmında düzenlenen bazı suçlar seçimlik hareketli suç kategorisindedir. Seçimlik hareketli suçlar yapısı gereğince birden fazla farklı fiille aynı suça meydan verebilmektedir. Öyle ki kanunda gösterilen farklı fiillerden birisi işlenerek oluşan suça içtima hükümleri uygulanmayarak sadece tek bir suç oluşturmaktadır (Alacakaptan, 1975, s. 47). Örneğin çocuğun istismarına yol

açacak fiiller bilişim sistemleri aracılığıyla işlenebileceği gibi fiziki olarak fiilen de işlenebilen suçlardandır. Öyle ki TCK'da çocuğun her türlü cinsel istismarı yasaklanmış olup söz konusu fiiller mevzuatımızın muhtelif maddeleri altında bilişim sistemleri aracılığıyla işlenip işlenmediğine bakılmaksızın düzenlenerek suç olarak kabul edilmiştir.

Taslak haldeki Sözleşme'nin ilk kısmında düzenlenen *cyber dependant* suçlar Avrupa Konseyi Siber Suçlar Sözleşmesi'nde mevcut olan suçlardır. Ancak bu metinde yer alan birçok *cyber enabled* suçunun Avrupa Konseyi Siber Suçlar Sözleşmesi'nde yer almadığı görülmektedir. Söz konusu kısımda düzenlenen maddelerde ifade edilen fiiller fiziki şekilde işlenebileceği üzere bilişim sistemleri vasıtasıyla da işlenebilmektedir (UNODC, 2023a). Bu kısımda düzenlenen suç tipleri bilgi ve iletişim teknolojisi kullanılarak işlenen suçlar konumunda bulunmaktadır. Tartışma konusunu oluşturan husus ise bu suç tiplerinin ayrıntılı hükümler içermeyen muğlak şekilde çerçevesi çizilmiş bir yapıda olmasıdır. Mezkûr suç tiplerinin belirsiz şekilde düzenlenmiş olmasından ötürü yerel mevzuatlara aktarılması aşamasında hangi suç tipleri açısından geçerli olacağı hususunda tartışmalar söz konusu olacaktır. Suç olarak taraf devletlerce kabul edilmesi öngörülen eylemlerin kapsamının, seçenek hareketlerinin ve bu hareketlere ait hukuki boyutların sınırlarını tespit etmek oldukça güçtür. Nitekim, mezkûr maddelerde tanımlanan eylemler bilişim sistemleri aracılığıyla gerçekleştirilebileceği gibi fiziki olarak da gerçekleştirilebilmektedir. Bu sebeple fiziki ve çevrim içi olarak işlenen suçlar noktasında ilgili suç tipi ayrımının yapılması konusunda da problemler ortaya çıkmaktadır.

Sözleşme'nin bağlayıcılığı konusunda bir kesinlik olmasa dahi uygulayıcı ülkelerin bu sözleşmeyi temel alarak iç mevzuatlarına Sözleşme hükümlerini aktarmaları öngörülmektedir. Bu kapsamda söz konusu Sözleşme'de *cyber related ve cyber enabled* suçların düzenleniyor olması yerel mevzuatların da bu yönde şekillenmesinde etkili olacaktır. Sınıflandırma yapıldığında bazı ülkeler siber suçların bilişim sistemleri vasıtasıyla işlenmesini temel alarak sınırlı bir kategorizasyon yapmasına rağmen, bazı ülkeler siberin araç şeklinde kullanılarak işlendiği çok daha geniş yelpazedeki suç türünü siber suçlar kapsamına almaktadır. Örneğin internet ortamında çocuğun cinsel istismarı suçu da bazı ülkelere göre *cyber related* olarak kabul edilip siber suçlar kapsamına alınmaktadır. Uluslararası sözleşmelerde tartışılan *cyber enabled* terimi siberle kolaylaşan suçları ifade etmektedir.

Birçok suç türü siber araçlar vasıtasıyla kolay bir şekilde işlenebilmektedir. Burada kastedilen normal şartlarda işlenmesinde zorluk bulunan veya suçun faillerinin yakalanmasının daha kolay olduğu belirli suç tiplerinin, siber araç olarak kullanılmak suretiyle rahatlıkla işlenebilmesidir. Siberin kolaylaştırdığı bu yolla failler kolluk kuvvetleri ve sorgulama mercilerinden rahatlıkla kaçarak söz konusu suçları işleyebilmektedir. Kendilerini gizleme konusunda başarılı olarak suçu işleme motivasyonlarını giderek artırmaktadırlar. Bahse konu ifadesel ayrımlara bakıldığında dünya üzerindeki siyasi kutuplaşmaların ülkelerin görüşlerini belirtmesinde etkili olduğu gözlemlenmektedir.

Sözleşme'nin oluşturulması aşamasında gerçekleştirilen toplantı oturumlarında siber suça ilişkin devletler arası ifade ayrımları dikkat çekmektedir (UNODC, 2022b). Öyle ki ABD ve AB ülkelerinin başını çektiği grup tarafından, Sözleşme'ye ilişkin ortak görüşlerinde kısa bir sözleşme metni olmasını istemelerinin yanı sıra evrensellik ve uygulanabilirlik açısından esnek bir yapının inşa edilmesi gerekliliğini belirtilmiştir. Sözleşme'nin ilk evrede *cyber dependent* suçlar ekseninde düzenlenmesinin faydalı olacağı fakat *cyber enabled* suçların daha sonraki evrelerde *cyber dependant* suçlara ilişkin işleniş biçimlerini önemli oranda etkilemesi veya sonuca tesir etmesi halinde sözleşmenin içeriğine eklenmesi şeklinde görüş bildirilmiştir. Sözleşme'nin ilk aşamasında yer verilmeyen suç tiplerinin UNTOC gibi sözleşmelerde olduğu gibi ek protokol şeklinde sonradan eklenebileceği ifade edilmiştir. *Cyber enabled* suç tiplerinin söz konusu sözleşmeye dahil edilmesine olumsuz bakılmasının bir sebebinin de ilgili suç tiplerinin kabulüne ilişkin görüşmelerin sözleşmenin kabul edilme süresini uzatacak olması olduğunu bildirmişlerdir (UNODC, 2021a ve 2022d).

Buna karşılık ABD ve AB üyesi ülkelerin karşıt görüşünde yer alan Rusya Federasyonu, İran, Çin Halk Cumhuriyeti ve Hindistan gibi ülkeler, BM Genel Kurulu'nun 74/247 sayılı kararı esas alınarak Sözleşme'nin *cyber enabled* suçları da kapsayacak şekilde hibrit formatta oluşturulmuş bir sözleşme olması gerektiğini ifade etmiştir. Bu kapsamda bilişim sistemleriyle işlenen suçların yanı sıra bilişim sistemleri tarafından kolaylaştırılan suçların da etkin şekilde tartışılması gerektiği vurgusu yapılmıştır. Bu görüş gerekçesinde *cyber dependant* olarak nitelendirilen suçların yanı sıra *cyber enabled* suçların bilgi ve iletişim teknolojileri vasıtasıyla işlenebildiği ve zarar verici nitelikte bir boyutta olduğu dile getirilmiştir (UNODC, 2021b)(UNODC, 2022e). Bu görüşün gerekçesini sunan İran tarafı, bilgi ve

iletişim teknolojileri vasıtasıyla meydana getirilen siber suçların Sözleşme kapsamında mücadeleye yönelik hareket alanının görülmesinde fayda sağlayacağını ve bu suçların verdiği zarar çemberinin daraltılabileceğini ifade etmiştir (UNODC, 2021a ve 2022d).

Sözleşmeye ilişkin toplantı oturumlarında terimlere ilişkin tartışma konularından bir tanesi *"computer systems* (bilgisayar sistemleri)*"* ve *"information and communication technology* (bilgi ve iletişim teknolojileri)*"* ayrımı noktasında olmuştur. Bu ifadesel ayrımda müşterek görüş birliği çerçevesinde Rusya Federasyonu, İran, Çin Halk Cumhuriyeti ve Hindistan'ın içerisinde bulunduğu grup Sözleşme'de *cyber dependant* kapsamında ele alınan "bilgisayar sistemleri" ifadesine karşılık *cyber enabled* kapsamında ele alınan "bilgi ve iletişim teknolojileri" ifadesinin kullanılmasını uygun görmüşlerdir. Burada amaç siber suçların daha geniş yoruma mahal verecek şekilde Sözleşme'ye dahil edilmesidir (UNODC, 2022f). Bahsi geçen ülkelerin söz konusu terimin kullanılmasında ısrarcı olmasının bir sebebi de sürekli olarak gelişen teknolojilere ayak uydurabilecek genel ve esnek ifadelerin gerekliliğidir. Öncül olarak siber suçları kapsamına alacak esnek bir ifade, teknolojik ilerlemeler doğrultusunda ileriye dönük farklı suç tipleri oluşsa dahi ulusal ve uluslararası mevzuatlarda tekrar bir düzenleme yapma külfeti oluşturmadan kolaylıkla uygulanma olanağı sunacaktır. Sözleşme'nin geniş yorumlanarak kapsamlı şekilde ele alınmasının söz konusu düzenlemenin her ne kadar ülkelerin birbirlerinin hakimiyetindeki suçlu konumunda bulunan kişileri talep edebilmesine olanak tanısa da devletlerin egemenlik bakımından eşitliği ilkesine aykırı uygulamalara mahal verilmemesi gerektiğine vurgu yapılmıştır. Bunun yanı sıra toprak bütünlüğü, siyasi bağımsızlık ve iç işlerine karışmama ilkelerine de saygı gösterilmesi gerektiği hususu ifade edilmiştir. Yine İSS'ler de dahil olmak üzere özel sektör yetkililerinin Sözleşme'nin ortaya çıkarılmasında önemli rol üstleneceği belirtilmiştir (UNODC, 2022b).

Sözleşme metninde geçen *"any criminal offence* (cezai siber suç)*"* ve *"serious crimes* (ciddi siber suç)*"* ifadelerinin arasında yapılan seçim ülkeler arasında tartışılan bir diğer konu olmuştur. Sözleşme toplantılarına katılan bazı ülkeler, bu ifadelerin ülkesel yorum farklılıkları sebebiyle uygulamada da sıkıntılılara yol açabileceğini ve yeknesak olmayan uygulamaların karşılıklı iş birliği konularında sıkıntı doğurabileceğini ifade etmiştir. Öyle ki bu ifadelerin yerine *"offenses set forth in this Convention* (sözleşmede belirtilen siber suçlar)*"* ifadesinin metne

işlenebileceği fikri diğer devletler nezdinde paylaşılmıştır. Özellikle ciddi siber suçların hangi suç tiplerini içereceği, hangi fiillerin ciddi suça mahal verecek yapıda olduğu üzerinde fikir birliği olmaması söz konusu seçenekler arasında kalınmasında önemli bir etken konumundadır. Sözleşme'nin temel olarak ciddi siber suçların tespiti, araştırılması ve soruşturulmasına yönelik olması gerektiği belirtilmiş ve insan haklarının adaletin merkezinde yer aldığı ifadeyle metinde insan haklarına saygı gösterilmesinin önemine değinilmiştir (UNODC, 2023d). Microsoft Corporation tarafından, Sözleşme metninde yer verilen terminolojinin kesin ve açık şekilde düzenlenmesi gerektiği ve "açık suç kastı" atfında bulunulabilen ciddi siber suçların metin kapsamında değerlendirilmesi gerektiği hususları ifade edilmiştir. Öyle ki söz konusu ciddi suç kategorisine girmediği halde bu kategoriye sokulabilecek sızma testi gibi test faaliyetlerinin yanlış anlaşılarak suç olarak nitelendirilebileceği tehlikesi gündeme getirilmiştir (Microsoft Corporation, 2022). United Kingdom International Chamber of Commerce (ICC) tarafından toplantının üçüncü oturumunda talep konusu edilen hususlar arasında Sözleşme hükümlerinin ciddi siber suçlara uygulanması da bulunmaktadır (ICC, 2022). Burada amaç kapsamın daraltılarak belirli ciddi suçlarla bir sınırlandırmaya gidilmesi olmuştur. Uygulamada netlik kazandırması ve ileride oluşabilecek hukuki ihtilafların önüne geçilmesi adına toplantı raporlarında Siber Barış Enstitüsü de bunun önemine vurgu yapmıştır (The CyberPeace Institute, 2023). Söz konusu Sözleşme'nin ön söz kısmında (UNGA, 2023) siber suçlara maruz kalan kişilerin korunmasının amaçlandığı, öncül ve ardıl tedbirlerin düzenleneceği, siber suçla etkin bir şekilde mücadelede bulunularak gerekli caydırıcılığın sağlanacağı, devletler arası teknik yardıma ilişkin araçların geliştirileceği, siber güvenliğe ilişkin kapasitelerin inşası ve güvenlik düzeyinin artırılması için gerekliliklerin sağlanacağı belirtilmiştir.

Aralarında ABD, Kanada, AB üyeleri, İsviçre ve Singapur'un olduğu ülkeler söz konusu Sözleşme bağlamında yer verilecek suçların dar yoruma tabi tutulması ve suç tanımlarının belirgin şekilde yapılması gerektiğini, bu suçların dışındaki suçların ise kısıtlı olarak metine aktarılabileceği görüşlerini belirtmişlerdir. Söz konusu suçlarla mücadelede Sözleşme görüşmeleri sırasında ikili bir ayrıma tabi tutulan siber suçlar için *"fight against the use of information and communications technologies for criminal purposes* (bilgi ve iletişim teknolojilerinin suç amaçlı kullanımıyla mücadele)*"* ve *"fight against cybercrime* (siber suçlarla mücadele)*"*

ifadelerinin kullanılması tartışma konusu olmuştur. Öyle ki bu ülkeler dar yorum kapsamında "siber suçlarla mücadele" ifadesinin kullanımının daha doğru olacağını değerlendirmişlerdir. Siber suçlarla mücadele ifadesi bilgi ve iletişim teknolojilerinin suç amaçlı kullanımı ifadesinin içerisinde barındırdığı suç tiplerini kapsamayan dar bir içeriğe sahiptir. Taslak Sözleşme metninde bu husus üzerinde iki farklı görüş etrafında kümeleşen ülkeler arasında tartışmalar yaşanmıştır. Karşı görüşte yer alan Rusya Federasyonu, İran, Çin, Mısır ve Hindistan'ın başını çektiği ülkeler Sözleşme'deki "bilgi ve iletişim teknolojilerinin suç amaçlı kullanımıyla mücadele" ifadesinin geniş yorum gerektiren bir ifade olduğunu belirterek metinde yer alması gerektiğini değerlendirmişlerdir. Bu ifadenin diğerine göre daha esnek bir yapıda olduğu, özellikle de bilgi ve iletişim teknolojilerinin gelişmesiyle ileride farklı suç tiplerinin de oluşabileceği ve bunların da söz konusu ifadenin içeriğinde kendisine yer bulabileceği ifade edilmiştir. Devletlerin toprak bütünlüğü, siyasi olarak özerklik ve iç işlerine karışılmama ilkelerine itaat edilmesi hususuna vurgu yapılmıştır. Bu kapsamda söz konusu ülkeler klasik siber suçların (bilgisayar ve sistemlerine yetkisiz girme, sistemlere yasa dışı müdahale ve siber saldırı türlerinin kullanımı, verilerin deformasyona uğratılması, içeriğinin değiştirilmesi veya silinmesi, teknolojik cihazların özellikle de bankacılık sistemlerinin kötücül amaçlarla kullanımı) yanı sıra siberin kolaylaştırdığı, internet ortamında işlenilmesiyle suçun sonucunun hızlandığı, niteliksel olarak farklı bir yöne evrildiği ve etki düzeyinin de farklılaştığı; çocukların cinsel istismarı, siber zorbalık, dolandırıcılık, fikri mülkiyete ilişkin suçlar gibi *cyber enabled* kategorisinde olan suç tiplerinin de Sözleşme'de düzenlenmesi gerektiği hususunda görüş bildirmişlerdir (UNODC, 2022b).

SONUÇ VE DEĞERLENDİRME

Siber suça ilişkin yapılan tanımlara bakıldığında sadece sibere bağımlı olan klasik suçların Sözleşme metninde olması, değişen ve gelişen teknolojilerle işlenebilen siber suç tiplerini dışarıda bırakmaktadır. Halbuki siberin kolaylaştırdığı (*cyber enabled*) ve siberle alakalı (*cyber related*) suç tipleri birçok farklı suç türünü de kapsamına alarak geniş çerçeveden bu suçlara ilişkin soruşturma, kovuşturma ve cezai yaptırım imkânı sunmaktadır. Bu kapsamda değerlendirme yapıldığında siberin kolaylaştırdığı ve siberle alakalı suçların da Sözleşme'de yer alması isabetli olacaktır. Geniş yorum vasıtasıyla siberle alakalı suçlar kapsama alınarak söz konusu terimlere ilişkin fikir birliği oluşturulmalıdır. Her ne kadar devletlerin çekince koydukları hususlara dair iç hukukta uygulanabilirlik hususunda sıkıntılar yaşanabilecek olsa da ayrıntılı şekilde hazırlanacak hükümler herhangi bir belirsizliğe yol açmadan iç hukuka aktarılabilecektir. Bununla birlikte Sözleşme görüşmeleri sırasında tartışılan "bilgi ve iletişim teknolojileri" terimi de metne dahil edilmesi gereken ifadelerdendir. Öyle ki siber suçların 2000'li yılların başında sadece bilgisayar sistemleri ile işlendiği teknoloji, yerini geniş çapta cihazlarla işlenebilen ve ağ üzerinden yıkıcı etki bırakabilen siber saldırı teknolojisine bırakmıştır. Diğer taraftan, hangi suçların Sözleşme kapsamı dahilinde değerlendirileceğine ilişkin devletler arasında yaşanan ihtilaflara bakıldığında siber suçlarla ilgili tespit faaliyetlerinin yürütülmesi ve adli makamlar tarafından soruşturma ve kovuşturma yapılabilmesi olanağının bu hususta belirleyici olduğu görülecektir. Öyle ki ciddi siber suçların soruşturma ve kovuşturmaya tabi tutulması konusunda devletler arasında anlaşmazlıklar yaşanabilecektir. Burada önemli olan mesele ise ciddi siber suçun kapsamı ve devletlerin hangi kıstaslara göre bir suçu ciddi siber suç sayacak olmasıdır. Devletlerin yerleşik hukuk kuralları ve mevzuatları kapsamında yazılı olarak suç atfedilmeyen fiiller ile toplum nezdinde suça sebebiyet vermeyecek fiillerin ciddi olarak nitelendirilmesinde amaç ve kapsam problemi yaşanacağı ortadadır. Bu sebeple siber suçların "ciddi" ifadesi yerine "Sözleşme'de belirtilen suçlar" ifadesiyle tamamlanabileceği değerlendirilebilir. Öyle ki metinde düzenlenmeyen suç tiplerinin kapsama dahil edilmesi devletler açısından uygulamada farklılıkların oluşmasına yol açarak belirsizliklerin doğmasına sebebiyet verecektir.

Son zamanlarda internet ortamında çocukların siber zorbalığa maruz kalması, sanal ortamda cinsel tacize uğramaları, dolandırıcılık, sahtecilik ve hırsızlıkla

ilgili siber suçların artışı siberin araç olarak kullanıldığı suçlar için açık bir düzenlemeye ihtiyaç duyulduğunu göstermektedir. Bu sebeple söz konusu Sözleşme bu konuda uluslararası alandaki hukuk boşluğunu doldurabilecek konumdadır. Siberle alakalı suçlarla ilgili düzenlemeler bu suçların gerçekleştirilmesine yönelik davranışları kısıtlayıcı bir etki yaratacaktır. Söz konusu düzenleme ile suçun faillerine yönelik caydırıcılık hususu gündeme gelecektir. Aynı zamanda suçluların soruşturulması, kovuşturulması ve iadesine ilişkin hususlarda siber suça müşterek bir yaklaşım sağlanarak uygulamada devletler arası yaşanabilecek ihtilafların önüne geçilmesi sağlanacaktır. Sınır tanımayan siber saldırıların ve siber suçluların tespitinde devletler arası hukuki ve teknik yardımlaşma geliştirilerek 7/24 bilgi ve veri akışı ağı sağlanabilecektir. Ortak bir siber suç yaklaşımı sonrasında siber uzayda birden çok devletin yargı yetkisine giren olayların çözüme kavuşturulmasını sağlayacak uluslararası adalet mekanizmaları ve mahkemelerin de oluşturulması gerekli olacaktır. Bu kapsamda bağlayıcı konumda olan uluslararası siber uzay mahkemeleri ve ara buluculuk merkezlerinin hayata geçirilmesi büyük önem arz etmektedir. Yine, ortaya çıkan hukuk boşlukları doldurularak siber suçluların kendilerini mahkeme önünde avukat marifetiyle savunabileceği sistemler de doğal olarak oluşacaktır.

KISALTMALAR

BM	Birleşmiş Milletler
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CMK	Ceza Muhakemesi Kanunu
EC3	European Cybercrime Centre
EHK	Elektronik Haberleşme Kanunu
EİK	Elektronik İmza Kanunu
ENISA	European Unıon Agency For Cybersecurity
ICC	United Kingdom International Chamber of Commerce
ICCP	Committee on Information, Communications and Computer Policy
ICT	Information and Communication Technologies
ITU	International Telecommunication Union
J-CAT	Joint Cybercrime Action Taskforce
NIST	National Institute of Standards and Technology
OECD	The Organisation For Economic Cooperation and Development
SPF	Singapur Polis Gücü
TCK	Türk Ceza Kanunu
UNGA	United Nations General Assembly
UNODC	United Nations Office on Drugs and Crime

KAYNAKÇA

AAG IT Services. (2023). The Latest 2023 Cyber Crime Statistics. https://aag-it.com/the-latest-cyber-crime-statistics/ adresinden 22 Eylül 2023 tarihinde erişildi.

Akpek, N. O. (2015). Siber Suçlar Sözleşmesinin Getirdikleri ve İç Hukuk Açısından Konuya Yaklaşım [Yüksek Lisans tezi, İstanbul Bilgi Üniversitesi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=GswZ7stjY2LTwxeBF7XsrQ&no=uR2ojMmxzbc0TS5hxDlpAQ adresinden 6 Haziran 2023 tarihinde erişildi.

Alacakaptan, U. (2022). Suçun Unsurları. Ankara Üniversitesi Hukuk Fakültesi Yayınları.

Aldoori, A. (2020). Uluslararası Hukukta Siber Suçla Mücadele. [Yüksek Lisans tezi, İstanbul Üniversitesi]. http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET002065.pdf adresinden 13 Haziran 2023 tarihinde erişildi.

Andress, J. ve Winterfeld, S. (2013). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners (2.Baskı). Syngress Press.

Bilgi Teknolojileri ve İletişim Kurumu Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı. (2022). Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri. https://www.btk.gov.tr/uploads/pages/arastirma-raporlari/dijitallesen-dunyada-bilisim-suclari-ve-mucadele-yontemleri-6218e2417eaea.pdf adresinden 12 Haziran 2023 tarihinde erişildi.

Brenner, S. W. (2010). Cybercrime: Criminal Threats From Cyberspace, School Of Law Faculty Publications, 115. https://ecommons.udayton.edu/law_fac_pub/115 adresinden 2 Haziran 2023 tarihinde erişildi.

Ceza Muhakemesi Kanunu. Kanun Numarası: 5271. sayılı Kabul Tarihi: 04.12.2004. RG 17.12.2004/25673.

Committee on Information, Communications and Computer Policy. (2010). OECD ICCP Committee. https://www.oecd.org/digital/ieconomy/37328586.pdf adresinden 14 Temmuz 2023 tarihinde erişildi.

Council Of Europe. (2001). Convention On Cybercrime. https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf adresinden 15 Ha-

ziran 2023 tarihinde erişildi.

Council of Europe. (2023). Council of Europe action against Cybercrime. https://www.coe.int/en/web/portal/coe-action-against-cybercrime adresinden 10 Ağustos 2023 tarihinde erişildi.

Çolak, H. (2016). Siber Terörizmin Önlenmesinde Kurumsal Yapılanma ve Uluslararası Adli Yardımlaşma. Türk Hukuk Araştırmaları Dergisi, 1(1), 4.

Elektronik Haberleşme Kanunu. Kanun Numarası: 5809. sayılı Kabul Tarihi: 05.11.2008. RG 10.11.2008/27050.

Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği. Bilgi Teknolojileri ve İletişim Kurumu. https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=19880&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5

Elektronik İmza Kanunu. Kanun Numarası: 5070. sayılı Kabul Tarihi: 15.01.2004. RG 23.01.2004/25355

Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı. (2023). SiberAy Sözlüğü. https://www.siberay.com/kurumlar/Siberay.com/SIBERAY-Sozluk.pdf adresinden 9 Haziran 2023 tarihinde erişildi.

Eur-Lex. (2023). Accesss To European Unıon Law. https://eur-lex.europa.eu/search.html?scope=EURLEX&text=d%C4%B1rective&lang=en&type=quick&qid=1694697439782 adresinden 10 Ağustos 2023 tarihinde erişildi.

Euromed Justice Program. (2023). The G7 24/7 Cybercrime Network. https://euromedjustice.eu/wp-content/uploads/2021/05/G7_Network.pdf adresinden 10 Ağustos 2023 tarihinde erişildi.

European Unıon Agency For Cybersecurity (ENISA). (2023). EU CyCLONE. https://www.enisa.europa.eu/topics/incident-response/cyclone adresinden 10 Temmuz 2023 tarihinde erişildi.

European Commission. (2022). New EU Cybersecurity Strategy And New Rules To Make Physical And Digital Critical Entities More Resilient. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 adresinden 14 Temmuz 2023 tarihinde erişildi.

European Commission. (2023a). Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). https://digital-strategy.ec.europa.eu/en/policies/nis2-directive adresinden 8 Ağustos 2023 tarihinde erişildi.

European Commission. (2023b). Cyber Resillience Act. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act adresinden 8 Ağustos 2023 tarihinde erişildi.

European Commission. (2023c). The EU Cybersecurity Act. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act adresinden 8 Ağustos 2023 tarihinde erişildi.

European Commission. (2023d). The EU Cyber Solidarity Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity adresinden 6 Ağustos 2023 tarihinde erişildi.

Europol. (2023a). European Cybercrime Centre – EC3. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 adresinden 8 Ağustos 2023 tarihinde erişildi.

Europol. (2023b). Joint Cybercrime Action Taskforce (J-CAT). https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce adresinden 9 Ağustos 2023 tarihinde erişildi.

Europol. (2023c). European Union CYBERCRIME TASK FORCE (EUCTF). https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf adresinden 10 Ağustos 2023 tarihinde erişildi.

Fikir ve Sanat Eserleri Kanunu. Kanun Numarası: 5846. sayılı Kabul Tarihi: 05.12.1951. RG 13.12.1951/7981.

Gordon, S. ve Ford, R. (2006). On the Definition and Classification of Cybercrime. Journal in Computer Virology, 2, 13-20. https://doi.org/10.1007/s11416-006-0015-z adresinden 4 Haziran 2023 tarihinde erişildi.

Holt, T. J. ve Bossler, A. M. (2020). The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan Press.

International Telecommunication Union. (2007). Global Security Agenda (GCA). https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx adresinden

17 Temmuz 2023 tarihinde erişildi.

International Telecommunication Union. (2009). Understanding Cybercrime: A Guide For Development Countries. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf adresinden 14 Haziran 2023 tarihinde erişildi.

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. Kanun Numarası: 5651. Sayılı Kabul Tarihi: 04.05.2007. RG 23.05.2007/26530.

INTERPOL. (2017). Global Cybercrime Strategy. https://www.interpol.int/content/download/5586/file/Summary_CYBER_Strategy_2017_01_EN%20LR.pdf?inLanguage=eng-GB adresinden 5 Ağustos 2023 tarihinde erişildi.

Lasky, J. (2022). Cyberspace. Salem Press Encyclopedia of Science. https://public.stacksdiscovery.com/eds/detail?db=ers&an=93787497 adresinden 13 Haziran 2023 tarihinde erişildi.

Lin, L. S. F. ve Masys, A. J. (Ed.). (2018). Asia-Pacific Security Challenges Managing Black Swans and Persistent Threats (1.Baskı). Springer Press. DOI: 10.1007/978-3-319-61728-2

Malisevic, N. (2022). Microsoft's Presentation at the Panel Titled: A Concerted Effort. [Poster Sunumu]. Third intersessional consultation of the Ad Hoc Committee on Cybercrime, Amerika Birleşik Devletleri, New york https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_intersessional_consultation/Presentations/Panel_4_Microsoft.pdf adresinden 10 Temmuz 2023 tarihinde erişildi.

National Institute of Standards and Technology. (2023). NIST Glossary. https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary#C adresinden 10 Ağustos 2023 tarihinde erişildi.

OECD. (2008). Policy Guidance on Online Identity Theft. https://www.oecd.org/sti/consumer/40879136.pdf adresinden 12 Temmuz 2023 tarihinde erişildi.

Singapore Police Force. (2023). Siber Suçun Sınıflandırılması ve Tanımı. https://www.police.gov.sg/Advisories/Crime/Cybercrime#:~:text=In%20Singapore%2C%20cybercrime%20is%20categorised,%2C%20website%20defacement-

s%2C%20ransomware%20etc adresinden 22 Ağustos 2023 tarihinde erişildi.

Smith, R. G., Grabosky, P., ve Urbas, G. (2004). Cyber Criminal on Trial. Cambridge University Press. https://www.researchgate.net/publication/233023456_Cyber_Criminals_on_Trial adresinden 2 Haziran 2023 tarihinde erişildi.

Suçluların İadesine Dair Avrupa Sözleşmesine Ek İkinci Protokol. https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020132606098_tur.pdf adresinden 10 Ağustos 2023 tarihinde erişildi.

The Crown Prosecution Service. (2022). Cybercrime Definition. https://www.cps.gov.uk/crime-info/cyber-online-crime#:~:text=drugs%20and%20firearms.-,Cybercrime,or%20simply%20to%20disrupt%20businesses adresinden 12 Haziran 2023 tarihinde erişildi.

The CyberPeace Institute. (2023). Submission to the Fifth Session. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/Multi-stakeholders/CYBERP1.PDF adresinden 24 Temmuz 2023 tarihinde erişildi.

Thomas, D. ve Loader, B. (Ed.). (2000). Cybercrime: Law Enforcement, Security and Surveillance in the Information Age (1. Baskı). Routledge Press.

Türk Ceza Kanunu. Kanun Numarası: 5237. Kabul Tarihi: 26.09.2004. RG 12.10.2004/25611.

Türk Dil Kurumu. (2023). Türk Dil Kurumu Sözlüğü. https://sozluk.gov.tr/ adresinden 2 Eylül 2023 tarihinde erişildi.

Ulaştırma ve Altyapı Bakanlığı. (2020). 2020-2023 Ulusal Siber Güvenlik Strateji ve Eylem Planı. https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf dresinden 24 Temmuz 2023 tarihinde erişildi.

United Kingdom International Chamber Of Commercee. (2022). Submission To The Third Sessions. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/ICC_UK_1.pdf adresinden 21 Temmuz 2023 tarihinde erişildi.

United Nations General Assembly. (2019). General Assembly Resolution 74/247. https://documnts-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/

N1944028.pdf?OpenElement eadresinden 4 Haziran 2023 tarihinde erişildi.

United Nations General Assembly. (2021). General Assembly Resolution 75/282. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement adresinden 4 Haziran 2023 tarihinde erişildi.

United Nations General Assembly. (2022). General Assembly Resolution 76/552. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/GA_decision_76-552.pdf adresinden 12 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2021a). Organizational session of the Ad Hoc Committee. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/Organizational_session adresinden 3 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2021b). The Draft Prepared By The Russian Federation Regarding The Contract. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf adresinden 3 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2022a). Road map and mode of work for the Ad Hoc Committee". https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Website/AHC_Road_map.pdf adresinden 6 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2022b). Compilation of draft provisions submitted by Member State. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/CRP11.pdf adresinden 2 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2022c). Comments and proposals of the Islamic Republic of Iran. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Islamic_Republic_of_Iran_contribution.pdf adresinden 10 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2022d). Report of First Session of the Ad Hoc Committee of the United States of America. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/USA_National_Statement_-_Cybercrime_AHC.pdf adresinden 10 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2022e). Contribution from The Russian Federation. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Russia_Contribution_E.pdf adresinden 16 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2022f). Compilation of proposals and contributions submitted by Member States. https://documents-dds-ny.un.org/doc/UNDOC/GEN/V22/023/23/PDF/V2202323.pdf?OpenElement adresinden 5 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2023a). Draft Text Of The Convention. https://documents-dds-ny.un.org/doc/UNDOC/GEN/V23/039/51/PDF/V2303951.pdf?OpenElement adresinden 4 Eylül 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2023b). Fifth session of the Ad Hoc Committee. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main adresinden 4 Haziran 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2023c). Draft Text Of The Convention. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session-docs/A_AC_291_22_Advance_Copy.pdf adresinden 3 Eylül 2023 tarihinde erişildi.

United Nations Office on Drugs and Crime. (2023d). Consolidated Negotiating Document On The General Provisions. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/CND_21.01.2023_-_Copy.pdf adresinden 11 Ağustos 2023 tarihinde erişildi.

US Department Justice Office. (2023). Office Of Justice Programs. https://www.ojp.gov/ adresinden 10 Ağustos 2023 tarihinde erişildi.

Usta, A. C. ve Benzer R. (2018). Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 4(2), 35-42. DOI:10.18640/ubgmd.512829.

KİTAP İNCELEMESİ
ALİ BURAK DARICILI, "SİBER UZAY VE SİBER GÜVENLİK: ABD VE RUSYA FEDERASYONU'NUN SİBER GÜVENLİK STRATEJİLERİNİN KARŞILAŞTIRMALI ANALİZİ", 2017, 320 SAYFA, DORA YAYINCILIK: BURSA

Arş.Gör.Erva KARADAĞ[1]

Yaklaşık on beş yıl boyunca Millî İstihbarat Teşkilatı çatısı altında çeşitli yurt içi ve yurtdışı görevler üstlenen, şu an Bursa Teknik Üniversitesi'nde görev yapan Doç. Dr. Ali Burak Darıcılı, 2017 yılında Uludağ Üniversitesi'nde hazırladığı doktora tezini, aynı yıl *"Siber Uzay ve Siber Güvenlik: ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi"* başlığıyla kitaplaştırarak akademi dışı okuyucunun da ilgisine sunmuştur. Darıcılı, siber uzay ve siber güvenlik çalışmalarının bilgi/bilişim teknolojilerinin sınırları içerisinde kalan salt "teknik" bir alan olduğuna yönelik dar kapsamlı değerlendirmelerden farklılaşarak, bu alanda meydana gelen değişim, dönüşüm ve gelişmelerin birey-kurum-devlet-uluslararası sistem olmak üzere farklı analiz düzeyinin güvenliğine yönelik dikkat çekici etkisine vurgu yapmaktadır. Bu bağlamda çalışma, geleneksel savaş ve çatışma alanlarının yanı sıra siber uzayda da birbirleriyle rekabet halinde olan ve çatışan, siber uzayın başat aktörleri olan Rusya ve Amerika Birleşik Devletleri'nin siber güvenlik stratejilerini neo-realist perspektiften mercek altına almaktadır.

Dört bölümden oluşan çalışmanın "Reel Politik Paradigmanın Uluslararası İlişkiler Disiplininde Kurumsallaştırılması" başlığını taşıyan ilk bölümünde, çalışmanın kavramsal ve teorik altyapısı inşa edilmiştir. Uluslarası İlişkiler'in başat teorilerinden klasik realizm ve neo-realizmin disiplin içerisindeki yeri, temelleri

[1] Arş.Gör.Erva KARADAĞ, Milli Savunma Üniversitesi, Alparslan Savunma Bilimleri ve Milli Güvenlik Enstitüsü, Güvenlik Araştırmaları Anabilim Dalı, ekaradag@kho.msu.edu.tr, ORCID: 0000-0001-5901-9572

ve savları, bu teorilerin güvenlik kavramına bakışları değerlendirilmiş, siber uzay ve siber güvenliğin kavramsal çerçevesi çizildikten sonra, Joseph Nye'nin güç tipolojisi ve güç difüzyonu yaklaşımları bağlamında ele alınmıştır., Bu bölümde ortaya konan argüman, siber uzayda yaşanan gelişmelere paralel olarak tehditlerin çeşitlendiği ve belirsizleştiği; bu durumun uluslararası sistemi hiç olmadığı kadar anarşik, güvensiz bir hale dönüştürdüğü ve siber uzayın getirdikleriyle devletlerin bu alanda da tehditleri bertaraf etmeye muktedir başat aktörler olarak rol ve sorumluluklarının pekiştiğidir.

"Amerika Birleşik Devletleri'nin Siber Güvenlik Stratejisinin Analizi" başlıklı ikinci bölümde bu stratejinin inşasında önemli rol oynayan başta ABD Savunma Bakanlığı, ABD İç Güvenlik Bakanlığı ve ABD istihbarat topluluğunda yer alan Federal Araştırma Bürosu (FBI) ile Merkezi Haber Alma Örgütü (CIA) olmak üzere ilgili kurum/kuruluşlar, federal ve eyalet seviyesinde hazırlanan başta yasalar olmak üzere çeşitli yasal düzenlemelerden müteşekkil hukuki altyapı ve stratejiyi ortaya koyan başkanlık emirleri, direktifler, resmi belge, doktrin ve planlar detaylı bir biçimde ele alınmıştır. Ek olarak Edward Snowden vakası, Wikileaks sızıntısı ve 2016 ABD Başkanlık Seçimlerini etkilemeye yönelik Rusya Federasyonunca düzenlendiği iddia edilen siber faaliyetler gibi örnekler incelenmiştir.

"Rusya Federasyonu'nun Siber Güvenlik Stratejisinin Analizi" başlıklı üçüncü bölümde, bir önceki bölüm ile paralel olarak Rusya Federasyonu'nun siber güvenlik konseptinin kavranabilmesi açısından Rus siber alanının temel özellikleri, başta Rus Askeri İstihbarat Direktörlüğü (GRU), Rus İstihbarat Servisi (SVR) ve Rus Federal Güvenlik Servisi (FSB) gibi istihbarat kuruluşları başta olmak üzere ilgili kurum/kuruluşların siber kapasitesi, çeşitli güvenlik doktrinleri, prensip ve konseptler, stratejik güvenlik belgeleri ile resmi dokümanlar detaylı bir incelemeye tabi tutulmuştur. İç politikada ortaya konan yol gösterici mahiyetteki bu belgelerin yanı sıra Rusya Federasyonu'nun siber güvenlik temelli işbirliği hedefleri kapsamında attığı adımlar, Birleşmiş Milletler'den Şangay İşbirliği Örgütü'ne kadar çeşitli uluslararası ortamda yürütülen diplomasi faaliyetleri ve başta Çin Halk Cumhuriyeti ile olmak üzere diğer devletlerle ortaya konan girişimler değerlendirilmiştir. Ayrıca Rus istihbarat servislerince gerçekleştiği iddia edilen çeşitli ülkeler, şirketler ve kritik altyapıların hedef alındığı siber saldırı ve espiyonaj vakalarının yanı sıra da yakın mercek altına alınmıştır. Bu bölümün temel argümanı, Rusya Federasyonu'nun siber uzayda hukuki, bürokratik ve teknolojik ge-

lişmelere paralel olarak sahip olduğu siber kapasite ve gücü alaka ve menfaatleri çerçevesinde, legal veya illegal yollar aracılığıyla, enformasyon savaşı ile destekli bir baskı ve zorlama aracı olarak kullandığıdır.

"Amerika Birleşik Devletleri'nin ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırılması" başlıklı dördüncü ve son bölüm ile, Soğuk Savaş'tan günümüze kadar Amerika Birleşik Devletleri'nin ve Rusya Federasyonu'nun siber alandaki rekabeti gerek pratik, gerek kurumsal, gerekse bağlamsal olarak ortaya konulmuştur. Pratik boyutta çalışma, Sputnik II'den ARPA-ARPANET-MILNET ağ projesine, Rus Askeri İşlerde Devrim (RMA) projesinden Amerikan Yıldız Savaşları Projesi'ne ve Soğuk Savaş'ın sona ermesinin ardından yürütülen siber saldırılar, siber operasyonlar ve enformasyon savaşına değin iki ülke arasındaki rekabet karşılaştırmalı olarak ele alınmıştır. Bağlamsal boyutta çalışma, Amerika Birleşik Devletleri'nin ve Rusya Federasyonu'nun siber alandaki rekabetinin resmi doküman, strateji ve doktrinlerin içerik analizini ortaya koymaktadır. Söz konusu analiz neticesinde her iki ülkenin siber uzay ve siber güvenlik stratejilerinin benzeşen, farklılaşan, çatışan ve uyuşan tarafları değerlendirilmiştir. Kurumsal boyutta ise Amerika Birleşik Devletleri'nin başta ABD Savunma Bakanlığı, ABD İç Güvenlik Bakanlığı ve ABD istihbarat topluluğunda yer alan Federal Araştırma Bürosu (FBI) ile Merkezi Haber Alma Örgütü (CIA) ve Rusya Federasyonu'nun Rus Askeri İstihbarat Direktörlüğü (GRU), Rus İstihbarat Servisi (SVR) ve Rus Federal Güvenlik Servisi (FSB) gibi siber güvenlik organizasyon yapıları karşılaştırmalı olarak mercek altına alınmıştır.

Sonuç olarak, siber uzay ve siber güvenlik düzlemlerini uluslararası güvenlik ve dış politika ekseninde inceleyen; bu alanları Rusya Federasyonu ve Amerika Birleşik Devletleri vakaları üzerinden ele alan bu çalışma, uluslararası ilişkiler ve bilgi/bilişim teknolojileri perspektiflerini bir araya getiren interdisipliner yönüyle dikkat çekmektedir. Bu yönü ile çalışmanın teknik bilimlerden sosyal bilimlere, akademik çevrelerden popüler/akademi dışı çevrelere, geniş bir okuyucu kitlesine hitap etmesine olanak sağladığı değerlendirilmektedir.

KAYNAK:

DARICILI A. B. (2017). Siber Uzay ve Siber Güvenlik: ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi. Dora Yayıncılık, Bursa


BİLGİ
TEKNOLOJİLERİ
VE İLETİŞİM
KURUMU