

T.C.
GAZİANTEP ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
GÜVENLİK STRATEJİLERİ VE YÖNETİMİ ANA BİLİM DALI

**SOSYAL MEDYANIN DEVLET VE KAMU
GÜVENLİĞİNE ETKİSİNİN İRDELENMESİ**

YÜKSEK LİSANS TEZİ

MÜCAHİT ÇAVUŞ

Tez Danışmanı: Prof. Dr. Yakup BULUT

GAZİANTEP, Nisan 2026

T.C.
GAZİANTEP ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
GÜVENLİK STRATEJİLERİ VE YÖNETİMİ ANA BİLİM DALI

Tezin Başlığı: Sosyal Medyanın Devlet ve Kamu Güvenliği Açısından İrdelenmesi

Adı ve Soyadı: Mücahit ÇAVUŞ

Tez Savunma Tarihi: 15/04/2026

Prof. Dr. Yakup Bulut danışmanlığında hazırlanan bu tez tarafımızca okunmuş, kapsam ve niteliği açısından oybirliği ile bir Yüksek Lisans tezi olarak kabul edilmiştir.

Jüri Üyeleri:

Prof. Dr. Yakup BULUT

Prof. Dr. Ali Fuat GÖKÇE

Prof. Dr. Burhanettin COŞKUN

İmzası

Bu tezin gerekli şartları sağlayarak yukarıda belirtilen jüri tarafından Yüksek Lisans tezi olarak kabul edildiğini onaylarım.

Prof. Dr. Ali Fuat GÖKÇE
Enstitü ABD Başkanı

Sosyal Bilimler Enstitüsü Onayı

Doç. Dr. Ahmet BOZDAĞ
SBE Müdürü

ETİK İLKELERE UYGUNLUK BEYANI

Gaziantep Üniversitesi Sosyal Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

İmza:

Adı ve Soyadı: Mücahit ÇAVUŞ

Öğrenci Numarası:22017111022

Tezin Savunma Tarihi: 15/04/2026

ÖZET

SOSYAL MEDYANIN DEVLET VE KAMU GÜVENLİĞİ AÇISINDAN İRDELENMESİ

ÇAVUŞ, Mücahit

Yüksek Lisans Tezi

Güvenlik Stratejileri ve Yönetimi Ana Bilim Dalı

Tez Danışmanı : Prof. Dr. Yakup BULUT

Nisan-2026, 131 sayfa

Sosyal medya, düşük maliyetle geniş kitlelere ulaşma imkânı sunması nedeniyle suç örgütleri, terör örgütleri ve istihbarat birimleri tarafından yoğun biçimde kullanılmaktadır. Suç örgütleri sosyal medyayı suç faaliyetlerinde araç olarak kullanırken terör örgütleri propaganda, eleman devşirme, finansman ve çevrimiçi eğitim faaliyetlerini bu platformlar üzerinden yürütmektedir. İstihbarat birimleri açık kaynak istihbaratı elde etmek amacıyla sosyal medya verilerinden yararlanmakta; devlet ve örgütler dezenformasyon yoluyla hedef ülkelerde kamu düzenini bozma ve devlet otoritesine olan güveni zayıflatma girişiminde bulunmaktadır. Bu çalışma, sosyal medyanın devlet ve kamu güvenliği üzerindeki etkilerini analiz etmeyi ve güvenlik politikaları açısından doğurduğu riskleri ortaya koymayı amaçlamaktadır. Araştırmada nitel yöntem kullanılmış; tehdit, şantaj, nitelikli dolandırıcılık ve halkı kin ile nefrete teşvik suçları ele alınmıştır. Gezi Olayları, Arap Baharı, Londra İsyanları, Myanmar, Kayseri Göçmen Olayı, 6 Ocak Kongre Baskını, Ukrayna-Rusya Savaşı ile PKK, DEAŞ ve FETÖ'nün sosyal medya operasyonları örnek olaylar olarak incelenmiştir. Sosyal medyanın hiyerarşik olmayan yapısı öngörülemez riskler oluşturmakta; dezenformasyon ve dijital propaganda kamu düzeni ile devlet güvenliği üzerinde olumsuz etkiler doğurmaktadır. Çalışma, sosyal medyanın güvenlik politikası açısından yeniden değerlendirilmesi ve dijital güvenliğin sağlanması için çözüm önerileri sunmaktadır.

Anahtar Kelimeler: Sosyal Medya, Güvenlik, Dezenformasyon, Sosyal Medya İstihbaratı (SOCMINT)

ABSTRACT

AN EXAMINATION OF SOCIAL MEDIA IN TERMS OF STATE AND PUBLIC SECURITY

ÇAVUŞ, Mücahit

Master's Thesis

Department of Security Strategies and Management

Thesis Advisor: Prof. Dr. Yakup BULUT

Nisan-2026, 131 pages

Social media, owing to its capacity to reach large audiences at low cost, is extensively utilized by criminal organizations, terrorist groups, and intelligence agencies. While criminal organizations employ social media as an instrument for illicit activities, terrorist groups conduct propaganda, recruitment, financing, and online training operations through these platforms. Intelligence agencies leverage social media data to obtain open-source intelligence, whereas state and non-state actors engage in disinformation campaigns aimed at disrupting public order and undermining trust in state authority in target countries. This study aims to analyze the effects of social media on state and public security and to identify the risks it poses from a security policy perspective. A qualitative research method was employed; criminal offenses including threat, blackmail, aggravated fraud, and incitement to hatred and hostility were examined. The Gezi Park Events, the Arab Spring, the London Riots, the Myanmar Crisis, the Kayseri Migrant Incident, the January 6th Capitol Breach, the Russia-Ukraine War, and the social media operations of terrorist organizations PKK, DAESH, and FETÖ were analyzed as case studies. the non-hierarchical structure of social media generates unpredictable risks, while disinformation and digital propaganda produce adverse effects on public order and state security. The study proposes that social media be reassessed from a security policy standpoint and offers recommendations for ensuring digital security.

Keywords: Social Media, Security, Disinformation, Social Media Intelligence (SOCMINT)

ÖN SÖZ

Bu çalışma sosyal medya ve hızlı gelişene iletişim teknolojisi ve kanallarının özellikle devlet ve kamu güvenliği açısından ne gibi riskleri içinde barındırdığını, buna ilişkin çözüm ve yaklaşımların ne olması gerektiğine vurgu yapmayı amaçlamıştır. Devletin varlık sebebini ve vatandaş açısından önemi dikkate alındığında kamu güvenliği ve devlet güvenliği açısından risk olacak hemen her konunun farklı şekillerde ele alınması gerektiği ortaya çıkmaktadır. İşte bu çalışmada genel bir adı taşıyan sosyal medya olmakla beraber içeriğinde siber güvenlik, algıya, devlet güvenliğinden kamu güvenliğine birçok konu dikkate alınarak bunların ne gibi riskler taşıdığı , hangi çözümlerin geliştirilmesi gerektiği konusunda analiz ve önerileri ortaya koymayı amaçlamaktadır. Bu tez çalışması sürecinde ve yürütülmesinde önemli katkı sağlayan danışmanım Prof. Dr. Yakup BULUT'a, fikir ve katkılarıyla destek olan bölüm hocalarıma ve aileme teşekkür ederim.

Mücahit ÇAVUŞ

İÇİNDEKİLER

ÖZET.....	i
ABSTRACT.....	ii
ÖN SÖZ	iii
TABLolar LİSTESİ	vii
ŞEKİLLER LİSTESİ	ix
KISALTMALAR	xi

GİRİŞ

I. BÖLÜM

KAVRAMSAL ÇERÇEVE, TARİHSEL SÜREÇ

1.1. Sosyal Medya Kavramı ve Genel Özellikleri.....	6
1.1.1.Yeni Medya ve Sosyal Ağ Siteleri Kavramı	6
1.1.2. Sosyal Medyanın Tanımı ve Temel Özellikleri	9
1.1.3. Sosyal Medyayı Etkileyen Faktörler ve Sosyal Medyanın Etkileri	12
1.2. Sosyal Medyanın Tarihsel Gelişimi	16

1.2.1. Web Teknolojileri (Web 1.0, 2.0, 3.0, 4.0) ve Sosyal Medya İlişkisi	16
1.2.2. Dünyada ve Türkiye’de Sosyal Medyanın Tarihsel Süreci	20
1.2.3. Türkiye ve Dünyada Güncel Kullanım Oranları	22
1.3.Sosyal Medya Araçları	25
1.3.1. Bloglar Ve Mikrobloglar.....	25
1.3.2. Sosyal Ağlar	27
1.3.3. Anlık Mesajlaşma Uygulamaları	28
1.3.4 Sosyal İşaretleme(İmleme) Ağları.....	29
1.4. Güvenliğin Sosyal Medya İle İlişkisi.....	30
1.4.1. Devlet Güvenliğinin Tanımlanması ve Kapsamı.....	30
1.4.2. Kamu Güvenliğinin Tanımlanması ve Kapsamı.....	31
1.4.3. Siber Uzak ve Siber Güvenlik Kapsamında Sosyal Medya	32
1.4.4. Sosyal Medya-Devlet Güvenliği Etkileşimi.....	33
1.4.5. Sosyal Medya-Kamu Güvenliği Etkileşimi.....	34

II. BÖLÜM

SOSYAL MEDYANIN DEVLET VE KAMU GÜVENLİĞİNE ETKİSİ: TEHDİTLER VE YASAL DÜZENLEMELER

2.1. Kamu Güvenliği Açısından Sosyal Medyada İşlenen Suçlar.....	37
2.1.1. Nitelikli Dolandırıcılık ve Veri Güvenliği.....	38
2.1.2. Tehdit ve Şantaj Suçları	40
2.1.3. Halkı Kin ve Nefrete Teşvik Etme	41
2.1.4. Veri İhlalleri: Cambridge Analytica Örneği	43
2.2. Sosyal Medyada Algı Yönetimi ve Sebepleri	44
2.2.1. Dezenformasyon Faaliyetleri	49
2.2.2. Toplumsal Hareketler ve İstihbarat	54
2.3. Devlet Güvenliği Açısından Terör ve Radikalleşme	56
2.3.1. Terör Örgütü Propagandası ve Dijital Stratejiler.....	57

2.3.2. Radikalleşme Sürecinde Sosyal Medyanın Rolü.....	60
2.3.3. Deaş Terör Örgütünün Sosyal Medya ve Dijital Alan Kullanımı.....	61
2.4. Sosyal Medya İstihbaratı(Socmınt).....	67
2.4.1. Dijital Ayak İzi ve Profesyonel Ağların Rolü.....	69
2.4.2. "Honeypot" (Bal Tuzağı) ve Sahte Profil Operasyonları	71
2.5. Hibrit Savaş ve Stratejik İletişim	72
2.5.1. Psikolojik Savaş ve Etki Operasyonları	75
2.5.2. Siber Operasyonlar ve Zararlı Yazılım Yayıılımı (Malware)	77
2.5.3. Terör Örgütleri(PKK/DEAŞ/FETÖ) ve Devletlerin Dezenformasyon Faaliyetleri.....	78
2.6. Sosyal Medya İle İlgili Yasal Düzenlemeler: Ülke Örnekleri.....	80
2.6.1. Almanya ve AB: Dijital Hizmet Yasası	80
2.6.2. Çin ve Rusya Uygulamaları	82
2.6.3. Türkiye'deki Mevcut Yasal Düzenlemeler ve Sosyal Medya Yasası	83

III. BÖLÜM

SOSYAL MEDYANIN DEVLET VE KAMU GÜVENLİĞİNE ETKİSİ: UYGULAMA VE VAKA ANALİZLERİ

3.1.Siyasi İstikrar ve Rejim Güvenliği Odaklı Vakalar.....	87
3.1.1.Arap Baharı Bağlamında Sosyal Medyanın Etkisi: Dijital Aktivizm.....	89
3.1.2. 6 Ocak ABD Kongre Baskını: Sosyal Medyada Radikalleşmenin Fiziksel Şiddete Dönüşümü	89
3.2. Kamu Düzeni ve Toplumsal Barış Odaklı Vakalar	91
3.2.1. Myanmar Vaka Analizi: Etnik Çatışmalar.....	92
3.2.2. Covid-19 Pandemisi ve İnfodemi: Kamu Sağlığı Güvenliğine Yönelik Dijital Tehditler.....	94
3.2.3. İngiltere (2011) Londra İsyanları ve Yağma.....	95

3.3. Siber Güvenlik, İstihbarat ve Hibrit Savaş Odaklı vakalar	97
3.3.1. Stuxnet ve Sonrası: Nükleer Tesislere Yönelik Keşif Aşamasında Sosyal Medyanın Rolü	98
3.3.2. Ukrayna- Rusya Savaşı: Sosyal Medya Cephesi (Dijital Savaş)	100
3.4. Türkiye Özelinde Sosyal Medya ve Güvenlik Vakaları	101
3.4.1. Gezi Parkı Olayları: Kitle Hareketlerinde Sosyal Medyanın Dönüştürücü Rolü	102
3.4.2. Kayseri Göçmen Olayları (2024): Dezenformasyonun Toplumsal Şiddeti Tetiklemesi	103
3.4.3. Terör Örgütlerinin (PKK/FETÖ/DEAŞ) Güncel Sosyal Medya Operasyonları	105

SONUÇLAR VE ÖNERİLER

4.1. Sonuçlar	108
4.2. Öneriler	111

KAYNAKLAR.....	114
-----------------------	------------

ÖZGEÇMİŞ.....	131
----------------------	------------

TABLÖLAR LİSTESİ

Tablo 1. Web1.0-Web2.0-Web 3.0- Web4.0 Özelliklerinin Karşılaştırılması	19
Tablo 2. Web'in Tarihsel Gelişimi	19
Tablo 3. En çok kullanılan blog siteleri	27

ŞEKİLLER LİSTESİ

Şekil 1. Başlıca sosyal ağların açılış tarihleri ve sosyal ağ özellikleriyle yeniden piyasaya sürülen platformlar	8
Şekil 2. Sosyal Medya İşlevselliği	10
Şekil 3. İşlevselliğin Gerekleri.....	11
Şekil 4. Web1.0'ın Özelliği.....	17
Şekil 5. Web 3.0 Özellikleri	18
Şekil 6. Aktif kullanıcı sayılarına göre en çok kullanılan sosyal medya platformları.....	23
Şekil 7. Sosyal Medya Kullanımına Genel Bakış	24
Şekil 8. Bir blog sayfasının görünümü	26
Şekil 9. Örnek Sosyal Ağ Görünümü: Facebook	27
Şekil 10. Örnek Sosyal İşaretleme(imleme) Ağı: Pinterest	29
Şekil 11. Bilgi Kirliliğinin Türleri	50
Şekil 12. Temmuz Şehitler ve Fatih Sultan Mehmet köprüleri satışa çıkarılıyor” başlıklı paylaşım, CNBC-e Resmî X Hesabı	53
Şekil 13. T.C. İletişim Başkanlığı Dezenformasyonla Mücadele Merkezi (DMM) paylaşım	53
Şekil 14. Deaş destekçilerinin oluşturduğu tweet sayısının zaman içindeki dağılımı.....	62
Şekil 15. Deaş destekçi hesaplarının günlük askıya alınma sayılarının zaman çizelgesi.....	63

Şekil 16. Deaş terör örgütü'nün militan toplamak amacıyla kurduğu birçok X hesaplarından bir tanesi.....	63
Şekil 17. Deaş terör örgütü'nün militan toplamak için kurmuş olduğu Facebook hesaplarından bir tanesi.....	64
Şekil 18. İngiliz gazeteci James Foleyn'in kafasının kesildiği videonun Youtube platformu'nda haber olması	65



KISALTMALAR

AB	: Avrupa Birliđi
ABD	: Amerika Birleşik Devletleri
AKİS	: Açık Kaynak İstihbaratı
DEAŞ	: Irak ve Şam İslam Devleti
DSÖ:	: Dünya Sağlık Örgütü
DSA:	: Dijital Hizmetler Yasası
FETÖ:	: Fethullahçı Terör Örgütü
MİT:	: Millî İstihbarat Teşkilatı
NETZDG:	: Almanya Sosyal Ağ Kanunu
NATO:	: Kuzey Atlantik Antlaşması Örgütü
OSINT:	: Açık Kaynak İstihbaratı
PKK:	: Kürdistan İşçi Partisi
PLC:	: Programlanabilir Mantık Denetleyicisi
SCADA:	: Denetleyici ve Veri Toplama Sistemi

SOCMINT	: Sosyal Medya İstihbaratı
STRATCOM	: Stratejik İletişim
T.C.	: Türkiye Cumhuriyeti
TCK	: Türk Ceza Kanunu
TSK	: Türk Silahlı Kuvvetleri
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
YÖK	: Yükseköğretim Kurulu



GİRİŞ

İnternet teknolojilerinin Web 1.0'dan Web 2.0'a evrilmesi, bilginin tek taraflı akışını kırarak kullanıcıyı içeriğin merkezine konumlandırmıştır. Web 1.0 sürecinde insanlar bilginin alımlayıcısı durumunda pasif konumda bulunurken Web 2.0 sürecinde kullanıcılar içerik üreticisi konumuna dönüşerek aktif konuma geçmişlerdir (Latorre, 2018/2021). Kullanıcılar artık içerik üretilen mevcut içeriklere katkı sunabilmektedir.

Bu yeni teknoloji zamanla geliştirilmiş, insanlar tarafından yüksek rağbet görmüştür. Zira günümüzde sosyal medya olarak adlandırılan mecralar, 5 milyar kullanıcıya sahiptir. Dünya nüfusunun yüzde 60'ı bu platformları kullanmaktadır. İnternete bağlı olan insanların yüzde 90'ı sosyal medya platformlarını kullanmaktadır. Bu mecralarda kullanıcılar ortalama olarak 2 saat 21 dakika vakit geçirmektedir (Statista, 2025). Günlük hayatta yoğun kullanılması ve dünya çapında kullanıcısının yüksek sayıda olması, sosyal medyanın olumlu kullanımının yanı sıra olumsuz kullanımını da beraberinde getirmektedir. Birtakım olumsuz etkiler ise devlet ve kamu güvenliğini dolaylı veya doğrudan tehdit etmek suretiyle etkilemektedir. Bu doğrultuda çalışmanın konusu; Web 2.0 teknolojisiyle insanların hayatına giren sosyal medyanın birtakım tekniklerle ve yöntemlerle devletin ve kamu güvenliğinin tehdit edilmesi için stratejik bir araç olarak kullanılmasıdır.

Bu noktada araştırmanın problemleri; sosyal medyada işlenen siber suçların ve dezenformasyonun devlet ve kamu güvenliğine etki etmesidir.

Araştırmanın bir diğer problemi; Terör örgütlerinin propaganda faaliyetlerini gerçekleştirdikleri, eleman devşirdikleri, eyleme yönlendirdikleri ve para kazandıkları mecralar haline dönüşmesidir (Ferrara, 2017). Güvenlik güçleri ve diğer güvenlik birimlerinde çalışan kamu personellerinin askeri üniformayla bulundukları üslerden

sosyal medya mecralarında fotoğraf ve video paylaşarak stratejik bilgilerin ifşa olmasına yol açmasıdır (Bural, 2024).

Araştırmanın bir diğer problemi veri güvenliği ve veri egemenliği sorunudur. Nitekim sosyal medya üzerinde kullanıcılarını belirten ve kendini ifade etme biçimi olan profillerde; kullanıcıların adı soyadı, okul bilgisi, gezdikleri konumlar, beğenileri, yorumları gibi dijital ayak izleri bulunmaktadır. Bu ayak izleri sayesinde kişinin kişisel bilgileri, hangi konumları ne sıklıkla kullandığı, günlük rutinleri, tercihleri, duygu durumları, yorumlarıyla siyasi görüşünden eğlence anlayışına kadar birçok veri bu mecralarda bulunmaktadır (Polat ve Öcal, 2020). Bu bilgilerin platform tarafından reklam ve pazarlama adı altında işlediği verileri hangi amaçla kullanacağını bilinmemesi, veri güvenliği açısından risk teşkil etmektedir.

Bir diğer sorun ise sosyal medya ortamlarının siber saldırılar ve diğer yöntemlerle dijital casusluk faaliyetlerinin alanı haline gelmesidir. Özellikle veri sızıntıları, kötü amaçlı yazılımlar, phishing gibi kandırma saldırıları ve sosyal mühendislik yöntemleri, kişisel veri güvenliğini doğrudan tehdit eden başlıca unsurlardır (Çetin, 2014, s. 5).

Araştırmanın bir diğer problemi süreçte sosyal medyanın çok önemli bir araç haline gelmesidir. Hibrit savaşta sosyal medya aracılığıyla sağlanmak istenen amaç, dezenformasyonla ve diğer yöntemlerle düşmanı fiziksel olarak mağlup etmek değil; savaşma iradesini zayıflatmak, iç cephesinin tahkim edilmesini engellemek ve psikolojik olarak yıkmaktır. Bu amaç doğrultusunda hibrit savaş modelinde, sosyal medyada dezenformasyon ve kara propaganda ile toplumda güvensizlik hissi oluşturarak devlete olan güvenin kırılması istenmektedir. Kitle hareketlerine yol açmak, toplumda kaos ortamı oluşturmak amacını gerçekleştirmek için sosyal medya en iyi araçlardan biridir (Gerasimov, 2016).

Bu çalışma, sosyal medyanın devlet ve kamu güvenliğini tehdit edecek çok boyutlu etkilerini analiz etmek amacıyla aşağıdaki sorulara yanıt aramaktadır:

1. Terör örgütleri tarafından sosyal medya nasıl kullanılmaktadır?
2. Sosyal medya mecraları, nasıl hibrit savaş modeline uygun bir araca dönüşmektedir?
3. Sosyal medyada istihbarat noktasında ne tür dijital istihbarat faaliyetleri devlet ve kamu güvenliğine risk teşkil etmektedir?

4. Devlet ve kamu güvenliği açısından sosyal medyada depolanan veriler, veri güvenliği açısından nasıl bir tehdit içermektedir?

5. Modern devletler, sosyal medya aracılığıyla devlet ve kamu güvenliğine yönelik oluşan asimetrik tehditlere karşı ne tür yasal düzenlemeler ve tedbirler geliştirmelidir?

Yukarıda sıralanan araştırma sorularına verilecek yanıtlar doğrultusunda; bu çalışmanın temel amacı sosyal medyanın yalnızca eğlence, öğrenme, sanal iletişim gibi temel ihtiyaçları karşılayan mecralar olmasının yanında modern güvenlik anlayışı içerisinde devlet ve kamu güvenliğini tehdit eden stratejik bir araç olduğunu ortaya koymaktır. Çalışma, bu amaçlar doğrultusunda şu hedefleri gerçekleştirmeye odaklanmaktadır:

- Terör örgütlerinin sosyal medyayı kullanma taktiklerini DEAŞ terör örgütü örneği üzerinden inceleyerek deşifre etmek,
- Sosyal medyanın hibrit savaş türünün içindeki yerini tespit etmek, dezenformasyon ve toplumsal hareketleri bu doğrultuda analiz etmek,
- Sosyal medya üzerinden sağlanan istihbaratın devlet ve kamu güvenliği üzerindeki etkisini örnek olay analizleriyle tanımlamak ve güvenlik zafiyetlerini ortaya koymak,
- Sosyal medya platformlarında biriken verilerin veri güvenliği açısından içerdiği tehditleri olay örneği ile incelemek,
- Elde edilen bulgular ışığında devlet ve kamu güvenliğine karşı oluşan tehditlere yönelik devletlerin alması gereken yasal düzenlemeler ve stratejiler için çözüm önerileri sunmak.
- Bu çalışma; sosyal medyanın devlet ve kamu güvenliğine etkisini sosyal, siyasal, ekonomik ve hukuksal boyutlarıyla inceleyerek, istihbari boyutunu da ele alan bütüncül bir güvenlik anlayışıyla bu sorunu ele alması bakımından önem taşımaktadır. Çalışmanın önemini belirleyen unsurlar; literatür taraması sonucunda yeni medya, sosyal medya ve sosyal ağ kavramlarını kategorize etmesi; kamu personellerinin dijital ayak izleriyle güvenlik zafiyeti oluşturacağı vurgulanarak sosyal medya kullanım rehberleri ve kurum içi eğitimlerle kurumsal farkındalığın geliştirilmesine katkı sunması; konuya bütüncül bakış açısıyla bakılarak sosyal

medyanın sosyal, hukuki, ekonomik ve idari alandaki etkilerinin ele alınması; hibrit savaş kavramının önemli bir aracı olduğunun vurgulanarak literatüre katkı sağlanması; modern devletin özgürlük-güvenlik dengesi içerisinde ne tür yasal tedbirler ve önlemler alması gerektiği yönünde somut öneriler sunmasıdır.

Çalışmanın iddialarını bilimsel bir temele oturtmak ve araştırmanın belirtilen hedeflerine ulaşması için bu çalışma nitel araştırma yöntemini benimsemiştir. Çalışmada literatür taraması ve doküman analizi kullanılmıştır. Konuyla ilgili ulusal ve uluslararası yayınlar, güncel istatistikler, resmi raporlar, vaka analizleri, dergi ve kitaplar incelenmiştir. Araştırma, Web 2.0 süreciyle ortaya çıkan sosyal medyanın devlet ve kamu güvenliğine yönelik asimetrik tehditlerine odaklanmaktadır. Elde edilen veriler betimsel yaklaşımla ele alınmış, sosyal medyanın özellikleri ile güvenlik zafiyetleri arasında neden-sonuç ilişkisi kurulmuştur.

Bu çalışma üç ana bölümden oluşmaktadır. Birinci bölümde, "Sosyal Medyanın Kavramsal Çerçevesi ve Tarihsel Süreci" ele alınmaktadır. Bu aşamada; yeni medya, sosyal ağ ve sosyal medya kavramları açıklanarak sosyal medyanın geleneksel medyadan ayrılan yönleri ve büyük veri kavramıyla ilişkisi incelenmektedir. Ayrıca, Web 1.0'dan 4.0'a uzanan teknolojik dönüşümün toplumsal etkileri ile sosyal medyanın Türkiye'de ve dünyada geçirdiği evrim ve güncel kullanım istatistikleri bütüncül bir perspektifte değerlendirilmektedir.

İkinci bölümde, "Sosyal Medyanın Devlet ve Kamu Güvenliğine Etkisi: Tehditler ve Yasal Düzenlemeler" başlığı altında, dijital mecraların ortaya çıkardığı asimetrik riskler analiz edilmektedir. Sosyal medyada işlenen adli suçlar, terör örgütlerinin radikalleşme ve propaganda stratejileri, dezenformasyon kampanyaları ve hibrit savaş unsurları gibi konular geniş bir çerçevede ele alınmaktadır. Bölüm sonunda, bu tehditler karşısında geliştirilen yasal düzenlemeler, Almanya, Çin ve Rusya gibi ülke örnekleri üzerinden incelenmekte; Türkiye'deki mevcut hukuki çerçeveye karşılaştırmalı bir değerlendirme sunulmaktadır.

Üçüncü bölümde ise, "Uygulama ve Vaka Analizleri" üzerinden teorik yaklaşımların pratik sonuçları gözler önüne serilmektedir. Arap Baharı, Ocak ABD Kongre Baskını, Ukrayna-Rusya Savaşı'nın dijital boyutu ve Türkiye'de son dönemde yaşanan güncel dezenformasyon örnekleri (Kayseri olayları, çevrimiçi sorgu panelleri) derinlemesine analiz edilmektedir. Bu vakalar; siyasi istikrar, kamu düzeni, siber

güvenlik ve ekonomik güvenlik alt başlıkları altında sınıflandırılarak sosyal medyanın kriz anlarındaki dönüştürücü etkisi irdelenmektedir.

Sonuç ve Öneriler kısmında ise, çalışmanın tüm bulguları üzerinden değerlendirme yapılmaktadır. Devlet ve Kamu Güvenliğini Sosyal Medya platformları üzerinden gelecek tehditlere karşı daha etkin bir şekilde korunmasına yönelik stratejik çözüm önerileri sunulmaktadır.



I. BÖLÜM

KAVRAMSAL ÇERÇEVE, TARİHSEL SÜREÇ

1.1. Sosyal Medya Kavramı ve Genel Özellikleri

Sosyal medya kavramının teorik zeminini oturtmak ve bu mecrayı benzer kavramlardan ayırt edebilmek amacıyla bu bölümde; öncelikle "yeni medya" ve "sosyal ağ" terimleri açıklanacak ardından sosyal medyanın literatürdeki tanımları ve bu platformları işlevsel kılan temel özellikleri üzerinde durulmuştur. Sosyal medyanın doğasını daha net kavrayabilmek, tek yönlü iletişimden çift yönlü etkileşime geçişi anlamak için "geleneksel medya" ile olan yapısal farklılıkları analiz edilmiştir. Sosyal Medyanın özelliklerinden bahsedilmiştir. Anlık mesajlaşma uygulamaları, telefon numaralarının gizliliği, profillerin birbirlerine olan bağlantısallığının olmaması, keşfet ve durum gibi özelliklerinin henüz geliştirilme aşamasında olması nedeniyle sosyal medyanın bağlantısallık ve açıklık özelliklerini henüz tam manasıyla kapsamadığı için bu çalışma kapsamı dışında bırakılmıştır.

1.1.1.Yeni Medya ve Sosyal Ağ Siteleri Kavramı

Geleneksel medya araçları; “Gazeteler, dergiler, radyolar ve televizyonlar, bunların hepsi de tekil ürün ya da programların kitle halindeki kullanıcılara dağıtıldığı birden-çoğa (one-to-many) biçiminde çalışan iletişim ortamlarıdır.” (Çakır, 2007, s. 125). “Gazete, radyo, televizyon gibi kitle iletişim araçları; şimdilerde geleneksel (traditional), anaakım (mainstream) veya eski (old) medya olarak tanımlanmaktadır. Bilgisayarlara (bilgi-işlem) ve iletişim araçlarına (haberleşme-telekomünikasyon ve

yayıncılık) özgü yapılar yöndeşerek yeni (new) medyayı ortaya çıkarmıştır.” (Törenli, 2005, s. 87 Akt: Nuran, 2015, s. 9). Bu şekilde klasik kitle iletişim araçları eski medya olarak adlandırılırken gelişen iletişim teknolojisiyle internet tabanlı, hipermetinsel, etkileşimli dijital iletişim ortamları ise yeni medya olarak adlandırılmaktadır (Lister vd., 2009, s. 13-14)

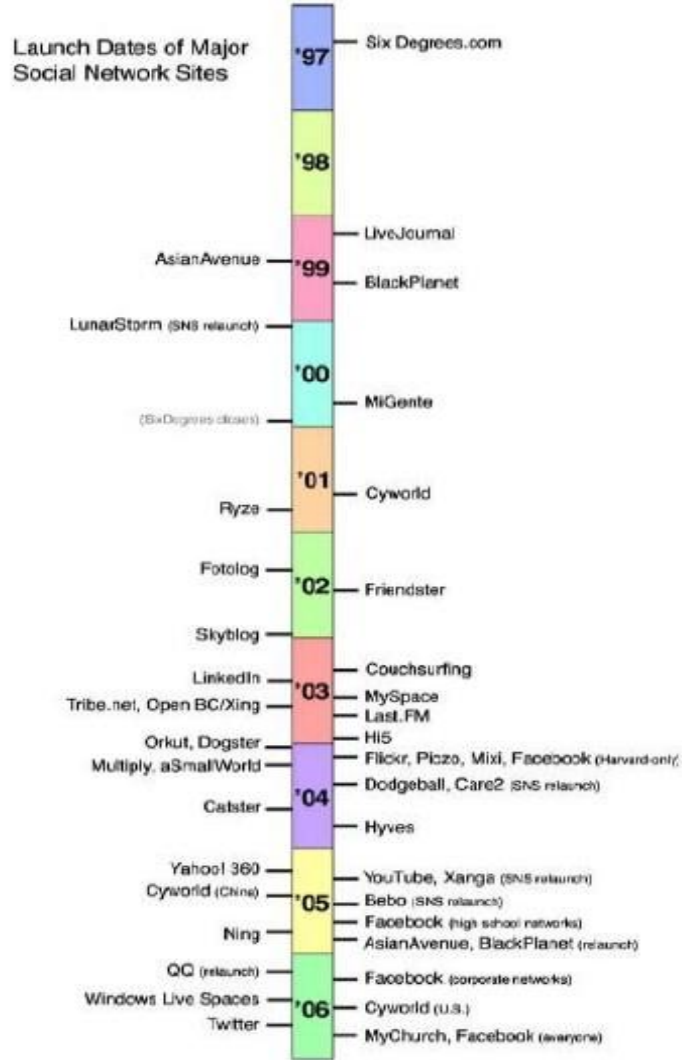
Yeni Medyanın türleri olarak e-uygulamalar, internet tabanlı platformlar, arama motorları, sosyal ağlar gibi platformlar sayılabilir (Bulunmaz, 2014, s.28). Yeni Medya; Dijital kodlamaya dayanan, iletişimin tek taraflı değil, tüm aktörler arasında eş zamanlı, karşılıklı bir etkileşim ve multimedya biçimselliğine sahip bir ekosistemi temsil etmektedir (Van Dijk, 2006, s.7-9). Yeni medya; geleneksel kültürel formların bilgisayar kodlarıyla birleşmesiyle ortaya çıkan dijital bir nesnedir (Manovich2003 s.13).

Mutimedya biçemlerinin farklı olması ve etkileşimdeki farklılıklar eski ile yeni medya arasındaki farklılığın temel farklarıdır (Binark, 2007, s.21). Binark ve Bayraktutan (2013, s. 19)’a göre yeni medyayı geleneksel medyadan ayıran temel özellikler; Kullanıcı tarafından içerik üretilebilmesi, etkileşimsellik, multimedya biçimselliği, sanallık, yayılım, dijitallik olarak belirtilebilir.

Sosyal Medya kavramını açıklamadan önce sosyal ağ kavramına değinmek gerekmektedir. Literatür taramasında sosyal ağ kavramı, farklı disiplinler tarafından farklı boyutlarıyla tanımlanan çok boyutlu bir olgudur (Boyd ve Ellison, 2007, s.211). sosyal ağ sitelerini çevrim içi profiller ve görünür bağlantılar üzerinden ele almış, kullanıcıların kişisel bilgilerinin yer aldığı profil oluşturduğu, arkadaş listesi oluşturdukları, diğer kullanıcıların profillerini, durumlarını, paylaşımlarını ve ilişkilerini takip edebildikleri web tabanlı hizmetler olarak tanımlamıştır. Sosyal Medya ve Sosyal Ağlar arasında aynı özellikleri taşımalarından dolayı kavramlar arasında karışıklık görünse de aslında sosyal ağların daha çok ilişki ve sosyal yapı odaklı, sosyal medya ise içerik ve stratejik iletişim odaklı yapısıyla aradaki ayrım anlaşılmaktadır (Zhao, 2021, s.512).

Tanımlamalardan anlaşıldığı üzere sosyal ağ sitelerinin odak noktası mevcut çevrimdışı bağların çevrimiçi ortamda görünür kılınması ve bağlantıların görünürlüğü (Boyd ve Ellison, 2007, s.211) sosyal medyada ise içerik üretimi, paylaşımı ve etkileşim ön plandadır. Sosyal ağ siteleri, sosyal medyanın alt türlerinden biri olarak değerlendirilmektedir. Bu bağlamda sosyal ağ siteleri daha çok ilişki kurma

ve bağlantıları görüntüleme amacına hizmet ederken sosyal medya farklı türlerde içeriklerin üretilmesi ve paylaşılmasını amaçlamaktadır.



Şekil 1. Başlıca sosyal ağların açılış tarihleri ve sosyal ağ özellikleriyle yeniden piyasaya sürülen platformlar (Boyd ve Ellison, 2007 s.212).

Bu zaman çizelgesi, 1997 yılında SixDegrees.com ile başlayan sosyal ağ sitelerinin gelişim sürecini göstermektedir. 1997–2001 arasında (SixDegrees, AsianAvenue, LiveJournal, BlackPlanet, MiGente gibi) ilk örnekler ortaya çıkmış fakat bu siteler görece sınırlı kullanıcı kitlelerine hitap etmiştir. Friendster, LinkedIn, MySpace, Hi5, Orkut gibi web siteleri 2002–2004 yılları arasında sosyal ağ sitelerini küresel sahnedeki-popülerlik kazanmıştır. Özel olarak 2003–2004, sosyal ağ sitelerin

oldukça çok yönlü hale geldiği ve farklı hedef kitlelere hitap eden (profesyonellere dönük LinkedIn, gençlere dönük MySpace, yerel ağlara dönük Orkut gibi) platformların ivme kazandığı yıllardır. 2005–2006 yıllarında sosyal ağ sitelerinin kritik kırılma noktasıdır. Buna göre Facebook, önce Harvard öğrencileriyle sınırlı bir ağ iken 2004-2005'te lise ağlarına, 2006'da ise geniş kitlelere açılarak kısa zamanda küresel ölçekte en güçlü aktör olmuştur. Aynı tarihte YouTube gibi içerik paylaşım odaklı platformlar da sosyal ağ özellikleri kazanmaya başlamıştır. Bu çizelge aynı zamanda bazı platformların zamanla kendini yenileyerek yeniden açıldığını göstermektedir. Bu göstergeler sosyal medya ortamının sürekli stratejik yeniden yapılanma ve kullanıcı talepleri doğrultusunda uyum sağlama potansiyelini işaret etmektedir. Tümü genel olarak tablo sosyal ağ sitelerinin ilk evresinin (1997–2001) deneysel, İkinci evresinin (2002–2004) yaygınlaşma, Üçüncü evresinin (2005 sonrası) ise küreselleşme ve kurumsallaşma süreci olduğunu göstermektedir. (Boyd ve Ellison, 2007, ss.212-219)

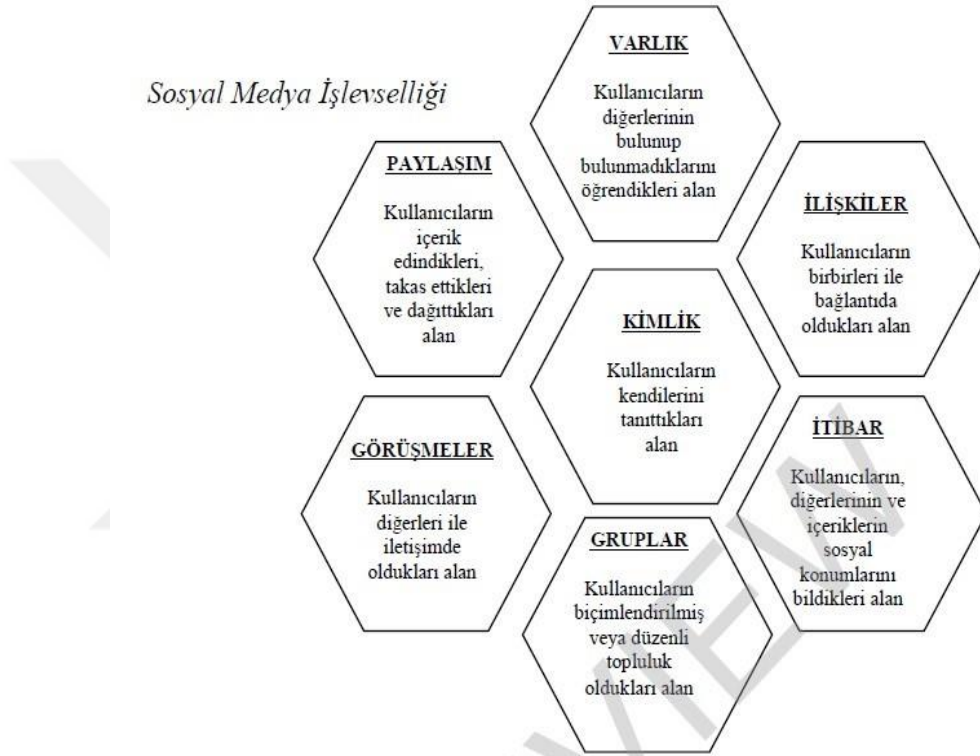
1.1.2. Sosyal Medyanın Tanımı ve Temel Özellikleri

Türk Dil Kurumu'na göre medya ; ‘‘iletişim ortamı, iletişim araçları’’ olarak tanımlanmaktadır. Sosyal medya kavramı ise disiplinler arası bir olgudur. Sosyal medya kavramı literatürde farklı disiplinler tarafından çeşitli yönleriyle ele alınmıştır. Sosyal medya Web 2.0 teknolojileriyle geliştirilmiş, kullanıcıların kendine ait içerikleri üretip paylaşımlarına imkân tanıyan internet tabanlı uygulamalardır (Kaplan ve Haenlein,2010, s.61). Başka bir tanıma göre sosyal medya; internet kullanıcılarının çevrimiçi ortamda etkileşimde bulunmalarına imkân tanıyan, paylaşım ve kişisel yorum gibi aktiviteler üzerine kurulu sosyal ağ platformları olarak ifade edilmektedir (Güzel, 2020, s.94). Sosyal Medya bir başka tanıma göre ‘‘sanal iletişim ortamı’’ olarak görülmektedir (Çalışkan ve Mencik, 2015 s.255). Literatür taramasında bazı çalışmalarda sosyal ağ, yeni medya ve sosyal medya kavramlarının aynı anlamda kullanıldığı görülmektedir.

Sosyal ağlar ilişki odaklı yapıdadır. Sosyal Medya ise içerik ve stratejik iletişim temelli çok yönlü etkileşim sunan yapıya sahiptir (Zhao, 2021, s.554).

Sosyal Medyayı diğer iletişim araçlarından ayıran temel nitelikler; kullanıcıların içerik üretimine katılımı, geri bildirimine açıklık, karşılıklı etkileşime dayalı iletişim, toplulukların ortak ilgi alanları etrafında örgütlenebilmesi ve farklı ağlar arasında bağlantı kurulabilmesidir (Mayfield, 2008, s.5). Bu özellikler sayesinde

sosyal medya, geleneksel medyanın tek yönlü yapısından farklı olarak kullanıcı merkezli ve etkileşimli bir ortam sunmaktadır. Sosyal medya platformlarının nasıl işlediğini, kullanıcıların deneyimlerini de açıklayacak biçimde ortaya koyan ‘’sosyal medya petek modeli’’ olarak bilinen kavramsal çerçeve ortaya konulmuştur. Bu bileşenler; kimlik, varlık, paylaşım, sohbet, gruplar, itibar ve ilişkiler olarak belirlenmiştir (Kietzmann vd.,2011, s.243).

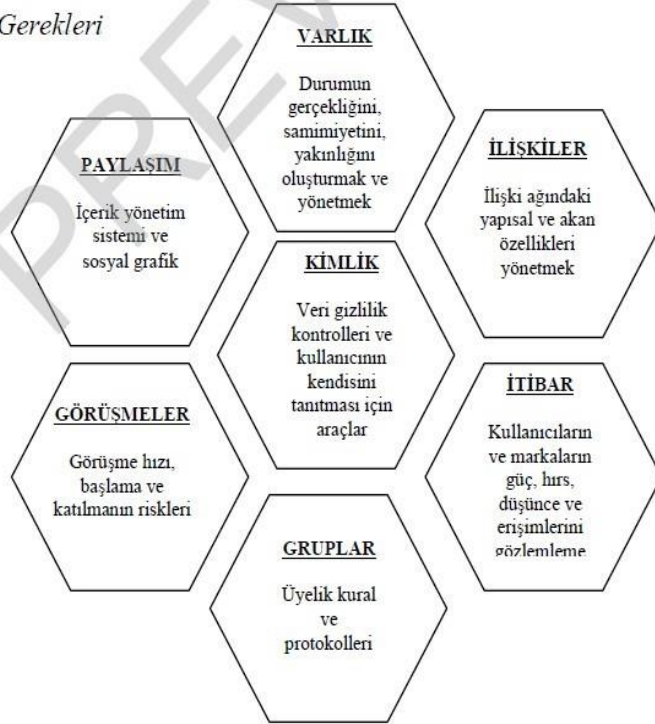


Şekil 2. Sosyal Medya İşlevselliği (Kietzmann vd., 2011, s. 243).

Modelin ilk bileşeni olan kimlik, kullanıcıların kendini ifade edişini ifade etmektedir. Oluşturdukları kişisel profil hesaplarında yer alan kişisel bilgiler; ad, cinsiyet, yaş, hobiler gibi kısımlarda yer alan bilgileri ifade etmektedir. Kimlik noktasında kullanıcıların sunmuş olduğu bilgiler, kendi gerçek bilgileri olabildiği gibi kendini diğer kullanıcılara idealize ettiği şekliyle de ortaya koyabilmektedir. Bu anlamda hem kimlik inşasında ve kendini ifade etme biçimi noktasında önemlidir. İkinci unsur olan varlık (presence), bir kullanıcının çevrimiçi ortamda kendini ne ölçüde orada olduğu, diğer kullanıcılar tarafından görünürlüğünün olup olmadığı ile ilgilidir (Kietzmann vd., 2011, s. 243-245). Örnek olarak Instagram uygulamasındaki

anlık aktif veya pasif durumunu ifade eden göstergeler varlık unsurunun göstergeleridir.

İşlevselliğin Gereklere



Şekil 3. İşlevselliğin Gereklere (Kietzmann vd., 2011, s. 243).

Üçüncü unsur olan paylaşım (sharing), sosyal Medya'nın en temel işlevlerinden biridir. Kullanıcıların içerik üretmesi, metin, görsel, video veya bağlantıları kendi profilinde diğer arkadaşlarına paylaşması, paylaşım unsuruna örnektir.. Sohbet (conversations) unsuru ise kullanıcılar arasındaki etkileşim tarzını ifade etmektedir. Geleneksel medyada tek yönlü bir iletişim ortamı varken sosyal medyada yorum, beğeni, paylaşımın yanında kullanıcıların aralarında mesajlaşmasını sağlayan çift yönlü bir iletişim söz konusudur (Kietzmann vd., 2011, ss. 245-246).

Beşinci unsur olan gruplar (groups), ortak ilgi alanlarına sahip olan kişilerce oluşturulan toplulukları ifade etmektedir. Gruplar, bireylerin ortak amaç etrafında toplanabilmesini, kendi aralarında örgütlenmesini sağlayabilen bir unsur olmaktadır. Altıncı unsur olan itibar (reputation), sosyal Medya'da güvenilir olma, prestij sağlama veya popülerite kavramlarıyla bağlantılıdır. Sosyal Medyada yapılan yorumlar,

beğeniler, geri bildirimler bu kavramı sağlayan önemli ölçütlerdir. Son unsur olan ilişkiler (relationships), kullanıcıların diğer kullanıcılarla iletişime geçebilmesini ifade etmektedir. Beğeni, yorum, paylaşım, etiketleme gibi etkileşimleri de kapsamaktadır (Kietzmann vd., 2011, ss. 246-247). Facebook sohbet grupları veya X platformundaki keşfet kısmındaki başlıklarda sunulan ağlar, bu işlevin tipik örnekleridir.

1.1.3. Sosyal Medyayı Etkileyen Faktörler ve Sosyal Medyanın Etkileri

Sosyal Medyayı etkileyen birçok faktör ve etkileri mevcuttur. Bunlardan öncelikli olarak biri sosyal medya kullanıcılarıdır. Yapılan bir araştırmada kültürel değerlerin ve davranış kalıplarının sosyal medya kullanımını şekillendirdiğini göstermektedir. Kullanıcılardan gençlere yönelik yapılan araştırmaya göre kolektivist değerlere sahip Koreli öğrencilerin daha çok sosyal ilişkilerden sosyal destek sağlamaya önem gösterirken buna karşılık bireyci kültür özelliklerinin baskın olduğu Amerikan kültüründe ise öğrencilerin sosyal medya platformlarını daha çok bireysel eğlence amacıyla kullandığı belirlenmiştir (Kim, Sohn ve Choi, 2011, ss. 365-372). Sosyal Medyada kişiler günlük yaşamında kendini ifade etmekte zorlanan kişilerin ya da bu mecralar üzerinden dikkat çekmeye çalışan kişilerin kendi duygu durumlarını ifade etmeye yönelik paylaşımlar yapabildiği bir alan haline gelmiştir (Kıran vd., 2020, s. 436). Aynı zamanda platformların işleyişinde ekonomik faktörler de önemlidir. İçerik üreten yüksek izlenme oranına sahip bir hesap, yüksek reklam gelirleri, sponsorluk gelirleri elde edebilmektedir. Sosyal medyada dünya çapında pazarlama ve reklamın önemli bir payı bulunmaktadır. Örnek olarak Youtube platformunun içerik üreticilerinin izlenme sayısına göre belli bir payı içerik üreticisine paylaşması, dünya çapında Youtuberlık adında bir mesleği ortaya çıkarmıştır (Kuyucu, 2023, ss. 14-18). Son olarak sosyal medya, devlet politikalarından doğrudan etkilenmektedir. Devletlerin sosyal medya yasaları olarak bilinen yasal düzenlemelerle temsilci bulundurma zorunluluğu, sansür, içerik engellemesi, verilerin gizliliği, işlenmesi, korunması gibi politikalardan doğrudan etkilenmektedir. Nitekim Türkiye’de temsilci bulundurma zorunluluğu, veri koruması, içerik engellenmesi gibi birtakım düzenlemeler hayata geçirilmiştir (7253 Sayılı Kanun, 2020).

Teknolojik gelişmelerin sonucunda sosyal medya, günümüzde önemli bir yer tutmaya başlamıştır. Etki alanı ve nüfuz etme gücünün yüksek olması, toplumlar üzerinde olumlu ve olumsuz etkilerde bulunabilmektedir. Aynı zamanda sosyal medya çok boyutlu bir dijital ekosistemdir. Bireylerin iletişim biçimlerinden toplumsal

yapıya, siyasal süreçlerden kültürel üretim ve tüketimine kadar geniş bir yelpazede etkiler yaratabilmektedir. Sosyal medya, kullanıcıların düşüncelerini daha özgür biçimde ifade edebileceği, aynı zamanda toplumsal olaylara katılım sağlayabileceği yeni bir etkileşim ortamı sunduğu, geleneksel medyaya hegemonik bir eleştiri olduğunu savunan yaklaşımların yanında, sosyal medyanın sağladığı sınırları olmayan iletişim ortamının, özgürlük alanını kötüye kullanmaya açık hale getirmesi ve bireylerin mahremiyetini ifşa etme potansiyelinden dolayı bu mecraayı sorgulayan yaklaşımlar da bulunmaktadır (Toruk ve Sine, 2016, s.460). Sosyal Medya, dünyanın her kesiminden ve her fikirden insanların bir araya gelip fikirlerini beyan ettiği, tartıştığı ve müzakerelerde bulunabildiği demokratik ve yeni kamusal alan olup olmadığı tartışılmaktadır (Yegen, 2013, s.119). Sosyal medyanın bir araya getirme gücüyle, tek taraflı iletişim düzeni yerine çoğulculuk ve eşitlik ilkelerinin hâkim olduğu bir iletişim düzeni oluşmuştur. Bu ortamda tam bir ifade özgürlüğünden bahsedilebilecekken sansürün yaygınlaşması sosyal medyanın tam manasıyla bağımsız demokratik bir kamusal alan olup olmadığı tartışmaya açılmaktadır (Yegen, 2013, ss. 133-134). Sosyal Medyanın bireylerin yaşamlarında birçok etkisi bulunmaktadır. Bunlardan biri sosyal etkileridir. Sosyal Medya'nın bireyler ve toplum üzerinde olumlu ve olumsuz etkileri bulunmaktadır. Buna göre Pew Araştırma Merkezi'nin Amerika'da gençlere yönelik 2018 yılında gerçekleştirdiği ankette sosyal medyanın gençler üzerindeki olumlu ve olumsuz etkileri incelenmiştir. Gençlerden yüzde 40'ı Sosyal Medya'nın aile, akraba ve yeni tanışılan kişilerle iletişimi kolaylaştırdığını belirtmiştir. Gençlerin yüzde 16 'sı sosyal medyada bilgiye erişimi hızlandırdığını, Yüzde 15'lik kesim sosyal medyanın ortak ilgi alanları üzerinden topluluklar kurmayı kolaylaştırdığını, %9'u sosyal medyayı eğlence amacıyla kullandığını %7 ifade özgürlüğü sağladığı, %5 sosyal destek alma açısından faydalı bulduğunu belirtmiştir (Anderson ve Jiang, 2018, s.5-6). Buna göre gençler, sosyal medyayı ilişki kurma, bilgiye erişim, yeni ilişkiler kurma ve geliştirme gibi çok boyutlu amaçlar doğrultusunda kullanmaktadır.

Ankete katılan gençlerden yüzde 27 si sosyal medyanın siber zorbalık, hakaret ve karalama, nefret söylemi, anonim hesapların kullanıcılar üzerinde saldırgan tavır üretme potansiyeli olduğunu belirtmiştir. Yüzde 17 si sosyal medyanın yüz yüze iletişimi azalttığını belirtmiştir. Yüzde 15lik kesime göre sosyal medya gerçekçi olmayan yaşam algıları oluşturmakta, gençleri sürekli karşılaştırma baskısına

sokmaktadır. Bu durumlar psikolojik olarak gençleri etkileyebilir. Yüzde 14'lük kesime göre sosyal medya dersleri engellediği ve bağımlılığa yol açtığını ifade etmektedir. Yüzde 12'lik kesim sosyal baskıya uyma, dışlanma korkusu yaşadığını belirtmektedir (Anderson ve Jiang, 2018, s.6-7).

Sosyal medya platformlarında fazla zaman geçirilmesi, bireylerin aile bağlarının zayıflamasına sosyal çevresinden koparak sanal gerçekliğin içerisinde yalnızlaşmasına ve bağımlılığa yol açabilmektedir (Aydoğan, 2024, ss.31-33). Sosyal medyada sürekli yayınlanan kötü haberler, krizler, küresel sorunlar gibi olumsuz bilgi akışına sürekli maruz kalan bireylerin doomscrolling (felaket kaydırması) olarak adlandırılan bireylerin endişe veren haberleri arama eğiliminde olma bağımlılığına yol açmaktadır. Felaket kaydırması yapan bireyler stres, anksiyete bozukluğu veya depresyona yol açabilmektedir (Sayar, 2021). Sosyal medyanın aşırı kullanılması aynı zamanda kaygı bozukluğu, uyku sorunları gibi birçok soruna yol açabilmektedir (Doğan ve Çelik, 2023, s. 164). Sosyal medya platformları ve özellikle sosyal ağlarda kullanıcılar tarafından zamanla gelişen sınırsız paylaşım kültürü, toplumların değerlerini, örf ve adetlerini aşındırmaktadır. (Erdal, 2013, ss. 7-8). Son zamanlarda çok popüler olan sosyal medya platformlarında yediği yemeği paylaşmak, kimlik sunumu, sosyal sınıf göstergesi, kendi kültürünü ifade ediş biçimi ve dijital gösteri kültürünün birer parçası olmasının yanında yemeği görenlerin istek ve arzusunu arttırdığı için bireylerin tüketim alışkanlıklarını değiştirebilmektedir (Çaycı, 2019, ss. 133-134). Sosyal medya platformlarında sıradan insanlar, kendi gösterilerini yaparak şöhret olabilmektedir. Şöhret kültürü her platformda farklı işlemektedir. Örnek olarak Youtube video paylaşımlı bir sosyal ağ olduğundan dolayı içerik üreticilerinin odağı video paylaşmak üzerinedir. Facebook ise sanal bir cemaat halinde hareket dilen bir sosyal ağıdır (Arık, 2013, ss 110-111).

Demokrasinin gereği olarak siyasi partiler, seçmenleri ikna ederek oylarını alıp iktidara gelme amacını taşımaktadırlar. Seçmeni ikna etme yolu da siyasal iletişimden geçmektedir. Sosyal medya platformları; paylaşım ve etkileşim özellikleri sayesinde farklı siyasi düşüncelere sahip kişilerin bir araya getirdiği platformlardır. Milyonlarca aktif kullanıcısı olan ve günlük hayatta önemli yer edinen bu platformlar siyasal aktörler için önemli bir siyasal iletişim aracı haline gelmektedir (Ulusal ve Özdemir, 2024, ss. 36-38). Örnek olarak Youtube, geniş kullanım ağının içinde siyasal olarak kullanımı da barındırmaktadır. Örnek olarak Türkiye Büyük Millet Meclisinde

grubu bulunan Adalet ve Kalkınma Partisi @akparti hesabıyla 400bin aboneye sahiptir ve bu kanaldan 8.500 adet video paylaşılmıştır (Adalet ve Kalkınma Partisi, 2025). Cumhuriyet Halk Partisi ise @chpgenelmerkezi ismiyle 242 bin aboneye sahiptir. Bu hesaptan 7.100 adet içerik paylaşılmıştır. (Cumhuriyet Halk Partisi, 2025) Halkların Eşitlik ve Demokrasi Partisi (DEM) ise @DEMGeneMerkezi isimli hesabı bulunmaktadır. 222 Bin abonesi bulunmaktadır. Bu hesaptan 5 bin içerik paylaşılmıştır (Dem, 2025). Milliyetçi Hareket Partisi @milliyetcihareketpartisi isimli hesabı bulunmaktadır. 124 bin abonesi mevcuttur. Bu hesaptan 9.100 video içerik paylaşılmıştır. (Milliyetçi Hareket Partisi, 2025) Bu hesaplardan mitingler, seçim kampanyaları, siyasi tüm içerikler paylaşılmaktadır. Birbirine entegre olan sosyal medya platformları sayesinde bu videolar diğer sosyal medya mecralarında dolaşıma sokulmaktadır.

Bir diğer sosyal medya platformu olan Twitter’da ise günümüz siyasal aktörlerin neredeyse tamamının birer hesabı bulunmaktadır. Devlet kurumları, siyasal partiler, sivil toplum örgütleri, kamu kurumlarının resmi hesapları ve devlet yöneticilerinin Twitter hesabı bulunmaktadır. Türkiye’deki tüm bakanlıkların resmi X hesabı bulunmaktadır (Göçoğlu, 2019, s. 426). Bu mecrada devlet başkanının özel günlerde yaptığı tebrik ve kutlama mesajlarından günlük siyasi çekişmelere ve kamu kurum ve kuruluşların yaptığı duyurulara kadar her türlü toplumsal olay bu platformda yer edinebilmektedir. ABD Başkanı Donald Trump ile Twitter, uluslararası ilişkiler ve diplomasi alanlarında yeni bir siyasal araç haline gelmeye başlamıştır. Donald Trump’ın 2018 Kasım ayında İran ile ilgili “Yaptırımlar 5 Kasım’da Geliyor!” adlı paylaşım yapması ve karşılık olarak İran Devrim Muhafızları Kudüs Gücü Komutanı olan Kasım Süleymani’nin Instagram’dan “Sana Karşı Duracağım” mesajıyla karşılık vermesi örnek olarak gösterilebilir (Yeni Asya, 2018).

Sosyal medya platformları siyasal amaçlı olarak kullanılması dönemsel olarak farklılık göstermektedir. Sosyal medya ortamında kullanıcılar siyasi gelişmeleri sosyal medya haberleri üzerinden takip ederek değerlendirmelerde bulunabilmektedir. Özellikle X platformunda gündem olan başlıkların altında başlıkla ilgili yorumlar, tartışmalar gerçekleştirilebilmektedir. Özellikle seçim dönemleri ve siyasal gelişmelerin olduğu dönemler sosyal medyanın daha çok siyasal amaçlı kullanıldığını göstermektedir (Arklan, 2016, ss. 622-623).

Sosyal medya, kamu yönetimi ve idari işleyişler üzerinde dönüştürücü rol oynamaktadır. Sosyal medya platformlarında kamu hizmeti gören kamu kurumlarının kurumsal hesaplarının olması halkla ilişkiler açısından önemli dönüşüm sağlamaktadır. Halkla ilişkilerin iki önemli sac ayağı tanıtmak ve tanınmaktır. Yapılan icraatları paylaşma, ilgili haberleri duyurma tek yönlü iletişimin gerektirmektedir. Tanıma faaliyeti ise halkın talep ve şikayetlerini öğrenmeyi içermektedir. Kamu hizmetlerinin duyurulması, kriz yönetimi, bilgilendirme faaliyetleri, kurumsal imaj yönetimi ve tanıtımı , alınan eleştiri ve görüşlerden ve sosyal medyaya yansıyan olumsuz haberlerden etkilenecek hizmet sunumunda değişikliklerin sağlanmasıyla kamu hizmetlerinde kalitenin artırılması gibi birçok alanda etkili bir araçtır (Yağmurlu, 2011, ss. 7-8).

Yargılamaya konu olan olayların sosyal medyaya yansımaları ve kullanıcılar arasında oluşan algılar, yargılama sürecine olumsuz etki edebilecek bir kamuoyu baskısı doğurabilmektedir. Sosyal medyada yargılama süreçlerinde oluşturulan kamuoyu toplumun dikkatini çekmesine, düşünce özgürlüğü kapsamında tartışılması imkanını oluştursa da yargı tarafsızlığını etkileyebilmektedir (Can ve Ercan, 2022, ss.15-16).

Buna göre ülkeden ülkeye değişen kültürel normlar ve değerler, kullanıcıların davranış kalıpları, yapılan yasal düzenlemeler, ekonomik değer, sosyal medyayı etkileyen faktörlerdir. Sosyal Medyanın sosyal, ekonomik, siyasi, idari, hukuki etkileri mevcuttur.

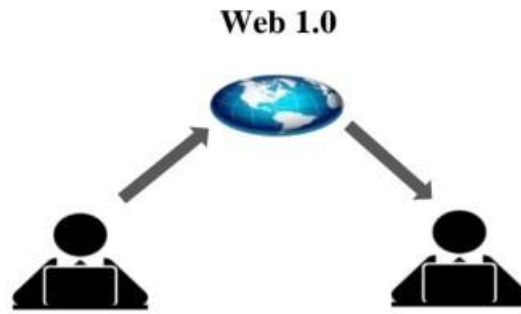
1.2. Sosyal Medyanın Tarihsel Gelişimi

Web teknolojilerindeki gelişme ile ortaya çıkan Web2.0 versiyonu ile birlikte kullanıcılar; beğeni, yorum, paylaşım, karşılıklı iletişim gibi özellikleri kullanabilme becerisi elde etmiştir. Kullanıcıların pasif okuyucu olmaktan çıkarak aktif katılımcı konuma geçmesiyle sosyal medya ortaya çıkmıştır. (Kaplan ve Haenlein,2010) Buna göre sosyal medyanın tarihsel gelişimi internet ve web teknolojilerindeki gelişimle doğrudan ilişkilidir. Günümüze kadar değişim ve dönüşüm geçirerek gelmiştir.

1.2.1. Web Teknolojileri (Web 1.0, 2.0, 3.0, 4.0) ve Sosyal Medya İlişkisi

Sosyal medya kavramı world wide web (www) teknolojisinin geliştirilmesi ve yaygınlaşması sonrasında ortaya çıkmıştır. Web(www) dünya genelinde ağ olarak

bilinmektedir (Akyıldız ve Yılmaz, 2020, s.1418). Web; “internet üzerinden ulaşılan hiper metinler sistemi” olarak tanımlanmakta ve web hizmetleri bilgisayarların internet üzerinden birbirleriyle konuşmasına yardımcı olan yazılımlar olarak görülmektedir (Baş vd., 2022, s. 8). Dijital teknoloji üzerinden her türlü dokümanın birbirine bağlandığı World Wide Web (www) teknolojisi, Web 1.0 dan başlayarak gelişimini sürdürmektedir. Web 1.0 teknolojisi; metin odaklı, kullanıcıların internet aracılığıyla web sitesine girdiği ancak katılımcının yorum yapamadığı, sadece bilginin alımlayıcısı konumunda olduğu yani kullanıcının pasif bir konumda bulunduğu, tüm kontrolün içerik yöneticisinde olduğu, kullanıcının etkileşime giremediği bir teknolojidir (Latorre, 2018/2021, s.345). Bilişim teknolojilerinde gerçekleşen ilerlemelerin yanında internet bağlantılarının sunduğu özelliklerin kullanılması yoluyla web teknolojileri de gelişimine devam etmektedir. Web 1.0 teknolojileri devrim veya dönüşüm geçirmeyen HTML (Hyper Text Markup Language) sayfaları içeren bir yapıdadır (Ersöz, 2020, s.59). 1990’lı yıllarda internetin yaygınlaşmasıyla birlikte Web 1.0 dönemi başlamış ve bu dönemde web siteleri etkileşimi olmayan, temel bilgiler sunan ve görsel açıdan sınırlı bir yapıya sahip olmuştur (Kapan ve Üncel, 2020, s.277).

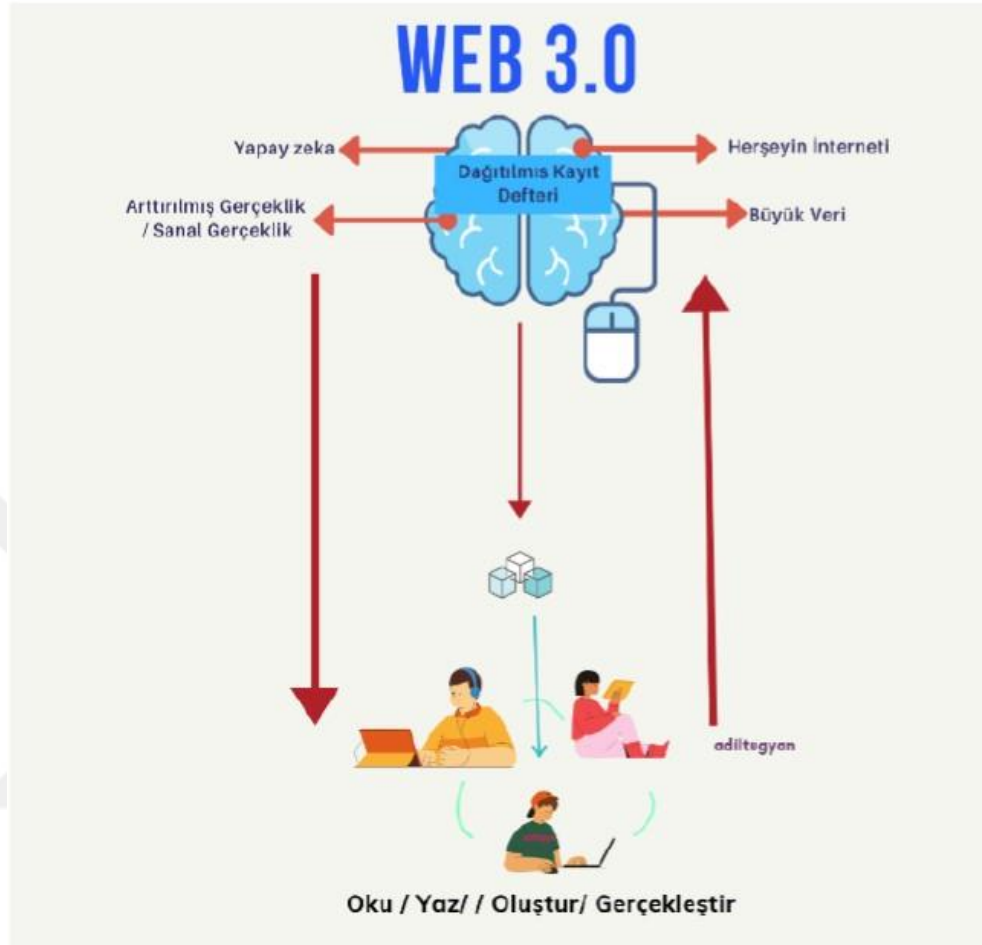


Şekil 1. Web 1.0

Şekil 4. Web1.0'ın Özelliği (Baş vd,2022).

Web 2.0 teknolojisi, internet teknolojilerinde ikinci dalgayı ifade etmekte olup Web1.0'ın tersine monolog ve statik değil dinamik ve katılımcı ve ziyaretçilerin iş birliğine odaklı bir yapıdadır. Sosyal medya kavramının gelişmesi 2000’li yıllarda Web2.0’ın icadıyla sağlanmıştır. Web2.0 teknolojisiyle kullanıcılar pasif konumdan aktif konuma, bilginin alımlayıcısı konumundan bilgi üreticisi konumuna geçmiştir.

Aynı zamanda üreticiye geri bildirim sağlanabildiği, içerik üretiminin yapılabilirdiği, etkileşime açık bir web tabanını ifade etmektedir (Latorre, 2018/2021, s.346).



Şekil 5. Web 3.0 Özellikleri (eTwinning Online Eğitimler (t.y.).

Web3.0, İçerik ve veri arasındaki etkileşimi tanımlayarak kişisel deneyimi arttırmak amaçlı kullanıcının yapmış olduğu internet aramaları, ziyaret geçmişi gibi yapmış olunan eylemler üzerinden kullanıcının yapacağı yeni tercihlerinde bilgi ve öneri sunmaktadır. Yeni bir saat almak isteyen bir kullanıcının yaptığı aramalar ve internet araştırmalarını veri olarak kullanıp buna istinaden oluşturulan kişiselleştirilmiş tercihler üzerinden yeni önerilerini sunan teknolojik gelişmedir (Latorre, 2018/2021, s.347).

Web 4.0, kullanıcıların yalnızca bilgiye ulaşmasını değil, aynı zamanda ihtiyaçlarına uygun çözümler elde etmesini sağlayan bir aşama olarak tanımlanmaktadır. Bu dönemde öne çıkan teknoloji şirketleri, yapay zekâ temelli

öğrenme yöntemlerini bulut altyapıları üzerinden kullanarak verileri işleyebilmekte ve sesli komut gibi araçlarla farklı seçenekler sunabilmektedir (Latorre, 2018/2021, s.348).

Tablo 1. Web1.0-Web2.0-Web 3.0- Web4.0 Özelliklerinin Karşılaştırılması (Özden, 2021'den aktaran Özden, 2022, s. 33).

Özellik Başlıkları	Web 1.0	Web 2.0	Web 3.0	Web 4.0
Geçerlilik Yılı	1995-2000	2000-2010	2010-2020	2020-
Odak Noktası	Doküman odaklı	İnsan odaklı	Bilgi odaklı	Sanal gerçeklik odaklı
İletişim Türü	Tek taraflı/statik	İnteraktif	Gerçek zamanlı	Gerçek zamanlı
İçerik üretimi	Tasarlayıcılar tarafından üretilen statik içerik	Sosyal temelli ve kullanıcılar tarafından üretilen içerik	Çevrimiçi metrikler tarafından yönlendirilen içeriklerin devreye girmesi (ilgi alanına göre reklamların çıkması)	Bulut işletim sistemi
Aksiyon	Yalnızca okuma/statik	Okuma-yazma/interaktif	Okuma-yazma-konuşma/interaktif	Okuma-yazma-konuşma-depolama/interaktif
Web türü	Statik Web	İnteraktif Web	Semantik Web	Akıllı Web (intelligent web)
Örnek Uygulamalar	Britinnica online	Facebook, Twitter, Youtube vs.	IPone Siri	Robot süpürgeler, Glide

Tablo 2. Web'in Tarihsel Gelişimi (www.bilgibilimi.net t.y.).

Web Teknolojisi	Geçerlilik Yılı	Odak Noktası
Web 1.0 (monolog)	1995 - 2000	Döküman Odaklı
Web 2.0 (interactive web)	2000 - 2010	İnsan Odaklı
Web 3.0 (semantic web)	2010 - 2020	Bilgi Odaklı
Web 4.0 (intelligent web)	2020 - 2030	Sanal Gerçeklik Odaklı

Bu tablolardan da anlaşılacağı gibi Web1.0 teknolojisi monolog tarzda doküman odaklı olup iletişim tek taraflıyken Web2.0 ile insan odaklı, sosyal özellikleri olan kullanıcı tarafından üretilen içerikleri olan karşılıklı etkileşime evrilmiştir. Facebook, Youtube, Bloglar gibi siteler örnek gösterilebilir. Web3.0 versiyonunda

semantik web olarak makine öğrenmesiyle sadece kelimeler değil kelime anlamları da değer kazanmıştır. Bilgi odaklı bir yapıdır. Web4.0 ise yerel disklere ihtiyaç duyulmadan sanal ortamda depolama sistemlerinin olduğu yapay zeka ve zenginleştirilmiş gerçekler ön plana çıktığı versiyondur (Bilgibilimi, t.y.).

1.2.2. Dünyada ve Türkiye’de Sosyal Medyanın Tarihsel Süreci

İnsanların ilk zamanlarda iletişim dili olarak ateş ve dumanı kullanması, mağaraların duvarlarına birtakım resimler çizme yoluyla iletişim kurması, insanların iletişim ihtiyaçlarını farklı yöntemlerle karşıladıklarını gösterdiği gibi medyanın gelişimini de göstermektedir. İnsanlar, yaşadıkları döneme uygun iletişim kurmanın yollarını aramışlardır. Sözlü iletişimin yanı sıra yazının ve matbaanın icadıyla medya gelişimi hızlanmıştır (Özçağlayan, 2014, s.133). 20.yüzyılda internetin bulunması ve yaygın olarak kullanılması, iletişim teknolojilerinde kayda değer bir değişim ve dönüşüm sağlamıştır. “Genel ağ” manasına gelen internet (TDK, t.y.). ve ona bağlı olarak gelişen teknolojiler; akıllı telefonlar ve indirilen uygulamalar, sosyal ağlar, e-dergiler, web siteleri ve diğer tüm internet tabanlı teknolojiler, insanların yaşamında merkezi bir konuma gelmiştir (Global Digital Citizen Foundation, 2015, s. 142). Ancak insanların yaşamında merkezi bir konuma gelmesi, bilgisayar altyapı sistemlerinde meydana gelen teknolojik gelişmeler sayesinde olmuştur.

İnternetin evrimi, sosyal medyanın gelişimindeki tarihsel geçmişini oluşturmaktadır. İnternetin icadı 1960’lı yıllarda bilginin küresel çapta bir sistem üzerinden birbiriyle paylaşılabileceği düşüncesiyle başlamıştır. Licklider’in 'Galaktik Ağ' kavramı, bilgisayarların dünya üzerindeki bir sistemde birbirleriyle iletişim kurma yeteneğini ortaya koyan ilk çalışması "kısa notlar" adıyla yayımlanmıştır. Lavrence Roberts, 1965'te döner telefon hatları aracılığıyla farklı şehirlerdeki bilgisayarları birbirine bağlamayı başarmıştır. 1969 yılında ARPA (Gelişmiş Araştırmalar Projeleri Ajansı) kurulmuş ve internet kelimesi olarak kullanılmaya başlanmıştır. ARPANET ağı, o zamanlar dört ayrı üniversitenin ana makineleriyle bağlantı sağlamayı başarmıştır. Diğer resmi kurumlar da zamanla bu ağa dahil olmuştur. Bilgisayar ve internet ağ teknolojisi, karmaşık ve yeni bir alan olduğundan, o dönem yalnızca bilgisayar uzmanları, kütüphaneciler ve kurumlar tarafından kullanılmıştır. 1972 ve 1973 yıllarında imzalanan protokollerle e-posta tanımlanmış, uzak bir bilgisayara bağlantı kurulmuş ve internet siteleri arasında ilk defa dosya paylaşımı yapılmıştır. Günümüz internetinin temellerini atan İletişim Kontrol Protokolü (TCP/IP) sayesinde

daha geniş ağlarla bağlantı imkânı elde edilmiştir. (Kutup, 2018, s.3). 1990 yılında Tim Berners-Lee tarafından Avrupa Nükleer Araştırmalar Merkezi'nde (CERN) Wide Web (www) geliştirilmiştir. Bu gelişme, internetin ticarileşmesini hızlandırdı hem de multimedya kullanımına hazır hale getirdi. Www üzerindeki iletişim kurallarını belirleyen hipermetin aktarım protokolünün ortaya çıkmasıyla www hızla yaygınlaşmıştır (Başaran, 2006, s. 19). Türkiye'deki Gelişim 1993 yılında ABD'deki NSFNet (National Science Foundation Network) TCP/IP Protokolü kullanılarak ODTÜ Bilgi İşlem Daire Başkanlığı salonundaki yönlendiriciler aracılığıyla Türkiye'deki ilk internet bağlantısı gerçekleştirilerek Türkiye'deki sosyal medya gelişim süreci başlamıştır (Saka, 2017, s.958). 1999 Yılında Türkiye'de anonim veya kimliği bilinen şekilde kullanıcı odaklı metin paylaşımı yapılan Ekşi Sözlük adlı çevrimiçi iletişim ağı zamanla kullanıcıların bilgi, görgülerini paylaştığı yer olmasının ötesinde Türkiye'deki gündemin tartışıldığı yer konumuna gelmiştir (Vegasis Medya, 2025). 2000'li yılların başında ise MSN Messenger gibi çevrimiçi iletişim ağları gençler arasında hızla yayılmış, sosyal etkileşimi dönüştürmeye başlamıştır (Arena, 2025). Bu dönem sosyal medya kavramının tam olarak yer edinmediği ön-sosyal medya dönemi olarak değerlendirilebilir.

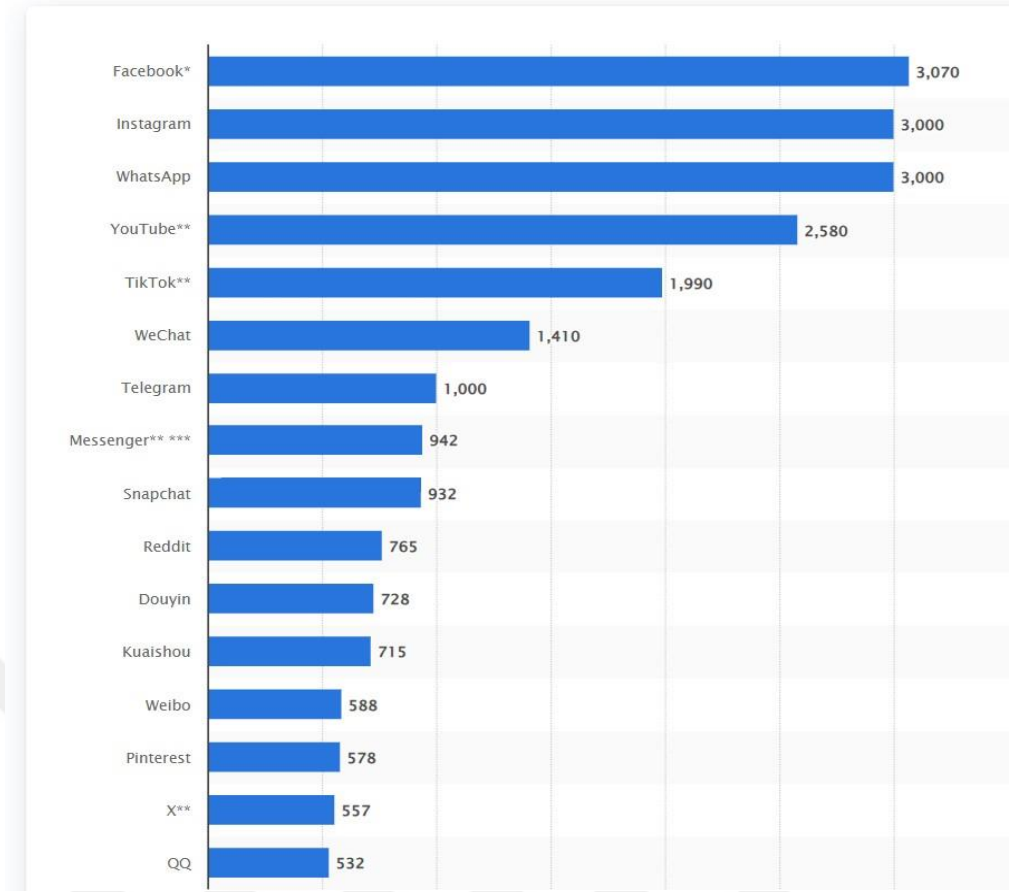
2005 yılı sonrasında küresel çapta sosyal ağların yaygınlaşmasıyla birlikte Türkiye'de sosyal medya kullanımı hızlanmıştır. 2004 yılında kurulan Facebook Türkiye'de 2007 yılında, 2006 yılında kurulan Twitter 2010 yılında, 2010 yılında kurulan Instagram, 2012 yılında popüler olmuştur (Kültür ve Yaşam, 2025). Yine 2005 yılında kurulan YouTube platformu Türkiye'de 2006 yılında kullanıma açılmıştır (Sabah, 2025). 2010 yılında ABD, 115,3 milyon kullanıcıyla Facebook'un en çok kullanıldığı ülkelerde birinci sırada yer alırken, İngiltere 26 milyon kullanıcıyla ikinci sırada bulunmaktadır. 25 milyon kullanıcıyla Endonezya üçüncü sırada, Türkiye ise 21 milyon kullanıcıyla dördüncü sırada yer almaktadır (Akyol ve ark, 2012, s.5).

2013 yılında Türkiye'de sosyal medya platformları üzerinden örgütlenen grupların Taksim Gezi Parkı'nda 5 ağacın sökülmesi haberlerinin akışıyla birlikte sosyal medyada örgütlenmesiyle birlikte toplumsal hareketler meydana gelmiştir. Dönemin başbakanının sosyal medyayı "baş belası" olarak nitelendirmesi ve sosyal medyanın toplumsal hareketlere aracılık etmesi, sosyal medyanın toplumsal dönüşüm, örgütlenme, siyasal iletişim açısından önemini göstermektedir (Yeni Şafak, 2013).

Gezi Parkı olayları sonrasında Türkiye, sosyal medyaya dijital güvenlik ekseninde bir devlet politikası olarak bir dizi önlemler almıştır. 2014 yılında 5651 sayılı İnternet Ortamında İşlenen Suçlarla Mücadele Kanunu'nda yapılan değişikliklerle sosyal ağ platformlarına da erişim engeli, içerik kaldırma gibi düzenlemeler getirilmiştir (5651 Sayılı Kanun, 2014). 2020 yılında 7253 Sayılı Kanun: Sosyal Medya Hizmetlerine İlişkin Düzenlemeler Hakkında Kanun ile günlük erişimi 1 milyondan fazla olan sosyal ağ sağlayıcılarının temsilci bulundurma zorunluluğunu getirmiştir. İçeriklerin hukuka uygun olmaması durumunda içeriklerin tamamen çıkarılabileceğine dair bir hüküm eklenmiştir. Türkiye'deki kullanıcı verilerinin Türkiye'de saklanması, 6 ayda bir veri ve içerik kaldırma istatistiklerinin raporlanması ve ilgili kurumlara bildirilmesi gibi hükümlerle içerik kaldırma, veri depolama gibi hükümler eklenmiştir. Uygulanmadığı takdirde uygulanacak yaptırımlar, detaylandırılmış ve düzenlenmiştir (7253 Sayılı Kanun, 2020). 7338 Sayılı Vergi usul kanunu ile bazı kanunlarda değişiklik yapılmasına dair Kanun'daki 2022 yılındaki değişiklikle yıllık kazancı 3 milyon TL'yi aşan içerik üreticileri, reklam ve sponsorluk gelirleri, uygulama içi satın alma gelirleri gibi gelirler yüzde 15 oranında stopaj vergisiyle vergilendirilmiştir (7338 Sayılı Kanun, 2021). Sosyal Medya, tüketicinin para kazandığı aşamaya evrilmiştir. Ancak kurallara bağlı olarak bu aşamada sosyal medya üzerinden para kazanan 3 milyon tl'yi aşan içerik üreticilerine yönelik vergilendirme getirilmiştir.

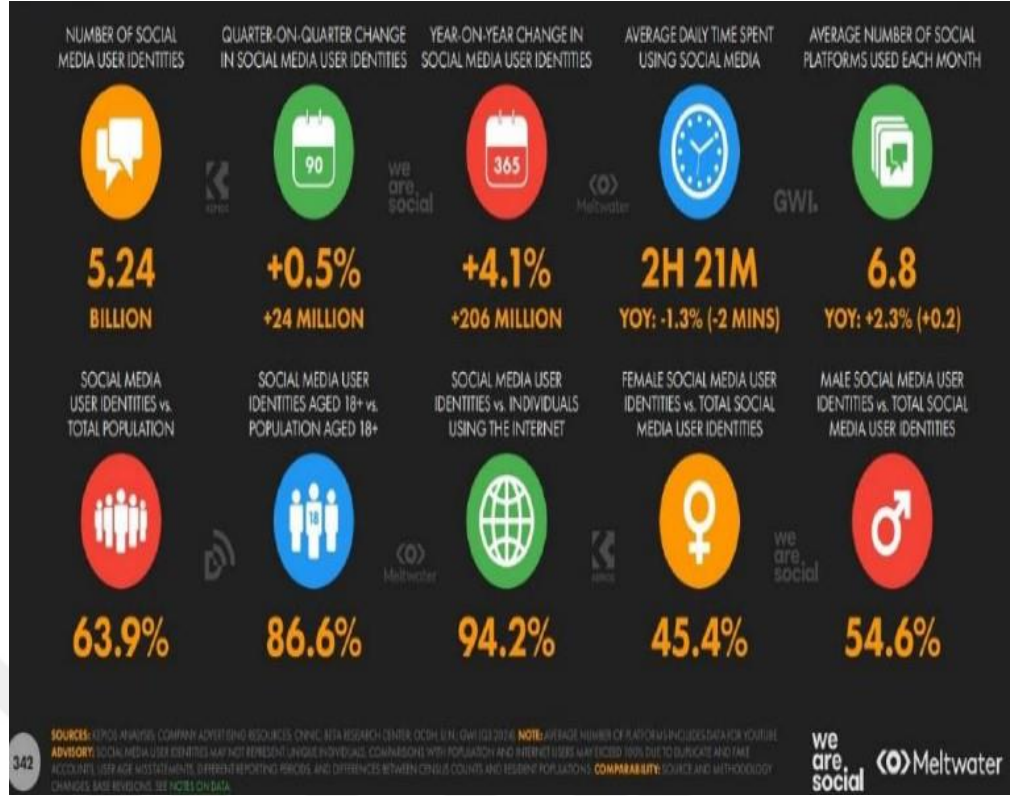
1.2.3. Türkiye ve Dünyada Güncel Kullanım Oranları

Dünya genelinde 100 milyon sayısını aşmış birçok sosyal medya platformu bulunmaktadır. Bunların büyük çoğunluğu Amerika Birleşik Devletleri menşesinde olmasına karşın Çin de son zamanlarda sosyal medya platformu geliştirmede önemli gelişim göstermiştir. Özellikle WeChat , QQ ve Douyin gibi platformlar Çin'de önemli bir kullanım alanına sahipken özellikle Douyin'in uluslararası versiyonu olan TikTok uygulaması küresel alanda özellikle gençler arasında popüler olmuş ve bu alanda ön plana çıkan bir uygulama olmuştur (Statista, 2025).



Şekil 6. Aktif kullanıcı sayılarına göre en çok kullanılan sosyal medya platformları (Statista, 2025).

Araştırma bulgularına göre, Meta bünyesinde faaliyet gösteren Facebook platformu 1 milyar kullanıcıyı aşan ilk sosyal medya platformu olması, bu alanda önemli bir dönüm noktasıdır. Şuan 3 milyar gibi bir kullanıcıya sahip olmasıyla küresel ölçekte en çok kullanıcıya sahip olan platform olma özelliğine sahiptir.



Şekil 7. Sosyal Medya Kullanımına Genel Bakış (Statista, 2025).

Tablodaki veriler soldan sağa sırasıyla incelendiğinde Şubat 2025 itibarıyla dünya genelinde sosyal medya kullanıcı sayısı 5,24 milyardır. Çeyreklik bazda sosyal medya kullanım değişimi 24 milyon artış sağlamıştır. Yıllık bazda sosyal medya kullanıcılarının değişimi yüzde 4,1 artarak 206 milyon yeni kullanıcı artışı olmuştur. Sosyal medya kullanıcılarının günde ortalama 2 saat 21 dakika zaman geçirdiği anlaşılmaktadır. Kullanıcıların aylık 6,8 sayısında farklı sosyal medya platformlarını ziyaret ettiği anlaşılmaktadır. Sosyal medya kullanıcılarının toplam dünya nüfusuna oranı yüzde 63,9 olmaktadır. Demografik olarak incelendiğinde 18 yaş ve üzeri nüfusun yüzde 86,6'sının sosyal medya kullandığı görülmektedir. İnternet kullanıcılarının %94,2'sinin aynı zamanda sosyal medya kullanıcısı olmaktadır. Cinsiyet dağılımında kadınların %45,4, erkeklerin %54,6 oranında temsil edilmektedir. Bu bulgulara göre internet kullanıcılarının sosyal medya kullanımı da genele yayıldığını, dünya toplam nüfusuna oranla sosyal medya kullanımının yaygın olduğunu, günlük 2 saat 21 dakika kullanım süresiyle insanların günlük yaşamında önemli bir yer edindiğini, yıllık büyüme oranıyla büyüme potansiyelinin devam ettiğini ancak çeyreklik bazda büyümenin sınırlı kaldığını, aylık bazda 6,8 farklı sosyal medya platformunun kullanılmasının kullanıcıların tek bir platformdan ziyade birden

çok platformu kullandığını, 18 yaş ve üzeri nüfusun yüzde 86,6'sının sosyal medyayı kullanması yetişkinler bireylerin arasında da kullanımının yaygın olduğunu, sosyal medyanın küresel ölçekte yaygın bir iletişim kanalı haline geldiğini göstermektedir (Statista, 2025).

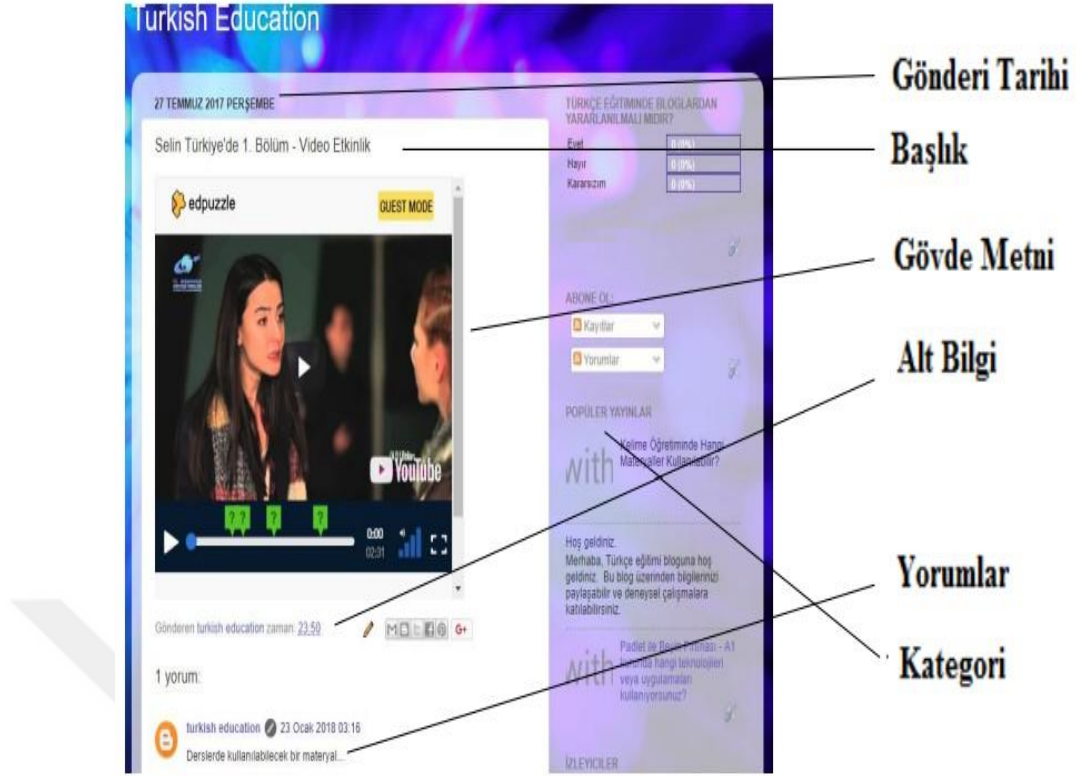
1.3.Sosyal Medya Araçları

Sosyal medya araçları; bloglar, mikrobloglar, sosyal ağlar, anlık mesajlaşma uygulamaları, sosyal işaretleme ağları olarak sınıflandırılmaktadır.

1.3.1. Bloglar Ve Mikrobloglar

Bloglar; web ve log kelimelerinin kısaltılmış hali olan çevrimiçi günlükler anlamına gelen basit ve anlaşılabilir formda olan kişilerin duygu, düşünce, fikir, öneri ve görüşlerini açılan başlıklar üzerinden paylaştığı, düzenli aralıklarla güncellenen ve en son yayınlanan gönderiden kronolojik olarak geriye doğru sıralanan web sayfası çeşididir. Türlerine göre blog çeşitleri bulunmaktadır. Bunlar; Kişisel Bloglar: - Bu blogların kullanımı basit ve eğlencelidir. İnsanların her gün ne yaptıklarını ve nasıl hissettiklerini yazdıkları kişisel günlükler gibidirler. En yaygın blog türüdür. Tematik Bloglar: - Bunlar tek bir şeyden bahseden ve o konu hakkında çok şey bilen kişiler tarafından oluşturulan bloglardır. Politika, para, yemek, teknoloji, tasarım ve daha birçok konu hakkında farklı türde içerikler hazırlıyorlar. Topluluk Blogları: Bunlar, insanların bir web sitesine katılmasına ve birlikte içerik oluşturmaya olanak tanıyan üyelik sistemine sahip bloglardır. Kurumsal Bloglar: Bunlar şirketlerin müşterilerine, ortaklarına ve diğerlerine şirket ile ilgili bilgilerin daha samimi olarak paylaşıldığı bloglardır (Afyon Kocatepe Üniversitesi, 2025).

Mikrobloglar ise insanların kendilerini hızlı ve sıklıkla ifade etmelerinin ve kısa mesajlar göndermelerinin bir yoludur. Daha uzun ve ayrıntılı gönderiler içeren bloglardan ve daha kısa ve resmi olmayan mesajların bulunduğu anlık mesajlardan farklıdır. X platformu bilinen en önemli örnektir (Mayfield, 2008, s. 27).



Şekil 8. Bir blog sayfasının görünümü (Moralı, 2018, s.44).

Şekil 8 de bir blog sayfasının içeriğinde ne zaman yayınlandığı, neyle ilgili olduğu, ne söylediği, ne tür bir blog olduğunu belirten birtakım temel bölümler yer almaktadır. Gönderim tarihi, içeriğin ne zaman yayınlandığını belirtmektedir. Bu sayede bloglar yayınlanma sırasına göre yapılandığı için okuyucuların eski ve yeni gönderileri bulmasına yardımcı olmaktadır. Başlık, içerikleri tanımlama ve genelde yıllara göre arşivlenmiş blog sayfalarında aranan içeriği bulma açısından önemli kolaylık sağlamaktadır. Metnin ana kısmı gövde metnidir. Metne resimler, videolar, bağlantılar veya alt başlıklar da eklenebilmektedir. Gönderinin altbilgi kısmında yazar kişinin adı ve paylaşılacak bazı simgeler bulunur. Ayrıca insanlar paylaşılan içeriğin altına yorum yapabilmektedir. Kategori bölümü gönderilerin konuya göre gruplandırılmasını ve aranan konunun bulunmasını kolaylaştırmaktadır (Moralı, 2018, s.43-44).

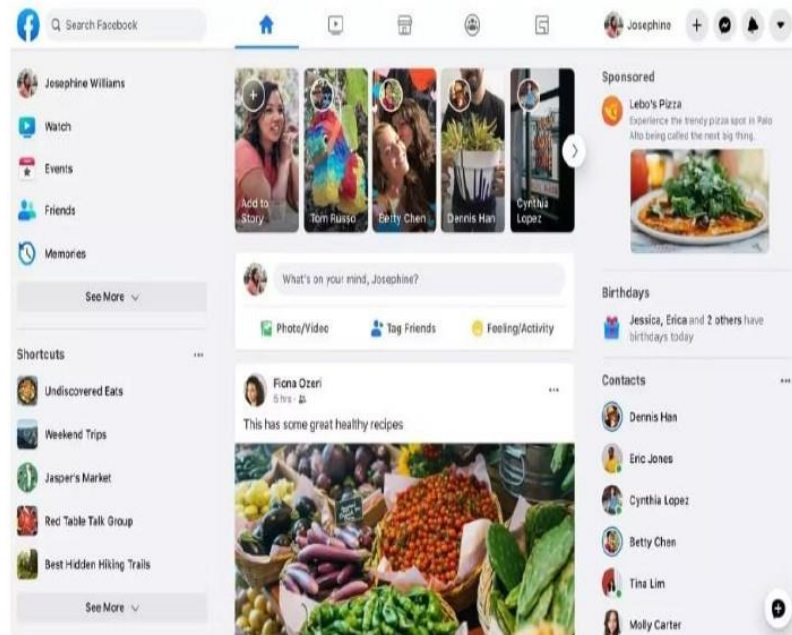
Blog ismi	Web uzantısı
Wordpress	http://tr.wordpress.com/
Weebly	http://www.weebly.com/?lang=tr
Edublogs	http://edublogs.org/
Blogger	https://www.blogger.com/
Xanga	http://www.xanga.com/
Tumblr	https://www.tumblr.com/

Tablo 3. En çok kullanılan blog siteleri Kaynak: (Moralı, 2018 s.43).

Tablo 3 te Wordpress, Weebly, Edublogs, Blogger, Xanga, Tumblr isimli blog siteleri, örnek olarak gösterilmiştir.

1.3.2. Sosyal Ağlar

Sosyal ağlar, insanların çevrimiçi olarak kendilerine profil oluşturmalarına, çevrimiçi olarak diğer insanlarla konuşmasına ve tanışmasına, çeşitli bilgiler paylaşmasına ve yeni arkadaşlar edinmesine ve ürettikleri içerikleri birbirlerine gönderdikleri web ortamlarıdır. Örnek olarak günümüzde en popüler sosyal ağ platformları Facebook , Twitter, Instagram, LinkedIn'dir (Tosun, 2019 s.305).



Şekil 9. Örnek Sosyal Ağ Görünümü: Facebook (www.teknoblog.com)

1.3.3. Anlık Mesajlaşma Uygulamaları

Anlık mesajlaşma bağımsız uygulamalar veya gömülü yazılım aracılığıyla yapılan gerçek zamanlıya yakın mesajlaşmadır. Mesajlaşmanın yanında grup sohbeti, video konferansları, sesli aramaların yapılabilirdiği, dosya ve görsel aktarımının yapılabilirdiği bağımsız uygulamalar veya birden fazla amaca hizmet eden gömülü uygulamalardır. Facebook, Messenger gibi sosyal medya platformlarına entegre edilebilmektedir. Bazı popüler anlık mesajlaşma uygulamaları Discord, Whatsapp Messenger, Snapchat gibi uygulamalar gösterilebilir (Lutkevich ve Scarpati, 2022). Anlık mesajlaşma uygulamalarının sosyal medya platformlarına entegre olmaya başlaması, bu uygulamaların sosyal medya platformlarına ait olan durum, keşfet, kanal takibi gibi birçok özelliği aktif etmesi, tam olarak sosyal medya özelliklerini taşımasa da sosyal medya platformlarına doğru evrilmeye başlamaları, sosyal medya aracı olarak incelenmesini gerektirdiği değerlendirilmiştir.

Türkiye’de FETÖ terör örgütüne yapılan operasyonda örgüt içi koordinasyon sağlama, emir ve talimat ile hiyerarşik yapılanmanın devamı, gizli bilgi paylaşımı amacıyla Signal ve WhatsApp uygulamalarını kullandığı görülmüştür. Bu uygulamaların içerdiği teknik şifreleme yöntemleri nedeniyle mesajlar, göndericiden çıktığı an şifrelenmektedir. Mesaj, ancak alıcı tarafından çözülebilmektedir. Yapılan bu operasyonda FETÖ terör örgütü üyesi olduğu belirlenen farklı devlet kurum ve kuruluşlarında görev yaptığı tespit edilen 19 şüpheli gözaltına alınmıştır (Cozumpark, 2025).

Terör örgütü Pkk’nın eleman devşirme hedeflerinden biri üniversitelerde öğrenim gören gençlerdir. Burada hedef şahıs ilk olarak Whatsapp uygulamasında kurulan özel bir gruba alınarak etkileme başlamaktadır. Pkk terör örgütünün eylemsellik içinde sağlanan materyallerin finansmanı için satılacak olan dergide yazılan yazıların Signal uygulaması üzerinden toplandığını, bu uygulamalarda yazılanın belli olmaması için kod adı veya mahlas kullanıldığı belirtilmektedir (Anadolu Ajansı, 2024).

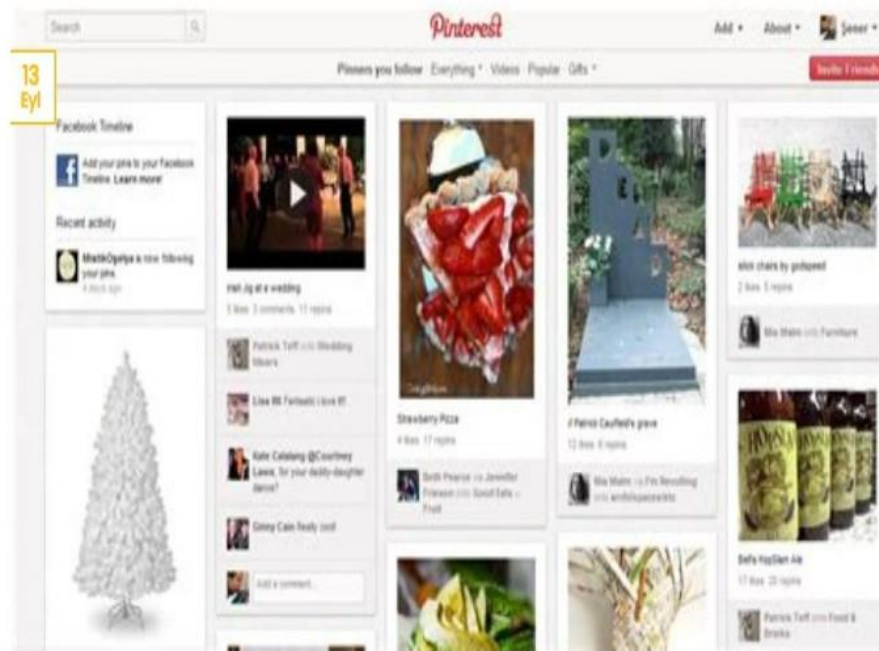
Suç örgütleri de kendi aralarında gizli iletişim sağlamak amacıyla Whatsapp gibi anlık mesajlaşma uygulamaları kullanmaktadır. Türkiye’de Casperlar suç

örgütüne yapılan soruşturmada örgüt içi WhatsApp yazışmaları ortaya çıkmıştır. Bu yazışmalar sonucunda örgüte yönelik operasyonlar gerçekleştirilmiştir (İhlas Haber Ajansı, 2026).

Buna göre terör örgütleri ve suç örgütleri, anlık mesajlaşma uygulamalarını aktif olarak birçok amaç doğrultusunda kullanmaktadır. Aralarındaki yazışmaların tespiti halinde örgüt içi kritik bilgiler elde edilerek operasyonlar yapılabilmektedir. Bu nedenle bu mecralara yönelik teknolojik birtakım tedbirler arttırılmalıdır.

1.3.4 Sosyal İşaretleme(İmleme) Ağları

Kullanıcıların web sitelerinde beğendiklerini yer imleri ekleyerek ve etiketleyerek paylaşımlarına olanak tanımaktadır. Diğer kullanıcılar daha sonra aynı paylaşımları anahtar kelimeleri kullanarak sosyal medyada paylaşabilmektedir. Böylece diğer kullanıcılar, paylaşılanları görebilmektedir. Favorilere eklenen fotoğrafları, metinleri vb. ne kadar çok kişi paylaşırsa gönderinin arama motorlarında ilk sıralarda görünme olasılığı o kadar artmakta ve daha popüler hale gelmektedir. Örnek olarak Pinterest sitesi verilebilir (Er,2023).



Şekil 10. Örnek Sosyal İşaretleme(imleme) Ağı: Pinterest (Eticaret Marketing, 2025)

1.4. Güvenliğin Sosyal Medya İle İlişkisi

Ulusal güvenlik açısından bakınca sosyal medya, terör örgütlerinin birçok ülkede sosyal medyayı propaganda yapmak, örgütlenmek, para toplamak ve radikalleştirmek için kullandığı araç konumundadır. Bu yüzden dijital platformlar güvenlik kurumları için hem takip edilmesi gereken bir istihbarat kaynağına, hem de dikkat edilmesi gereken bir tehdit unsuruna dönüşmektedir (Kara, 2024). Sosyal Medya platformlarında dezenformasyon ve misenformasyon paylaşımlarının yoğun bir şekilde kullanılması toplumsal düzenini, kamu güvenliğini ve bireysel huzurunu olumsuz anlamda etkileyen önemli bir araç haline gelmiştir (Bahar, 2020). Sosyal Medyada dezenformasyon Sosyal medya kullanıcıları dolandırıcılık, tehdit, şantaj, siber zorbalık gibi pek çok riskle karşı karşıya kalmaktadır. Özellikle veri güvenliği zayıf olan platformlarda, insanlar çoğu zaman farkında olmadan büyük güvenlik tehditlerine maruz kalınmaktadır. Bu durum büyük veri ihlalleriyle toplumsal güvenliğe de zarar verebilmektedir (Kaya, 2022). Nitekim Türkiye’de kişisel verilerin ele geçirildiği ve yasadışı amaçlar doğrultusunda tüm vatandaşların bilgilerinin Panel isimli uygulamadan satıldığı belirtilmektedir (Alakoyun, 2025).

1.4.1. Devlet Güvenliğinin Tanımlanması ve Kapsamı

Güvenlik kavramı en genel haliyle toplumsal düzenin sürekliliği ve insanların emniyet içerisinde korkudan kurtulma durumu olarak tanımlanmaktadır (Türk Dil Kurumu, 2026). Toprak bütünlüğüne bağlı olarak siyasal bakımdan örgütlenmiş millet veya milletler topluluğunun oluşturduğu tüzel varlık olan devletin (Türk Dil Kurumu, 2026) temel meşruiyet kaynağı, bireyden topluma uzanan bu güvenlik ihtiyacının tesis edilmesidir. Bu bağlamda Devlet Güvenliği; Soyut, hukuki tüzel kişiliği olan devletin iç ve dış tehdit ve tehlikelerden koruyarak varlığını sosyal ve hukuki anlamda bağımsız bir şekilde sürdürebilmesidir (Çınar, 1997, ss. 59-61). Geleneksel güvenlik anlayışı, uluslararası sistemdeki yapısal dönüşümler ve devlet dışı aktörlerin yükselişiyle birlikte kapsamını genişleterek ulusal güvenlik boyutuna evrilmiştir. Bu şekilde değişen düzlemde ele alınsa da günümüz dünya düzeninin en temel gerçekliği ulus devletlerdir. Uluslararası ilişkileri ve güvenliği düzenleyen üst otoritenin olmaması, devletlerin kendi güvenliğinin sağlanmasında ana aktör olmaya devam etmeye zorlamaktadır. Bu doğrultuda devletlerin maddi güç unsurları, yönetim tecrübesi, tarihsel dinamikleri, toplumsal teşkilatlanma düzeyi, güvenlik kapasitesini belirleyen

temel bileşenlerdir (Begenirbaş ve Ünver, s.93). Bu anlamda geleneksel olarak devlet güvenliği askeri güce, toprak bütünlüğü ve rejim güvenliği gibi konulara odaklansa da günümüzde siber uzay, siber güvenlik gibi konular da devlet güvenliği için önemli konular haline gelmiştir. Devletin bekasını ilgilendiren varlığına yönelik siber casusluk faaliyetleri, siber egemenlik anlamında veri güvenliğinin sağlanması, sosyal medya platformları üzerinden yürütülen dezenformasyonlar yoluyla toplumda algı yönetimi ve toplumu yönlendirme faaliyetleri veya devlet itibarının zedelenmesi , sosyal medyadaki açık bilgiler üzerinden sosyal medya istihbaratı sağlama , terör örgütlerinin propaganda faaliyeti, eleman devşirme, örgüt içi eğitim, haberleşme gibi birçok alandaki faaliyetler için kullanılan ve psikolojik harpte dijital saha olarak kullanılan sosyal medya, modern devlet güvenliğinin kapsamını fiziksel sınırlardan dijital sınırlara taşıyarak genişletmiştir.

1.4.2. Kamu Güvenliğinin Tanımlanması ve Kapsamı

Türk Dil Kurumu Sözlüğüne göre Kamu; Halk hizmeti gören devlet organlarının tümünü ve bir ülkedeki vatandaşların bütünü ifade etmektedir. Bu bağlamda kamu güvenliği; devletin egemenlik sınırları içinde yaşayan vatandaşlarının can ve mal güvenliğinin sağlanması, hak ve özgürlüklerinin muhafaza edilmesidir (Kızılyel, 2014, s. 63). Bir başka tanıma göre kamu güvenliği; “bir ülkenin coğrafi sınırları içerisinde, her türlü tehdit ve tehlikeden uzak olarak başta vatandaşların güvenlik ve huzurunun sağlanması, daha sonra da sırasıyla, devlete ve özel kişilere ait binaların her türlü sabotaj ve tehlikelere karşı korunması”dır (Seçkin, 2001, s. 20). Ekonomi, sağlık gibi temel ihtiyaçların karşılanabilmesi için kamu güvenliğinin sağlanması gerekmektedir (Mayerfeld, 2009, s. 58). Kamu güvenliği ve düzenini ilgilendiren her konuda devlet, vatandaşlarını korumak için tedbirleri kolluk hizmetleri vasıtasıyla gerçekleştirmektedir. Kolluk hizmetleri; İdarenin kamu güvenliği ve kamu düzenini sağlaması için görevlendirdiği kurumun yapmış olduğu tüm faaliyetlerdir (Fındıklı ve Bilgiç, 2006, s. 198). Devletin asli ve sürekli görevleri olan temel kamu hizmetleri; dış politika, dış savunma, iç güvenlik ve adalet, eğitim, sağlık ve diğer kamu hizmetlerinin görülmesidir. Devlet, çoğu kamu hizmetlerini gerçekleştirmek için çeşitli kurumsal mekanizmalar kullanmaktadır. Örnek olarak Dış politika için Dışişleri Bakanlığı’nı, dış güvenlik için silahlı kuvvetler, iç güvenlik için emniyet ve jandarma teşkilatı tarafından gerçekleştirilmektedir. Kamu güvenliğinin sağlanması da bu kurum ve kuruluşlar tarafından yerine getirilmektedir (Öztekin, 2015).

Güvenlik kavramı, tarihsel süreç boyunca çağın teknolojik ve toplumsal dinamiklerine paralel olarak sürekli evrilmektedir. Tehdit algısının değişmesiyle birlikte güvenlik yaklaşımları da yeni önlemler gerektirmekte ve bu durum dinamik bir etkileşim yaratmaktadır. Zira güvenlik tehditleri ile güvenlik anlayışları arasında güçlü ve karşılıklı bir ilişki bulunmaktadır. Bu tehditlerin en önde gelenlerinden biri olan terörizm, stratejilerini, eylem biçimlerini ve kullandığı araçları teknolojik gelişmelere uyum sağlayacak şekilde dönüştürmüştür; bu da devletlerin güvenlik politikalarını doğrudan etkilemiştir. Özellikle 11 Eylül 2001 saldırılarıyla birlikte terörizm yeni bir boyut kazanmış, terör örgütleri teknolojiden yoğun biçimde yararlanarak küresel ölçekte eylemler gerçekleştirmeye başlamıştır. Bu dönemde post-modern terörizm olarak adlandırılan yeni evrede, örgütler taktik ve tekniklerini önemli ölçüde yenilemişlerdir. Buna karşılık ulus devletler de terör örgütlerini kaynak alanında etkisiz hâle getirmeye yönelik proaktif stratejiler geliştirerek güvenlik anlayışlarını yeniden şekillendirmişlerdir (Gökçe, 2021).

1.4.3. Siber Uzay ve Siber Güvenlik Kapsamında Sosyal Medya

Güvenlik kavramının tanımına yönelik çalışmalar, dünya savaşları döneminde başlamıştır. Bu dönemde güvenlik kavramında aktör olarak devlet benimsenmişken zamanla güvenlik kavramının kapsamı genişlemiştir. Başlangıçta devletin güvenliği ve askeri güç olarak algılanan güvenlik anlayışı, güvenlik kuramlarının da etkisiyle devletin güvenliği anlayışından çıkarak zamanla kapsamı genişlemiştir. Özellikle İkinci Dünya Savaşı'ndan sonra Ulusal Güvenlik kavramıyla birlikte güvenliğin odak noktası devlet haricinde, ekonomi, siber dünya, çevre, enerji, bireyler ve kurumları kapsayacak şekilde genişlemiştir. Bu çerçevede birey güvenliği, çevre güvenliği, gıda güvenliği, ekonomik güvenlik gibi boyutlar öne çıkmaktadır (Yenal, 2020, s.10). Enerji Güvenliği Uluslararası Enerji Ajansı(IEA)' na göre enerji kaynaklarının ucuz maliyetle ve kesintisiz olarak temin edilebilmesi olarak tanımlanmaktadır. (University of Plymouth, t.y.) Güvenlik kavramının çerçevesi devlet haricinde belirtilen odak noktalarına doğru genişlemesiyle birlikte aynı şekilde tehdit kavramının kapsamı da ekonomi, çevre, enerji, siber dünya ve siber dünyanın içinde bulunan sosyal medyayı da kapsayacak şekilde genişlemiştir. Geleneksel olarak düşman, diğer devletler olarak anlaşılmaktadır. Ancak devletlere yönelik tehditleri devlet dışı aktörler de gerçekleştirmektedir (Yenal, 2020, s.9). Bu anlamda gelişen güvenlik anlayışına göre devlet dışı aktörler, asimetrik tehditler ile devletleri tehdit

edebileceği anlaşılmaktadır. Terör örgütleri, iletişim teknolojilerindeki gelişmelerin sunduğu imkanları kullanarak devletlere karşı asimetrik tehditler geliştirebilmektedir. Siber Uzak ve Siber Güvenlik alanları da dijital alan üzerinden devletlere yönelik geliştirilebilecek tehditleri ele almaktadır. Siber kavramı Yunancada rehberlik etme, kontrol etme manası taşımaktadır. Siber kelimesi ilk kez 1958 yılında Louis Couffignal tarafından kullanılmıştır. 1984 yılında William Gibson'ın Neuromancer adlı romanında siber uzak kavramının kullanılmasıyla kavram yaygınlaşmıştır. Elektromanyetik formda bilgi üretiminden farklı sistemler vasıtasıyla bilgiye erişimin mümkün kılındığı bütün sanal ortama siber uzak denilmektedir (Erendor,2025). Siber Güvenlikte ise üzerinde uzlaşa sağlanmış bir anlamı olmamakta olup bilgi güvenliği ve bilgisayar güvenliği anlamlarına yakın manada kullanılmaktadır. Bilişim sistemlerinin güvenliği bilgisayar güvenliği kavramına yakın anlam taşımaktadır. Bilgi güvenliği kavramı ise kişisel ve kurumsal verilerin güvenliğine yakın bir kavramdır. Siber Suçlar, siber güvenliğin konusudur. Elektronik ağlarla işlenen klasik suçlar, elektronik ağlara özgü suçlar; hackerlik olarak bilinen bilgisayar korsanlığı, Zararlı yazılımlar yoluyla zarar verme, hizmet engelleme, sosyal mühendislik saldırıları, elektronik medya üzerinde yayınlanan yasadışı içerikler siber güvenliğin konularıdır (Hekim ve Başbüyük, 2013). Siber Suçlar başlığı altında işlenen suçlar sosyal medya aracılığıyla işlenebilmektedir. Nitelikli Dolandırıcılık, Tehdit, Şantaj gibi suçlar sosyal medya kullanıcıları arasında yaşanabilmektedir. Yine Sosyal Medya kullanıcıları, siber saldırılara maruz kalabilmektedir. Sosyal Medya kullanıcılarına mesaj yoluyla iletilen zararlı yazılım linkleri üzerinden sosyal medya hesaplarının ele geçirilmesi, sosyal medya sitelerine bilgisayar korsanlığı yaparak hizmeti engelleme gibi birtakım siber suç faaliyetleri sosyal medya üzerinden gerçekleştirilmektedir. Siber Suçların sosyal medya üzerinden işlenmesi, kamu güvenliğinin sağlanması ve kamu düzeninin sağlanması açısından önlem alınması gereken dijital sahalardan biridir. Siber suç teknikleriyle devlet bürokrasisi içerisindeki kişilerden kritik istihbari bilgi sağlama gibi faaliyetleri önleme devlet güvenliği açısından önemlidir.

1.4.4. Sosyal Medya-Devlet Güvenliği Etkileşimi

Sosyal medya, günümüzde devlet politikalarından doğrudan etkilenen ve uluslararası alanda devlet güvenliği açısından kritik bir mücadele sahasına dönüşen çok boyutlu bir mecradır. Devletlerin sosyal medya yasaları olarak bilinen yasal düzenlemelerle; temsilci bulundurma zorunluluğu, sansür, içerik engellemesi, verilerin

gizliliği, işlenmesi ve korunması gibi politikalar bu platformların işleyişini doğrudan belirlemektedir. Bu platformlar sadece iç politika unsuru değil, aynı zamanda uluslararası ilişkiler ve diplomasi alanlarında yeni bir siyasal araç haline gelmeye başlamıştır. Örneğin, ABD Başkanı Donald Trump'ın 2018 Kasım ayında İran ile ilgili "Yaptırımlar Geliyor!" adlı paylaşımı ve buna karşılık İran Devrim Muhafızları Kudüs Gücü Komutanı Kasım Süleymani'nin Instagram üzerinden "Sana Karşı Duracağım" mesajıyla yanıt vermesi, dijital diplomasinin ulaştığı boyutu göstermesi açısından dikkat çekicidir (Yeni Asya, 2018).

Türkiye'de 7253 Sayılı Kanun ile 5651 sayılı kanunda yapılan değişiklikler, sosyal medya platformlarına yeni yasal yükümlülükler ve denetim mekanizmaları getirmiştir (Resmi gazete, 2020). Güvenlik perspektifinden bakıldığında, platformların herkese açık erişim özelliği terör örgütlerinin bu mecralarda propaganda yapmasına zemin hazırlamaktadır. Terör örgütleri, bu mecralarda görüşlerini kriminalize etmeden marjinal bir grup kisvesi altında saklayabilmektedir. Ses, görüntü ve metin paylaşımlarıyla sempatzan devşirmeyi ve kitleleri kendi ideolojilerine yönlendirmeyi amaçlamaktadır (Kartal, 2018, s.57).

Sonuç olarak, dijitalleşen dünyada dezenformasyon olgusu devlet güvenliği açısından mücadele edilmesi gereken en temel tehditlerden biri haline gelmiştir. "Darbelerin ve toplumsal hareketlerin temeli dezenformasyon ile atılmaktadır" tespiti, bu tehdidin ciddiyetini ortaya koymaktadır (Zengin vd., 2023, s. 17). Devletin operasyonel güvenliği açısından, özellikle güvenlik personelinin sosyal medya paylaşımları üzerinden konum veya stratejik kabiliyetlerini ifşa etme riski, harekât gizliliğini tehlikeye atabilmektedir. Bu nedenle, kamu kurumlarının sosyal medya üzerinden doğru bilgiyi zamanında paylaşması; kriz, savaş veya siber saldırı durumlarında oluşabilecek bilgi kirliliğinin önüne geçilmesi açısından stratejik bir öneme sahiptir. Sosyal medya, devletin hem yasal çerçevede denetlemesi gereken bir alan hem de toplum güvenliğini korumak adına aktif ve doğru kullanması gereken bir iletişim aracıdır.

1.4.5. Sosyal Medya-Kamu Güvenliği Etkileşimi

Sosyal medya platformlarının sunduğu hızlı haber akış özelliği, toplumsal olayların kullanıcılar arasında çok kısa sürede yayılmasını sağlayarak kamu hizmetlerinin yerine getirilmesinde yeni bir şeffaflık düzeyi oluşturmuştur. Bu

mecralar; kamu hizmetlerinin duyurulması, bilgilendirme faaliyetleri ve kurumsal imaj yönetimi gibi alanlarda etkili bir araç olarak kullanılmaktadır. Sosyal medyaya yansıyan eleştiriler ve olumsuz haberler, kamu hizmetlerinin sunumunda iyileştirmelere gidilmesini sağlayarak hizmet kalitesini artırabilmektedir (Yağmurlu, 2011). Ayrıca sosyal medyaya yansıyan toplumda infial oluşturan görüntüler üzerinden oluşturulan kamuoyu baskısı, adalet mekanizmasının hızlanmasına ve toplumsal taleplerin daha hızlı karşılık bulmasına zemin hazırlamaktadır (Sarioğlu, 2020, s.313). Devletin kamu düzenini sağlaması, kamu güvenliğini tesis etme görevlerinin yanında kamu yönetimini sorunsuz şekilde sağlama görevi de bulunmaktadır. 1980li yıllardan sonra toplumsal, teknolojik, ekonomik, kültürel birçok dünya devletleri arasındaki etkileşim devlet mekanizmasının kamu yönetimi alanında kendini reformize etmesi ihtiyacını doğurmaktadır. Merkezde kamuyu yönlendiren devlet, zamanla yerini başka önelere terk ettiği görülmektedir. Bu noktada yapılan yapısal reformlar neticesinde devlet, sonuç odaklı daha işlevsel, hızlı, pratik , güçlü, insanı merkeze alan kamu hizmetlerinin oluşturulması noktasına erişebilecektir. Kamu mal ve hizmetlerini üretme üretme noktasında halkın katılımı, açıklık, örgütlü yapıların oluşması, şeffaflık, hesap verilebilirlik gibi ilkelerin yer aldığı reformlarla yeni kamu yönetimi evrilmektedir. Türkiye bu noktada yapmış olduğu reformlar ile 200’li yıllar sonrasında önceden tespit edilemeyen ve beklenmeyen krizlere karşı daha dayanıklı duruma gelmiştir (Börklüoğlu ve Coşkun, 2019). Bu noktada Türkiye’de Cumhurbaşkanlığı bünyesinde faaliyet gösteren politika kurulları, hükümet politikalarının oluşturulması, devlet kurumlarının faaliyetlerinin izlenmesi ve yönlendirilmesi gibi kritik görevler üstlenmektedir. Bu kurullar Cumhurbaşkanına doğrudan bağlı olup, başkan ve üyelerinin Cumhurbaşkanınca atanması ile bütçelerinin Cumhurbaşkanlığı bütçesinden karşılanması nedeniyle yürütme organı içinde güçlü bir konuma sahiptir. Özellikle Cumhurbaşkanlığı İletişim Merkezi yapısıyla vatandaş ile devlet arasındaki bağ güçlendirilmiştir. Yine Türkiye’de devletin kamu kurum ve kuruluşlarının sosyal medya hesapları açmasıyla vatandaşların yorumlarına geri dönüş sağlanması, kriz ve afet anlarında bilgilendirici paylaşımlar, dezenformasyonla mücadele noktasında vatandaş-devlet arasındaki güvenin korunmasına katkı sağlamış, kamu kurum ve kuruluşların yönetiminde daha şeffaf, hesap verilebilir, açık, katılımcı, yapısı güçlendirilmiştir. Kamu yönetiminde kalıcı reformların sağlanmasında sosyal medya, katkı sunan yardımcı etkindir.

Sosyal Medyaya yansıyan yargılamaya konu olan olayların tüm yönleri netleşmeden dijital mecralarda oluşan genel algı, yargı tarafsızlığı ilkesini, masumiyet karinesini ve adil yargılanma hakkını zedeleme potansiyeline sahiptir. Örneğin, Türkiye’de Ayşegül Terzi davasında olduğu gibi, sosyal medya platformu X üzerinden yürütülen gündem çalışmalarının yargı organlarının kararları üzerinde etkili olduğuna ve adalet duygusunu tatmin etmeye yönelik uygulamaların geliştiğine dair veriler mevcuttur (Ulukaya, 2020 s.3). Bununla birlikte sosyal medya; kişisel verilerin hukuka aykırı paylaşımı, hakaret, iftira, tehdit ve dolandırıcılık gibi kamu güvenliğini tehdit eden suçların işlenmesine de aracılık edebilmektedir. Kimliği belirsiz hesaplar üzerinden yürütülen nefret söylemleri, şantaj ve siber zorbalık gibi eylemler, bu platformların suç mahalli olarak kullanılabilmesine neden olmaktadır (İletişim Bakanlığı, 2020).

Küreselleşen ve teknolojiyle iç içe geçen bu çağda sosyal medya, suçun öğrenilmesi ve yaygınlaşması gibi olumsuz durumların yanı sıra yalan bilginin (dezenformasyonun) hızla dolaşıma girmesine de neden olmaktadır. Teyit edilmemiş içeriklerin milyonlarca kişiyle etkileşime girmesi, özellikle kriz ve kaos dönemlerinde toplumu manipüle ederek paniğe sevk edebilmekte ve ciddi güvenlik riskleri doğurabilmektedir (Zengin vd., s.13). Bu bağlamda, kamu kurumlarının sosyal medyayı aktif ve doğru bilgiyle kullanması; doğal afetler, depremler veya kriz anlarında bilgi kirliliğini önlemek adına hayati önem taşımaktadır (Zengin vd.,). Nihayetinde sosyal medya, hem suç potansiyelini barındıran bir mecra hem de kamu güvenliğini tesis etmek için devlet ile vatandaş arasında köprü kuran çift yönlü, stratejik bir araç niteliğindedir.

II. BÖLÜM

SOSYAL MEDYANIN DEVLET VE KAMU GÜVENLİĞİNE ETKİSİ: TEHDİTLER VE YASAL DÜZENLEMELER

2.1. Kamu Güvenliği Açısından Sosyal Medyada İşlenen Suçlar

Geleneksel dönemde güvenlik anlayışı büyük ölçüde askeri tehditler ve savaşlarla sınırlı tutulurken, günümüzde bu kavram bireylerin ve toplumların günlük yaşamının neredeyse her alanına nüfuz etmiş durumdadır. Küreselleşme süreciyle birlikte ortaya çıkan yeni riskler, toplumsal değişimler ve artan ihtiyaçlar, güvenlik tanımının sürekli olarak yeniden şekillenmesini ve genişlemesini zorunlu kılmaktadır (Tirab, 2017).

Teknolojinin hızlı ilerleyişi, bireylere ve kurumlara büyük kolaylıklar sunmakla birlikte, aynı zamanda çeşitli risk ve tehditleri de beraberinde getirmektedir. Bu tehditler, ulusal kritik altyapılara, ekonomik yapıya ve genel olarak ulusal güvenliğe ağır hasarlar verebilecek niteliktedir. Özellikle siber saldırıların klasik biçimleri arasında virüsler, Truva atları, hizmet dışı bırakma (DoS) saldırıları, aldatma teknikleri, mahremiyet ve gizlilik ihlalleri, yetkisiz erişimler, yemleme (phishing) ve spam gibi unsurlar öne çıkmaktadır (Yılmaz ve Salcan, 2008).

Sosyal medya platformları, siyasal eylemliliği kökten değiştirmiş durumdadır. Beğenme, yeniden paylaşma (re tweet) ya da etiketleme (mention) gibi basit etkileşimler, geleneksel siyasette herhangi bir karşılığı olmayan yeniliklerdir. Yirmi yıl öncesine kadar siyasete katılmak genellikle bir partiye veya sivil toplum örgütüne üye olmayı gerektirirken, bugün insanlar yalnızca cep telefonları aracılığıyla,

ek bir araca ihtiyaç duymadan siyasal alanda etkin rol alabilmektedir. Bu tür düşük eforlu internet tabanlı eylemler –ki bunlara mikro-aktivizm de denilebilir– bazen hükümetleri hazırlıksız yakalayan büyük ölçekli sürpriz hareketlere dönüşebilmekte ve beklenmedik siyasal sonuçlar doğurabilmektedir (Margetts, 2019).

Başlangıçta sosyal medya, Arap Baharı gibi kitlesel toplumsal hareketlerin örgütlenmesinde güçlü bir araç olarak öne çıkarken, zamanla bu rol yerini seçim süreçlerinin manipüle edilmesine bırakmıştır. Özellikle ABD'deki 2016 başkanlık seçimleri ile Birleşik Krallık'taki Brexit referandumunda, Twitter ve Facebook gibi platformlar üzerinden sistematik müdahalelerin gerçekleştiği belgelenmiştir. Bu müdahaleler, veri odaklı hedefleme ve dezenformasyon stratejileriyle demokratik süreçleri etkileyecek nitelikte olmuştur (Cadwalladr, 2017; Nielsen, 2018).

2.1.1. Nitelikli Dolandırıcılık ve Veri Güvenliği

Türk Ceza Kanunu'nda dolandırıcılık suçu, hileli davranışlar yoluyla bir kişiyi yanıltarak onun ya da bir başkasının zararına, failin kendisine veya üçüncü bir kişiye haksız yarar sağlaması şeklinde tanımlanmıştır (TCK m. 157). Bu suç, temel olarak aldatma unsuru üzerine kuruludur ve cezai yaptırımını bir yıldan beş yıla kadar hapis ile beş bin güne kadar adli para cezasıdır.

Tümerkan'a (1987) göre dolandırıcılık kavramı iki boyutta ele alınabilir: Geniş anlamda, bir kimsenin herhangi bir hileli yöntemle kandırılarak malvarlığı üzerinde zarara uğratılmasıdır. Dar anlamda ise, kanunda açıkça öngörülen aldatma unsurlarının gerçekleştirilmesiyle, bir kişinin zararına başkasına haksız yarar sağlanması olarak nitelendirilir.

Teknolojinin hızlı ilerlemesiyle birlikte nitelikli dolandırıcılık suçlarında hile aracı olarak bilişim sistemleri –yani bilgileri otomatik işleyen cihazlar ve yazılımlar– giderek daha fazla tercih edilmektedir. Banka kartları, POS cihazları, cep telefonları gibi manyetik veya elektronik veri taşıyan araçlar, bu sistemler aracılığıyla otomatik olarak işlenerek suçun işlenmesini oldukça kolaylaştırmaktadır. Bu nedenle Türk Ceza Kanunu'nda (TCK m. 158). bilişim sistemlerinin araç olarak kullanılması, cezayı ağırlaştıran özel bir neden olarak düzenlenmiştir (Korkmaz, 2020).

Nitelikli dolandırıcılığın temelinde, çeşitli hile yöntemleri veya bireylerin zayıf yönlerini istismar ederek maddi kazanç elde etmek yatmaktadır. Bu tür eylemler mağdur sayısını artırırken, ülke ekonomisine de önemli zararlar vermektedir.

Dolayısıyla ekonomik suçlarla mücadelede korunmak istenen yalnızca bireysel mağdurlar değil, aynı zamanda ekonomik düzenin sağlıklı işleyiştir. Bu suçlar rekabetçi piyasa koşullarını bozmakta, vergi kayıplarına yol açmakta, gelir dağılımı adaletini zedelemekte, kayıt dışı ekonomiyi teşvik etmekte ve ticari hayatın güvenilirliğini sarsmaktadır. Bu bağlamda ekonomik suçlarla etkin mücadele, ulusal ekonomi için vazgeçilmez bir öneme sahiptir (EGM-KOMDB, 2012).

Teknolojinin hızla yayılmasıyla kişisel verilerin gizliliği ve güvenliği, bireyler ve kurumlar için vazgeçilmez bir öncelik olmuştur. Günlük hayatın ayrılmaz parçası haline gelen internet, akıllı telefon uygulamaları, sosyal ağlar ve diğer dijital araçlar, büyük miktarda kişisel bilginin kolayca toplanıp işlenmesine olanak tanırken, bu süreçte ciddi güvenlik açıkları da yaratmaktadır. Özellikle veri sızıntıları, kötü amaçlı yazılımlar, phishing gibi kandırma saldırıları ve sosyal mühendislik yöntemleri, kişisel veri güvenliğini doğrudan tehdit eden başlıca unsurlardır. Bu tür riskler, kullanıcıların farkındalık düzeyini de doğrudan etkilemekte ve korunma mekanizmalarının güçlendirilmesini zorunlu kılmaktadır (Çetin, 2014, s. 5).

Dijital ortamlarda veri güvenliği ihlalleri, kişisel bilgilerin korunmasını en ciddi şekilde riske atan unsurların başında gelmektedir. Bu ihlaller genellikle kötü niyetli kişiler veya hackerlerin sistemlere izinsiz giriş yaparak hassas verilere ulaşmasıyla meydana gelir. Örneğin bir veri tabanı korsanlığı (database breach) durumunda kullanıcıların kişisel bilgileri çalınabilir, ifşa edilebilir ya da değiştirilebilir. Bu tür olaylar, finansal detaylar, sağlık kayıtları, sosyal güvenlik numaraları gibi son derece hassas verilerin kötü niyetli kişiler tarafından istismar edilmesine zemin hazırlar (Scott, 2019; Tchakounté vd., 2020).

Benzer biçimde kötü niyetli yazılımlar da kişisel veri güvenliği için büyük bir tehlike oluşturur. Virüsler, Truva atları, solucanlar, casus yazılımlar (spyware) ve fidye yazılımları (ransomware) gibi malware türleri, kullanıcı cihazlarına sızarak verileri gizlice izleyebilir, çalabilir veya manipüle edebilir. Bu yazılımlar çoğu zaman fark edilmeden çalışır; böylece bireyler verilerinin ele geçirildiğini uzun süre anlamayabilir. Phishing saldırıları ise kullanıcıları doğrudan kandırmaya yönelik etkili bir yöntemdir. Saldırganlar, sahte web siteleri, e-postalar veya mesajlar yoluyla mağdurları yanıltarak kimlik bilgileri, banka hesap detayları gibi kişisel verileri elde etmeyi amaçlar. Kullanıcılar örneğin güvenilir bir banka sayfası sandıkları bir sitede

yönlendirilerek giriş bilgilerini girer ve bu sayede dolandırıcıların eline düşebilir (Alpaslan ve Delibalta, 2025 s.199)

Bir diğer kritik tehdit ise sosyal mühendisliktir. Bu yaklaşımda saldırganlar, teknik araçlardan ziyade insan psikolojisini hedef alır; insanları manipüle ederek gizli bilgileri açığa çıkarmayı başarır. Telefon dolandırıcılığı, yüz yüze veya uzaktan kişisel bilgi talepleri gibi taktikler sıkça kullanılır. Saldırganlar güven oluşturmak, dikkat dağıtmak veya aciliyet hissi yaratmak amacıyla psikolojik oyunlar, yalan hikayeler ve kandırma teknikleri uygular (Akca, 2016).

2.1.2. Tehdit ve Şantaj Suçları

Şantaj kelimesi, Türkçeye Fransızca "chantage" sözcüğünden geçmiş olup, kökeni Fransız argosunda "faire chanter" (konuşturmak, tehditle söyletmek) ifadesine dayanmaktadır. Türk Dil Kurumu'nun Güncel Türkçe Sözlük 'ünde şantaj, "Herhangi bir çıkar sağlamak amacıyla bir kimseyi, kendisiyle ilgili lekeleyici veya gözden düşürücü bir haberi yayma ya da açığa vurma tehdidiyle korkutma" şeklinde tanımlanmaktadır (Türk Dil Kurumu, 2022). Suç unsuru taşıdığında ise şantaj, 5237 sayılı Türk Ceza Kanunu'nda (TCK) "Hürriyete Karşı Suçlar" başlığı altında, ikinci kitabın ikinci kısmının yedinci bölümünde Madde 107 ile düzenlenmiştir. Bu madde, bireyin irade özgürlüğünü ve şeref/saygınlığını tehdit yoluyla ihlal eden eylemleri cezalandırmayı amaçlamaktadır.

Şantaj suçu, Türk Ceza Kanunu'nda hürriyete karşı suçlar kategorisinde yer alır. Hürriyet, bireyin bir eylemi yapma ya da yapmama kararını tamamen özgür iradesiyle verebilmesi olarak tanımlanabilir; ancak bu özgürlük, kişinin kendisine veya başkalarına zarar vermemesi koşuluyla sınırlıdır (Bilge, 2019, s. 131).

Şantaj, genel tehdit suçunun (TCK m. 106) özel ve nitelikli bir biçimi olarak kabul edilir (Hafızoğulları ve Özen, 2010, s. 171). Bu suçta fail, mağduru tehdit ederek belirli bir maddi veya manevi yarar sağlamayı amaçlar. Dolayısıyla şantaj suçuyla öncelikle korunan hukuki değer, bireyin irade özgürlüğü ve hürriyetidir; aynı zamanda tehdit unsuruyla birlikte haksız çıkar hedeflendiği için malvarlığı hakları da dolaylı olarak korunmaktadır (Bilge, 2019, s. 135).

Günümüz gençleri, günlük yaşamlarının büyük bir bölümünü sosyal medya olarak bilinen sanal platformlarda geçirmektedir. Bu mecralar, eğitim fırsatları, ticari etkinlikler ve sosyal etkileşim gibi pek çok olumlu katkı sunmakla birlikte, aynı

zamanda suç unsurlarının işlendiği riskli bir alan haline gelebilmektedir. Özellikle sosyal medya üzerinden işlenen şantaj suçları, genç bireyleri sıklıkla mağdur konumuna düşürmektedir. Sanal şantajda fail, mağdura karşı çeşitli dijital eylemlerle –sosyal medyada paylaşım tehdidi, görüntülü arama yoluyla baskı, mesaj gönderme gibi– zarar verme potansiyeli taşır. Bu tür suçlarda cinsellik odaklı unsurlar belirgin bir yer tutar; cinsel içerikli mesajlaşmalar, görüntülü görüşmeler, ses kayıtları veya benzeri elektronik veriler –bazen mağdurun rızasıyla, bazen rızası dışında– kaydedilerek ilerleyen aşamalarda şantaj malzemesi olarak kullanılabilir (Erdoğan ve Kaşlı, 2022, s. 149).

İnternetin ve teknolojik araçların hızla yaygınlaşmasıyla sanal şantaj suçu, her geçen gün daha büyük bir sorun haline gelmektedir. Özellikle gençler, sosyal medya gibi sanal ortamlarda tanımadıkları kişilerle arkadaşlık kurmamak, profillerinde uygun gizlilik ayarlarını uygulamak ve kişisel verilerini paylaşırken son derece dikkatli olmak gibi konularda bilinçlendirilmelidir. Bu tür önleyici farkındalık çalışmaları, potansiyel mağduriyetlerin önüne geçmede kritik öneme sahiptir. Mağduriyet yaşanması durumunda ise gençlerin durumu derhal yetkili makamlara (Örneğin Emniyet Siber Suçlar Birimi veya savcılık) ihbar etmesi teşvik edilmelidir. Bu süreçte şantaj amacıyla kullanılan mesajlaşmalar, arama kayıtları, görüntülü görüşmeler ve benzeri dijital delillerin korunarak toplanması büyük önem taşır; böylece suçun aydınlatılması ve failin tespiti kolaylaşır (Erdoğan ve Kaşlı, 2022, s. 149).

2.1.3. Halkı Kin ve Nefrete Teşvik Etme

Türk Dil Kurumu'nun Güncel Türkçe Sözlük 'ünde "nefret" kelimesi, "1. Bir kimsenin kötülüğünü, mutsuzluğunu istemeye yönelik duygu, 2. Tiksiniş, tiksinti" biçiminde tanımlanırken; "söylem" ise "1. Söyleyiş, söyleniş, sesletim, telaffuz, 2. Kalıplaşmış, klişeleşmiş söz, ifade, 3. Bir veya birçok cümleden oluşan, başı ve sonu olan bildiri, tez" olarak açıklanmaktadır. Nefret, temelde herhangi bir kişiye ya da nesneye karşı hissedilebilen ve insan doğasında var olan bir duygudur. Ancak bu çalışma özelinde, nefret söylemi kavramı çerçevesinde ele alınan nefret; bireylerin değiştirilemez özelliklerine –ırk, milliyet, etnik köken, dini inanç, cinsiyet, cinsel yönelim gibi unsurlara– yani doğrudan "varoluşlarına ve varoluş biçimlerine" yönelik bir düşmanlıktır. Bu tür nefret, salt bireysel bir duygu olmanın ötesinde, belirli bir ideolojinin parçası olarak sistematik bir nitelik kazanır (Güranlıoğlu, 2016).

Nefret söylemi kavramı konusunda uluslararası düzeyde tam bir uzlaşa bulunmamakla birlikte, genel olarak belirli bir gruba mensubiyetleri nedeniyle insanları aşağılayan, dışlayan veya hedef alan iletişim biçimleri olarak tanımlanabilmektedir (Sardini, 2018). Bu kavramın kapsamı oldukça esnektir; bazı yaklaşımlarda manipülasyona açık geniş bir çerçeve çizilirken, diğerlerinde söylemin doğrudan zarara, şiddete veya ayrımcılığa yol açma potansiyeli taşıyan "tehlikeli söylem" veya "korku söylemi" olarak daha dar bir şekilde sınırlandırılır (Ireton ve Posetti, 2018).

Nefret söylemi tipik olarak ayrımcı, korkutucu ve toplumsal olarak onaylanmayan içerikler barındırır; önyargılarla motive edilmiş bireylerin nefret dolu ifadeleri şeklinde kendini gösterir ve bazen tahrik edici unsurlar da içerir (Sezgin, 2017). Avrupa Konseyi Bakanlar Komitesi'nin 30 Ekim 1997 tarihli R(97)20 sayılı Tavsiye Kararı'nda nefret söylemi; ırkçılık, yabancı düşmanlığı, antisemitizm, azınlıklara, göçmenlere veya göçmen kökenlilere yönelik saldırgan milliyetçilik, etnik merkezcilik, ayrımcılık ve hoşgörüsüzlüğe dayalı diğer nefret biçimlerini yayan, kışkırtan, teşvik eden ya da meşrulaştıran her türlü ifade biçimi olarak tanımlanmıştır (Europ, 2019).

Geleneksel medyanın nefret söylemini üretme ve yayma biçimiyle, günlük hayatımızın ayrılmaz parçası haline gelen sosyal medyadaki nefret söylemi arasında güçlü bir ilişki gözlemlenmektedir. Son 20 yılda iletişim teknolojilerindeki devasa ilerlemeler, internetin hızla yaygınlaşmasını ve yaşamımızın merkezine yerleşmesini sağlamıştır. Artık bireyler, geleneksel medya kaynaklarından edindikleri kadar –hatta daha fazla– bilgiyi sosyal medya platformlarından edinmekte; bu mecralardaki yoğun ve hızlı bilgi akışı, toplumun algılarını, tutumlarını ve değer yargılarını doğrudan etkilemektedir. Sosyal medyanın geleneksel medyadan en belirgin farkı, zaman ve mekân kısıtlamalarından bağımsız olması, tek yönlü iletişim modelini kırarak etkileşimli bir yapı sunmasıdır. Herkesin erişebildiği bu ortam, internetin doğası gereği eşitlikçi ve demokratik bir iletişim alanı yaratır; çünkü sınırları aşma, mesafeleri ortadan kaldırma ve gerçek dünyadaki engelleri yok etme kapasitesine sahiptir (Banks, 2014, s. 33).

İnternet erişimi olan bireyler, sosyal medya platformları sayesinde mesajlarını çok kısa sürede milyonlarca kullanıcıya ulaştırabilmektedir. Bu özellik, içerik üretme ve yayma süreçlerini demokratikleştirmiş ve toplumda köklü değişimlere yol açmıştır.

Sosyal medya, kullanıcılara görüşlerini özgürce ifade edebilecekleri erişilebilir bir alan sunarak iletişimde büyük fırsatlar yaratmaktadır. Ancak bu fırsatlar, aynı zamanda ciddi zorlukları da beraberinde getirmektedir. Bunlardan en önemlisi, ifade özgürlüğü ile bireylerin onur ve saygınlığının korunması arasındaki hassas dengenin sağlanmasıdır; bu denge çeşitli biçimlerde sınıanabilmektedir. Nefret söylemi, bu tür zorlukların en tipik ve yaygın örneklerinden biridir (Silva vd., 2016). Üstelik nefret söylemi içerikleri, açıkça kin veya nefret ifadeleri içermeyen de oluşturulabildiği için tespit edilmesi oldukça güç olabilmektedir (Sezgin, 2017).

2.1.4. Veri İhlalleri: Cambridge Analytica Örneği

2021 yılının üçüncü çeyreği itibarıyla yaklaşık 2,91 milyar aylık aktif kullanıcıya sahip olan Facebook, küresel ölçekte en büyük sosyal ağ platformu konumunu sürdürmektedir (Statista 2021). Platform, bireysel kullanıcıların yanı sıra özel sektör kuruluşları ve kamu kurumlarının halkla ilişkiler faaliyetlerinde sıkça tercih ettiği bir mecra haline gelmiştir; bu sayede hizmet sağlayıcılarla tüketiciler arasında etkili bir sanal köprü işlevi görmektedir. Dünya nüfusunun neredeyse %40'ına yakın bir kesimi aktif Facebook kullanıcısıdır; ayrıca Facebook üyesi olmayan birçok kişi de şirketin sahibi olduğu Instagram gibi diğer büyük uygulamalar aracılığıyla Meta ekosistemine dahil edilmiştir. Bu durum, Facebook'u milyarlarca bireyin kişisel verilerini depolayan ve yöneten önde gelen teknoloji şirketlerinden biri yapmaktadır. Dolayısıyla bu devasa veri havuzunun nasıl saklandığı, işlendiği ve korunduğu konusu, özellikle Cambridge Analytica gibi skandallar ışığında dikkat çekici bir araştırma alanıdır (Aksoy ve Türkölmez, 2020, s. 48).

Dijital iletişim ortamlarında sosyal medya platformlarının ikili yapısı belirgindir: Bir yandan bireyleri birbirine bağlayan, bilgi paylaşımını kolaylaştıran araçlar olarak fayda sağlarken; diğer yandan gizlilik ihlalleri ve etik sorunlar gibi ciddi riskler yaratmaktadır. Bu risklerin en çarpıcı örneklerinden biri, 2018'de patlak veren Facebook-Cambridge Analytica skandalıdır; olay, platformlarda toplanan kişisel verilerin nasıl siyasi manipülasyon amacıyla istismar edilebileceğini gözler önüne sermiştir. Skandalın detaylarına bakıldığında, Cambridge Analytica'nın 2014-2016 döneminde 87 milyon Facebook kullanıcısının psikografik profillerini (kişilik özellikleri, siyasi eğilimler vb.) bir uygulama üzerinden toplayarak analiz ettiği ve bu verileri 2016 ABD başkanlık seçimlerinde hedefli reklam ve seçmen etkileme stratejilerinde kullandığı ortaya çıkmıştır. Bu olay, sosyal medya kullanıcılarının

mahremiyet algısını derinden sarsmış ve dijital etik tartışmalarında önemli bir dönüm noktası olmuştur; özellikle platformların veri koruma sorumluluğu ve kullanıcı güvenli açısından öğretici bir nitelik taşır (Brown, 2020, s. 1).

Cambridge Analytica Veri Skandalı, kişisel verilerin izinsiz toplanması ve kötüye kullanımı yoluyla gerçekleştirilen ciddi bir mahremiyet ihlali olarak nitelendirilebilir; bu olay, Web 2.0 dönemiyle birlikte yaygınlaşan açık erişim ve paylaşım kültürünü de olumsuz etkilemiştir. Skandal, demokrasi teorisi ve siyaset bilimi açısından yeni tartışmaları tetiklemiş; demokratik süreçler, siyasal popülizm, seçim güvenliği, siyaset psikolojisi ve oy verme davranışları gibi alanlarda derin analizlere kapı aralamıştır. Öte yandan olay, sosyal medya kullanıcılarını platformların veri toplama pratiklerini sorgulamaya yöneltmiş ve toplanan bilgilerin yalnızca reklam hedeflemesi veya kullanıcı deneyimi iyileştirmesi için değil, aynı zamanda geniş ölçekli siyasi manipülasyonlarda da kullanılabileceğini gözler önüne sermiştir. Facebook açısından en ağır sonuçlardan biri, çok sayıda kullanıcının hesaplarını kalıcı olarak silmesi olmuştur. Dijital iletişim etiği bağlamında incelendiğinde, sosyal ağlarda dürüstlük ve etik kurallara uyulmamasının, sosyal medya ile siyaset arasındaki sınırların bulanıklaşmasına yol açtığı söylenebilir. Bu tür sorunlar, siyasette şeffaflığın azalmasına ve demokratik toplum anlayışının aşınmasına katkıda bulunarak dijital çağın etik krizlerini hızlandırmaktadır (Işık, 2022).

2.2. Sosyal Medyada Algı Yönetimi ve Sebepleri

Algı yönetimi, yabancıların tutumlarını ve tarafsız düşünme kapasitelerini etkilemeye yönelik her türlü girişimi kapsayan geniş bir kavramdır. Bu süreç, kamu diplomasisi, psikolojik operasyonlar, kamu bilgilendirme, aldatma ve gizli eylemler gibi birbirine iç içe geçmiş faaliyetleri içerir. Halkla ilişkiler disiplininde 1980'li yıllardan itibaren kullanılmaya başlanan algı yönetimi, kamu diplomasisi bağlamında bir imaj oluşturma ve itibar yönetimi süreci olarak değerlendirilmektedir (Yakın, 2004, s. 87).

Algı yönetimi kavramı, ilk kez ABD Savunma Bakanlığı tarafından sistematik olarak ele alınmış ve tanımlanmıştır. ABD Savunma Bakanlığı'na göre algı yönetimi; hedef kitlenin duygu, düşünce ve motivasyonlarını etkilemek amacıyla seçilmiş bilgilerin vurgulanması, gizlenmesi veya inkâr edilmesi yoluyla

gerçekleştirilen stratejik bir süreçtir. Bu süreçte, hedef kitlenin istihbarat sistemleri ve liderlerinin karar alma mekanizmaları etkilenecek, algı yönetimi uygulayan tarafın amaçlarına uygun davranışlar ortaya çıkarılması hedeflenir (Hügöl, 2011, s. 3). Nye’a göre ise algı yönetimi, ikna ve propaganda tekniklerinin etkin bir şekilde kullanılmasından ibarettir. Hedef toplumun düşünce, duygu ve davranışlarını istenilen yönde değiştirebilmek için bu iki aracın ustaca devreye sokulması gerekmektedir. Bu süreçte inandırıcılık, hukuki meşruiyet, hedef kitlenin kültürel değerleri, yaşam tarzı, eğitim seviyesi ve bilginin güvenilirliği gibi unsurlar büyük önem taşımaktadır (Hügöl, 2011, s. 22-23).

Tarih boyunca devletler, amaçlarına ulaşmak ve kamuoyunu yönlendirmek için çeşitli algı yönetimi teknikleri uygulamışlardır. Çinliler, Hun, Göktürk ve Moğol imparatorluklarını iç çatışmaları kışkırtarak zayıflatma stratejisi izlemişlerdir. Moğol ordusu ise savaş alanına girmeden önce kendisini son derece güçlü ve yıkıcı bir güç olarak göstererek düşmanları psikolojik olarak etkisiz hale getirmeye çalışmıştır. Osmanlı Devleti ise fethedilen bölgelerde korku ve sindirme yerine hoşgörü ve adalet vurgusu yapan bir propaganda yaklaşımı benimsemiş; keşişler ve tüccarlar aracılığıyla bu algıyı yaymıştır. Tüm bu örnekler, algı yönetiminin tarihsel olarak kullanılan stratejik bir araç olduğunu göstermektedir (Özarslan, 2014, s. 32-33).

Algı yönetiminin tanımı ve yorumu, bireylerden devletlere, kurumlara göre değişiklik gösterir. Bu farklılık nedeniyle bazıları algı yönetimini hedef kitleyi kendi çıkarları doğrultusunda kandırma olarak görürken; diğerleri bunu amaçlara ulaşmak için kullanılan meşru bir iletişim disiplini olarak tanımlar. Bireyler veya gruplar, içgüdüsel olarak "öteki"ne karşı haklı çıkma, kendini kabul ettirme ve yönlendirme amacıyla bu yöntemi uygular. Siyasal partiler rakip partilerin oy potansiyelini düşürmek, iktidarlar muhalefeti zayıflatmak, muhalefet ise iktidarın gücünü kırmak için algı yönetiminden yararlanır (Tunç ve Atılğan, 2017, s. 229).

Algı yönetiminin başarılı olabilmesi için belirli temel kurallara uyulması gerekmektedir. Ali Saydam’ın çalışmasında bu kurallar on bir başlık altında toplanmıştır (Kazu, 2018, s. 39):

1. Hedef Kitlenin Değerlerine Uyuma: Her toplumun kendine özgü değer yargıları, gelenek ve görenekleri vardır. Algı yönetimi sürecinde bu değerlerle çatışmamak temel koşuldur.

2. Hedef Kitlenin Kültürüne Önem Verme: Evrensel bir yaklaşım yerine, hedef kitlenin milli ve yerel kültürel yapısına uygun hareket etmek başarıyı artırır.

3. Beklentilerin Üzerinde Yaklaşım Sergileme: Özellikle kriz dönemlerinde beklenmedik olumlu tutumlar, hem krizi yönetmede hem de ikna sürecinde etkili olmaktadır.

4. İnsanların Zihinlerini Karıştırmama: İletilen mesajın sade, anlaşılır ve akılda kalıcı olması gerekmektedir.

5. Sonuca Odaklanmak: İletişim sürecinde amaçtan sapmamak, istenilen sonuca ulaşmayı hızlandırır.

6. Ölçerek Yapmak: Algı yönetiminde her aşamada ölçüm ve değerlendirme yapılmalıdır.

7. Gerçeklere Dayanmak: Uzun süreli etki yaratabilmek için mesajın gerçek olaylara ve bilimsel verilere dayanması şarttır.

8. Tekrar Etme: Kilit mesajların belirli aralıklarla tekrar edilmesi, hedef kitlenin belleğinde kalıcılığı sağlar.

9. Farklılaşmaları Yönetebilmek: Farklılaşma, diğer kurallarla uyumlu olduğu sürece etkili bir araç haline gelebilir.

10. Görselliği Doğru Yönetmek: Görsel unsurlar, işitsel unsurlardan daha güçlü etki yaratır. Jest, mimik ve davranışlar inandırıcılığı doğrudan etkiler.

11. Düşüncelerden Ziyade Duygulara Seslenmek: Hedef kitlenin duygusal dünyasını iyi tanımak, algı yönetiminin en kritik unsurlarından biridir.

Günümüzde algı yönetimi, bireylerin yaşamlarını şekillendiren ve dönüştüren güçlü bir araç haline gelmiştir. Bazı araştırmacılar bunu “kandırma sanatı” olarak nitelendirse de, asıl önemli olan bu yeteneğin etik sınırlar içinde ve bireylere fayda sağlayacak şekilde kullanılmasıdır. Algı yönetimi, hem dış politikada diğer ülkeleri ulusal çıkarlar doğrultusunda hareket etmeye ikna etmek hem de iç politikada seçmenleri etkilemek açısından stratejik bir öneme sahiptir. Bu araçları ustaca kullanan aktörlerin, siyasi, askeri ve kamusal alanda önemli başarılar elde etme potansiyeli taşıdığı söylenebilir (Kazu, 2018, s. 33). Algı yönetiminin temel amaçları şu şekilde sıralanabilir (Kazu, 2018, s. 32):

- Hedef kitlenin istenilen yönde düşünmesini ve inanmasını sağlamak,
- Kitleleri belirli hedefler doğrultusunda yönlendirmek,
- Kurum ve kuruluşların itibarını güçlendirmek,
- Kitlelerin duygu ve düşüncelerini etkilemek,
- Kamuoyu oluşturmak ve kamuoyu desteğini kazanmak,
- Düşman ve dış güçlere karşı güvenlik önlemi almak.

Kişilerin algısını şekillendiren temel unsur, dış dünyayı ve nesneleri bize yansıyan haliyle yorumlamamızdır. Algı sürecinde birey iki tür gerçeklikle karşılaşır: Birincisi kendi gözlemleriyle ulaştığı gerçeklik, ikincisi ise kitle iletişim araçları – özellikle medya– yoluyla sunulan gerçekliktir. Medya tarafından aktarılan enformasyonların, bireyin kendi algılarıyla edindiği bilgiye kıyasla zihnindeki imgeleri ve inandığı "sahte dünyayı" oluşturmadaki egemenliği oldukça dikkat çekicidir (Ceng, 2018, s. 668).

Günümüzde sosyal medya kanalları, algı yönetimi tekniklerinin en etkili şekilde uygulandığı alanlardan biri haline gelmiştir. Güçlü sosyal medya mecraları aracılığıyla hedef kitleye özel olarak tasarlanmış mesajlar iletilerek, bireyler belirli yönlere doğru yönlendirilmektedir. Bireyler algılama sürecinde kendi geçmiş deneyimleri, bilgi birikimleri ve mevcut şartlarla bilgiyi süzgeçten geçirirler. Bu nedenle aynı bilgi farklı kişiler tarafından farklı şekillerde algılanabilir. Bu noktada algı yönetimi stratejilerinin bilinçli ve sistematik uygulanması büyük önem taşımaktadır.

Toplumlari yönlendirme ve manipüle etme amacıyla tarih boyunca sıkça kullanılan dezenformasyon, sosyal medyanın ana akım medyayı geride bıraktığı günümüzde çok daha yaygın bir araç haline gelmiştir. İnternet ve sosyal medya platformları, bilginin üretimi ve yayılımında kritik bir rol oynarken; bugün bilgi kirliliği nedeniyle güvenilirlikleri sıkça sorgulanmaktadır. Çevrimiçi ortamlarda yanlış bilgiler gerçeklerden daha hızlı yayılmakta, kullanıcıların bilginin doğruluğunu ayırt etmesi giderek zorlaşmaktadır. Kamuoyunun fikirlerini olumlu veya olumsuz yönde etkilemek, inançlarını kendi çıkarları doğrultusunda değiştirmek amacıyla kitle iletişim araçları tarih boyunca propaganda aracı olarak kullanılmıştır. Dezenformasyon da aynı amaca hizmet eder; ancak gerçek dışı bilgi içermesi ve manipülasyon niyeti

taşıması nedeniyle genellikle "kara propaganda" olarak sınıflandırılır. Bu süreç, yanlışlıkla hatalı bilgi iletimi olan mis-enformasyondan farklıdır; dezenformasyon bilinçli olarak rakipleri zayıflatmak veya algıları yönetmek amacıyla gerçekleştirilir (Ayhan ve Erkan, 2018, s. 206).

Alan yazında dezenformasyon tanımlamalarının misenformasyona kıyasla daha net ve belirgin olduğu görülmektedir. Marwick ve Lewis (2017), sosyal medyada yayılan komplo teorilerini ve propaganda amaçlı içerikleri dezenformasyon kapsamında değerlendirmektedir. Fallis (2015), dezenformasyonu aldatıcı reklamlar, manipüle edilmiş fotoğraflar, sahte belgeler, düzmece web siteleri ve yanıltıcı haberler olarak geniş bir yelpazede özetlemektedir.

Ancak yalan haber (fake news) sorunu yalnızca bireysel kullanıcılar veya küçük gruplarla sınırlı değildir; ana akım medya kuruluşları, çok uluslu şirketler veya organize troller de dezenformasyon amacıyla bu tür içerikleri yayabilmektedir. Sosyal medya, günümüzün hızlı habercilik anlayışına göre haber üretilebilen bir ortam haline gelirken; aynı zamanda yalan haberlerin, yanlış bilgilerin ve söylentilerin en hızlı dolaştığı mecra konumuna gelmiştir (Ünal ve Taylan, 2017).

Sosyal medya kullanıcılarının paylaşımları, doğrulanmaya muhtaç içeriklerin özel hayatın gizliliği ihlali, nefret söylemi gibi etik sorunlara yol açması ve algı yönetimini kolaylaştırması bakımından tartışmalı bir alandır. Özellikle platformlardaki "hemen paylaşma" baskısı, genellikle teyit edilmemiş yalan veya yanlış bilgilerin hızla yayılmasına neden olur; bu da yeni medya ve yurttaş gazeteciliği pratiğinin en önemli etik ihlallerinden biri olan "teyitsiz paylaşım" sorununu ön plana çıkarır.

Medya, gerçekliğin belirli boyutlarını vurgulayarak, bazı boyutlarını ise bilinçli olarak karartarak veya değiştirerek kamuoyunu manipüle edebilir. Bu durum, literatürde "dezenformasyon" olarak adlandırılmaktadır. Manipüle edilmiş gerçekler, kısa sürede yalan olduğu ortaya çıkan sahte haberlerden daha tehlikelidir; çünkü daha kalıcı ve kışkırtıcı bir etki yaratır. Bu nedenle bireylerin kendilerine sunulan bilgilere eleştirel bir gözle yaklaşması ve zihinsel süzgeçlerden geçirmesi, manipülasyondan korunmada temel bir gerekliliktir (Utma, 2018, s. 2908-2911).

2.2.1. Dezenformasyon Faaliyetleri

Yanlış veya yanıltıcı bilgilerin yayılma amacı ve niteliğine göre farklı terimlerle adlandırılması yaygın bir yaklaşımdır. "Dezenformasyon", kasıtlı olarak yanlış veya yanıltıcı bilginin üretilmesi ve bu bilginin sistematik biçimde kamuoyuna yayılması sürecini ifade eder. Türk Dil Kurumu tarafından "bilgi çarpıtma" olarak tanımlanan dezenformasyon, bir kişi, topluluk, örgüt veya devlete zarar vermek amacıyla bilinçli olarak yanlış bilginin dolaşıma sokulmasıdır Karlova ve Fisher(2012) dezenformasyonu "zarar verme amacıyla oluşturulmuş ve yayılan bilgi" olarak nitelendirirken Avrupa Komisyonu (2018) ise bunu "kamuya zarar verme amacı taşıyan, kasıtlı olarak yanıltıcı veya tamamen sahte içerikler" şeklinde açıklamaktadır. Dezenformasyon yapan kişi, bilginin yanlışlığını bilerek kasten yayar; bu da onu tesadüfi hatalardan (misinformation) ayıran temel özelliktir (Dal ve Erdoğan, 2020, s. 4).

Yanlış bilgi bağlamında kullanılan bir diğer kavram "mezenformasyon"dur (misinformation). Dezenformasyondan farklı olarak burada kişiler paylaştıkları bilginin doğru olduğuna inanmakta ve zarar verme niyeti olmaksızın yaymaktadır. Kişisel bilgilerin çıkar sağlamak veya zarar vermek amacıyla kötü niyetle yayılması ise "malenformasyon" (malinformation) olarak adlandırılmaktadır (Wardle ve Derakhshan, 2017, s. 20). İletişim bilimleri açısından bu tür bilgilerin kullanımı, kişiler arası ilişkilerde dolaşan sıradan yanlışlardan çok daha ağır sonuçlara yol açabilmektedir. Bu çerçevede sahte haber (fake news), medyadaki haberleri taklit eden, kasıtlı olarak üretilmiş, genellikle tepki çekici, sansasyonel veya duygusal dil kullanan, insanları yanıltan ya da tamamen yanlış olan içerikler olarak tanımlanmaktadır. Yanlış bilgi ve haberlerin yayılması, iletişim devriminin bir sonucu gibi görünse de aslında tarihin her döneminde farklı araçlarla benzer propaganda ve manipülasyonlar yapılmıştır. Örneğin Roma döneminde Octavianus (sonradan Augustus), rakibi Antonius'un itibarını zedelemek için Kleopatra ile ilişkisini kullanarak bir karalama kampanyası başlatmıştır. Sikkeler üzerine yazılmış kısa ve keskin sloganlar –adeta "arkaik tweetler"– Antonius'u kadın avcısı bir sarhoş ve Kleopatra'nın kuklası olarak betimlemiştir. Bu kampanya başarılı olmuş ve Octavianus cumhuriyeti sonsuza dek değiştirerek ilk Roma İmparatoru olmuştur; böylece sahte haber ve dezenformasyon kullanarak siyasi sistemi "hack"lemiştir (Kaminska, 2017).



Şekil 11. Bilgi Kirliliğinin Türleri (Wardle ve Derakhshan, 2017, s. 20'den Türkçeye çevrilmiştir)

Bilgi kirliliğinin 3 türü, 3 aşaması ve 3 unsuru bulunmaktadır. Bilgi kirliliğinin 3 türü; Dezenformasyon, Misenformasyon ve Malinformasyondur. Bilgi kirliliğinin 3 aşaması ise ; Bilgi'nin oluşturulması, bilgi'nin üretilmesi, bilginin dağıtılmasıdır. Bilgi Kirliliğinin 3 unsuru ise Ajan, Mesaj ve Yorumlayıcıdır (Wardle ve Derakhshan, 2017, s.48).

Bilgi kirliliğinin 3 unsurundan biri Ajanlardır. Ajan; mesajı oluşturan kişi veya kişilerdir. Bilgiyi oluşturan ajanlar resmi yani istihbarat servisi elemanı haber kuruluşunda bir çalışan veya gayriresmi olabilir. Ajanların sahip olduğu motivasyonlar farklı olabilmektedir. Ajanların motivasyon çeşitleri; Finansal, Siyasal, Sosyal ve Psikolojik olabilmektedir (Wardle ve Derakhshan, 2017, s. 29). Ajanlardan diğeri troller ve bot hesaplardır. Troller; Sosyal medya platformlarında takma adla veya anonim bir kullanıcı adıyla profile sahip olan sosyal medya kullanıcılarına denmektedir. Bot hesaplar; bilgisayarların yönettiği kullanıcı yani gerçek kişilere dayanmayan hesaplardır. Troller, bot hesaplar gibi koordineli bir şekilde dezenformasyon oluşturabilmektedirler. Troller; botlardan farklı olarak bilginin doğruluğunu

araştırmak, gerçek bilgiye ulaşmak isteyen kullanıcıları hedef almaktadır. Genel olarak dezenformasyonun yayılma aşamalarının başlarında muhalifleri susturmak amacıyla anonim kullanıcı adları üzerinden koordineli saldırılar düzenleme, bu saldırılarla muhalif görüşleri bastırmak ve kendi doğrularını kullanıcılara kabul ettirmeye çalışma konularında etkilidirler. Bazı hükümetlerin kendi amaçlarını gerçekleştirmek amacıyla bot hesapları, troll orduları kurdukları ve bunları organize ettiği bilinmektedir. (Wardle ve Derakhshan, 2017).

Bilgi Kirliliğinin 2.Aşaması Mesajlardır. Verilmek istenen mesajı güçlü hale getiren ve geniş kitlelerce karşılık bulmasını sağlayan 4 özellik; Duygusal tepki uyandırması, güçlü bir anlatıya sahip olması, güçlü bir görsel bileşene sahip olması, mesajın sürekli tekrar edilmesidir (Wardle ve Derakhshan, 2017, ss 38-39).

Bilgi Kirliliğinin 3.Aşaması Yorumlayıcılar; Her birerinin mesajları farklı anlamlandırıp yorumladığı alıcıları ifade etmektedir. Anlamlandırma türüne göre farklılık göstermektedir. Hegemonik, Müzakereci, Muhalif olmak üzere 3 çeşit yorumlayıcı bulunmaktadır. Hegemonik Yorumlayıcı; Mesajı, olduğu şekliyle kabul eder. Müzakereci yorumlayıcı; Mesajın bazı kısımlarını kabul eder bazı kısımlarını reddeder. Muhalif Yorumlayıcı; Mesajı olduğu şekliyle reddeder. Paylaşılan her içeriğe yapılan yorum, beğeni, paylaşımlar içerik sahibi üzerinde dopamin salgısı etkisi oluşturmaktadır. Bu tür duygusal içerik paylaşımları yanlış bilgiye veya dezenformasyona hizmet edebilmektedir. (Wardle ve Derakhshan, 2017, s. 41).

Tarihsel perspektiften bakıldığında dezenformasyonun ilk örneklerinde, kasıtlı yanlış bilgilerin genellikle bilinmeyen devlet yetkilileri tarafından yayıldığı ve toplumda belirli tepkiler uyandırmanın hedeflendiği görülmektedir. Özellikle Soğuk Savaş yıllarında bu yöntem, istihbarat faaliyetleri ve propaganda savaşlarının ayrılmaz bir parçası haline gelmiştir. Rid (2020), bu dönemde dezenformasyonun siyasi rejimleri etkilemek üzere uygulanan "aktif önlemler" (active measures) kapsamında ele alındığını vurgular.

Zamanla dezenformasyon yalnızca devlet aktörleriyle sınırlı kalmamış; siyasi çıkar peşindeki diğer gruplar ve bireyler tarafından da kamu güvenini sarsmak amacıyla kullanılmaya başlanmıştır. Dijital çağın getirdiği dönüşümle birlikte sosyal medya platformları, yapay zekâ teknolojileri ve mikro-hedefleme gibi yenilikçi araçlar, dezenformasyonun hem yaygınlığını hem de karmaşıklığını artırmıştır. Bu

gelişmeler, manipölasyonun daha hızlı, hedef odaklı ve zor tespit edilir hale gelmesine yol açmıştır (Marwick ve Lewis, 2017).

Dezenformasyonun ve misenformasyonun sosyal medyada yoğun olarak yer alması toplumsal düzen ve kamu güvenliğini olumsuz anlamda etkilemektedir. Covid-19 pandemi döneminde aslı değiştirilmiş ses ve video görüntüleriyle kişilerin yanıltılması, insanlarda kafa karışıklığına ve panik, korku ve endişe haline sevk ederek kişilerin iletişimde birbirini ötekileştirmesine, kaos ortamı oluşmasına neden olmaktadır. Örnek olarak İngiltere’de 5G teknolojisinin koronavirüs salgınını yaydığı iddiaları sonrası baz istasyonlarının yakılmasına neden olmuştur (Bahar A, 2020, s.2772).

Sosyal medya platformlarındaki hızlı bilgi akışı kendi başına bir sorun yaratmaz; asıl problem, bu mecralarda yanlış bilginin doğru bilgiden daha baskın hale gelmesidir. Yapılan araştırmalar, özellikle siyasi dezenformasyon hacminin genel çevrimiçi siyasi bilgi hacmini aştığını göstermektedir (Tucker vd., 2018). Bu durumun başlıca nedenlerinden biri, doğruluğu şüpheli haberlerin hazırlanması ve yayılmasının dijital ortamda neredeyse sıfır maliyetli olmasıdır.

Tıklama odaklı siteler, aşırı parti yanlısı medya organları, sahte haber platformları, yabancı hükümetler ile botlar ve troller gibi aktörler, maddi kazanç veya ideolojik amaçlarla siyasi dezenformasyonu sistematik biçimde dolaşıma sokmaktadır. Buna ek olarak haber sıralama algoritmalarının çeşitli yollarla manipüle edilebilmesi, dezenformasyon içeriklerinin görünürlüğünü ve erişimini daha da artırmaktadır. Bir diğer kritik etken ise kullanıcı davranışlarıdır. Sosyal medya kullanıcılarının paylaştığı siyasi bilgiler büyük ölçüde partizan niteliktedir ve bu durum, çevrimiçi siyasi bilginin genel kalitesini önemli ölçüde düşürmektedir (Bakshy, Messing ve Adamic, 2015).



Şekil 12. "15 Temmuz Şehitler ve Fatih Sultan Mehmet köprüleri satışa çıkarılıyor" başlıklı paylaşım, CNBC-e Resmî X Hesabı (<https://x.com/cnbceofficial/status/1965398677406863538> erişim 9 Eylül 2025)

Şekil 18 de Sosyal medya platformu X'te uluslararası yayın yapan CNBC-e kanalının resmi X hesabı üzerinden yapılan 15 Temmuz Şehitler ve Fatih Sultan Mehmet Köprülerinin özelleştirilmesinin gündemde olduğu haberi yer almaktadır. Söz konusu haberi yaklaşık olarak 10 milyon kişi görüntülemiştir.



Şekil 13. T.C. İletişim Başkanlığı Dezenformasyonla Mücadele Merkezi (DMM) paylaşımı (<https://dbs.iletisim.gov.tr/hakikat/1457>)

16.09.2025 tarihinde Cumhurbaşkanlığı İletişim Başkanlığı bünyesindeki Dezenformasyonla Mücadele Merkezi, kurulan dbs.iletisim.gov.tr adlı sitede 15 Temmuz Şehitler Köprüsü, Fatih Sultan Mehmet Köprüsü ve Ülke Geneline Otoyollar Satılıyor adıyla dolaşıma sokulan haberi yayınladıkları metinde yalanlamıştır. Söz konusu metinde iddiaların kamuoyunu yanıltmaya yönelik bir dezenformasyon kampanyasının parçası olduğu vurgulanmaktadır. Otoyol ve köprülerin satışının hukuken mümkün olmadığını, sadece işletme ve bakım haklarının özel sektöre 1994 yılında çıkarılan 4046 sayılı Özelleştirme Kanunuyla devredilebileceği belirtilmektedir. İddialara konu işlemin satış değil finansal ve teknik danışmanlık hizmeti alım süreci olduğu anlatılmıştır (DMM, 2025).

2.2.2. Toplumsal Hareketler ve İstihbarat

Marshall, toplumsal hareketi dikkate değer sayıda insanın, toplumun temel özelliklerinden birini veya birkaçını değiştirmek (ya da bu değişikliğe karşı koymak) amacıyla örgütlü çaba göstermesi olarak tanımlar. Marshall'ın belirttiğine göre kavram, ilk kez 18. yüzyıl başlarında Saint-Simon tarafından Fransa'da ve başka yerlerde görülen toplumsal protestoları ifade etmek için kullanılmıştır; bu bağlamda "statükoya karşı çıkan yeni siyasi güçlerin bir özelliği" olarak görülmüş ve zamanla siyasi sistemin dışında kalan grupları/örgütleri kapsayan bir terime dönüşmüştür (Marshall, 2005, s. 746).

Bu tanıma göre toplumsal hareketler öncelikle siyasi nitelikli eylemler ve mücadeleler olarak algılanmaktadır. Ancak çalışmanın ilerleyen bölümlerinde ele alınacağı üzere, toplumsal hareketler yalnızca siyasi veya ekonomik temelli olmayıp daha geniş bir yelpazede ortaya çıkabilmektedir.

Türkdoğan'a (2013) göre toplumsal hareketler, toplumda yeni bir yaşam biçimi oluşturmak amacıyla kolektif davranış sergileyen grupların eylemleridir. Bu kolektif eylemler, mevcut yaşam biçiminden memnun olmayan, bunu değiştirmek isteyen ve bu yönde çözüm arayışına giren bireylerin tutum ve düşünce yapılarını etkileyen süreçlerdir (Türkdoğan, 2013, ss. 11-13). Başlangıçta yeterince örgütlü görünmeyen bu hareketler, zamanla daha nitelikli bir yapı kazanmakta ve toplumun değerler sistemi, normları ile kültürüne önemli katkılarda bulunmaktadır.

Arrighi, Hopkins ve Wallerstein ise toplumsal hareketleri sistem karşıtı hareketler olarak nitelendirir. Onlara göre ezilen kesimler çoğu zaman başkaldırı

girişimlerinde başarısız olur; bu tür hareketler ancak iktidarın sallantıda olduğu istisnai dönemlerde etkili olabilmektedir. Başkaldırılar genellikle kendiliğinden ortaya çıkar, kısa sürer ve süresiz kalır. Bu süresizlik, iktidarların en büyük avantajı olarak görülür (Arrighi, Hopkins ve Wallerstein, 2015, s. 35).

Bununla birlikte başkaldırıların geçici ve süresiz olması, toplumsal hareketlerin hiçbir etki yaratmadığı anlamına gelmez. Bu hareketler her zaman bir soruna dikkat çekmek, azınlığın sesini duyurmak amacıyla gerçekleşir. İktidarı ele geçirme gibi bir hedef taşımazlar; asıl amaç, kendi taleplerini ve varlıklarını görünür kılmaktır.

Castells (2008), üç ciltlik Enformasyon Çağı serisinin ilk kitabında toplumsal hareketleri ağ toplumu ve enformasyonelleşme çerçevesinde ele alır. Ona göre toplumsal hareketler ve siyaset, teknolojiye dayalı küreselleşme süreçleri, çeşitli kimlik güçleri (cinsel, dinsel, ulusal, etnik veya sosyobiyojik) ile devlet kurumları arasındaki etkileşimden doğar (Castells, 2008, ss. 5-6). Bu bağlamda toplumsal hareketleri, başarı veya başarısızlık sonucundan bağımsız olarak “toplumun değerlerini ve kurumlarını değiştirmeyi amaçlayan kolektif eylemler” olarak tanımlar. Bu yaklaşım, hareketlerin yalnızca bireysel veya yerel tepkilerden ibaret olmadığını; aksine küresel ağlar, enformasyon akışları ve kimlik dinamikleriyle iç içe geçmiş daha karmaşık süreçler olduğunu vurgular.

Günümüz uluslararası ilişkilerinde devletler, hasımlarını alt etmek için modern ordularını devreye sokup milyarlarca dolarlık konvansiyonel savaflara girişmeyi nadiren tercih etmektedir. Gelişen silah teknolojileri ve nükleer menzilin küresel kapsama ulaşması, olası bir doğrudan çatışmanın yıkıcı sonuçlarını en üst düzeye çıkarmış durumdadır. Bu caydırıcılık unsurları, devletlerin hedeflerine ulaşma çabalarını engellemese de, doğrudan silahlı mücadele yerine vekil aktörler üzerinden dolaylı eylemlere yönelmelerine yol açmaktadır. Vekil olsun ya da olmasın, hasım ülkedeki herhangi bir toplumsal olay, en çok desteklenen ve teşvik edilen faaliyetler arasında yer alır. Bu tür eylemlerin yürütülmesinde en kritik rollerden birini istihbarat teşkilatları üstlenir. Modern istihbarat teşkilatlarının görev tanımları ve kullandıkları araçlar, onları devletin stratejik hedeflerine ulaşmasındaki en etkili "silahlardan" biri haline getirmektedir. Bu bağlamda modern bir istihbarat teşkilatının dört temel fonksiyonu birbirini tamamlayıcı niteliktedir: Birincisi, devletin ihtiyaç duyduğu bilgileri toplamak ve istihbarat ürünü oluşturmak; ikincisi, psikolojik savaş faaliyetleri

yürüterek hedef kitleleri ikna etmek veya etkilemek; üçüncüsü, dış politika hedefleri doğrultusunda örtülü operasyonlar icra etmek; dördüncüsü ise kendi ülkesine yönelik tehditleri önlemek adına istihbarata karşı koyma (counterintelligence) faaliyetlerini yerine getirmektir (Yılmaz, 2018, s. 91). Bu dört alan dikkatle incelendiğinde, istihbarat teşkilatlarının asli görevleri ile toplumsal olaylar arasındaki kesişim noktaları belirginleşir. Özellikle psikolojik savaş/propaganda faaliyetleri ile örtülü operasyonlar, doğrudan toplumsal hareketler, protestolar veya iç karışıklıklarla ilişkilendirilebilecek en belirgin alanlardır.

İkinci Dünya Savaşı sonrası dönemde dünya genelinde yaşanan toplumsal olaylar, toplum bilimcilerin analizleri ve modern istihbarat teşkilatlarına yüklenen roller birlikte değerlendirildiğinde ortaya çıkan tablo oldukça dikkat çekicidir. Toplumsal olayların yorumlanması tarihsel süreçte çok sayıda teorinin doğmasına yol açmış; bu teorilerin büyük ölçüde sosyalist ve kapitalist yaklaşımlardan etkilendiği görülmüştür. Salt ekonomik temelli açıklamaların ötesinde, ekonomik dönüşümlerle birlikte kentlerin, toplumsal ilişkilerin ve devlet aygıtının eşzamanlı değişimi, bu olayların en belirgin çıkış noktaları arasında yer almaktadır. Soğuk Savaş'ın sona ermesiyle birlikte etnik ve dinsel farklılıklar ön plana çıkmış; birçok coğrafyada özne şartlara bağlı olarak toplumsal olaylar farklı biçimlerde tezahür etmiş ve etmeye devam etmektedir. Bu çalışmada temel soru "Bir toplumsal olayda istihbarat teşkilatları hangi rolleri üstlenebilir?" olarak belirlenmiş ve bu soruya yanıt aramak üzere "Rejim aleyhtarı bir toplumsal hareket hedefine nasıl ulaşır?" sorusu merkeze alınmıştır. Araştırmanın sonucunda, toplumsal olayların genel algıların aksine seyrettiği ortaya çıkmıştır. Bir rejimin tipi, iktisadi kalkınmışlık düzeyi, okuryazarlık oranı ya da toplumun etnik, dinsel veya dinsel fay hatları boyunca bölünmüşlük derecesi gibi değişkenler, sivil hareketlerin başarısı üzerinde anlamlı bir etki yaratmamaktadır (Marchant vd., 2008).

2.3. Devlet Güvenliği Açısından Terör ve Radikalleşme

Terör, Türk Dil Kurumu Sözlüğü'ne göre "karşı tarafa korku salma, cana kıyma, malı yakıp yıkma; yıldırı, tedhiş olarak tanımlanmıştır. Latince "terrere" kelimesinden türeyerek korkudan dehşete düşürmeye sebep olma" anlamı taşımaktadır. Terör kelimesi Türkiye'deki Terörle Mücadele Kanunu'nun 1. maddesine göre (Terörle Mücadele Kanunu, 1991, m. 1) "Terör; cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen

Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir.” olarak tanımlanmaktadır.

(Gökçe, 2018)’ye göre terör; iradenin söz konusu olmadığı “kontROLSÜZ kitlelerin yarattığı aşırı şiddet ve katliamlar” iken terörizm ise siyasi amaçları gerçekleştirmek için terör gerçekleştirilmesidir.

Radikalleşme kavramı ile ilgili literatürde üzerinde mutabık kalınan bir tanımı bulunmamaktadır. Ancak radikalleşme ile anlatılmak istenen bireylerin şiddet içerikli eylemleri meşru gören planlayıp uygulayabilen kişilerin geçirmiş oldukları zihinsel dönüşümdür. Radikaller, ulaşmak istedikleri ideale doğru engel olmadan devrimci hareketle kısa yoldan ulaşmak isterler (Köse, 2024).

Radikalleşmenin olabilmesi için kapalı gruplarda propaganda maruz kalmak gerekmektedir. Bu noktada sosyal medyanın kapalı gruplarda hızlı ve gizli şekilde haberleşme ortamına sahip olması, bu mecralarda yapılan propaganda faaliyetlerinin radikalleşmeye yol açtığı görülmektedir.

2.3.1. Terör Örgütü Propagandası ve Dijital Stratejiler

Dijital çağda en çok kullanılan internet ve dolaylı olarak sosyal medya platformları, son zamanlarda terör örgütlerinin faaliyet alanları haline gelmiştir. Aynı zamanda küresel çapta geniş bir kullanıcı kitlesine sahip olması , gizli iletişimin sağlanabilirliği, ucuz maliyet , hızlı bilgi akışı , hükümet kontrolü ve sansür uygulamasının nispeten daha az olması, videoları, görselleri , metinleri düzenleme ve değiştirme işlemlerini yapabildikleri multimedya ortamının olması, web sayfalarının bakımı ve geliştirilmesinin daha az maliyetli olması , geleneksel medya haberlerinin içeriklerine etki edebilme özellikleridir (Weimann, 2014, ss 2-3). Terör örgütleri bir nevi kendi reklamlarını yapmak, kendilerini tanıtmak için de sosyal medyayı kullanmaktadır.

Propaganda; Türk Dil Kurumu Sözlüğüne göre “bir öğreti, düşünce veya inancı başkalarına tanıtmak benimsetmek ve yaymak amacıyla söz, yazı vb. yollarla gerçekleştirilen çalışma, yaymaca” olarak tanımlanmıştır.

Terörizm; kavramsal, ideolojik ve teknolojik olarak zamanla farklı şekillerde tezahür ederek değişim ve dönüşüme uğramıştır. Bu değişim ve dönüşümler Fransız Devrimi’ne kadar olan klasik dönem, Fransız Devrimi’nden 11 Eylül 2001 saldırısına kadar uzanan modern dönem ve 11 Eylül 2001 saldırısından sonraki post modern dönem şeklinde üç döneme ayrılmaktadır. Terörizmin başlangıcını insanlar arasında iktidar ilişkilerinin başladığı döneme kadar götürmek mümkündür. İlk aşamada terörizm, vur-kaç ve suikast yöntemleriyle yerel, ulusal nitelik taşımaktadır. Fransız Devrimi sürecinde şiddetin hem iktidara karşı durma aracı olarak kullanılması hem de iktidarın karşı tedbir amaçlı şiddet kullanmasıyla terörizmin aktörleri arasında devletin yer almasını sağlamıştır. 20.yüzyılın başlarında terörizmin ideolojik boyutlarının hazırlandığı bir dönemdir (Gökçe, 2018).

Bu dönemde ilk kez terörizmin propaganda boyutu İtalyan anarşist Malatesta’nın “eylem yoluyla propagadanda” stratejisiyle oluşmaya başlamış, anarşist hareketlerin terörizme dönüşmesinin temelini atmıştır (Mango, 2005: 12; akt. Gökçe, 2018: s. 345) Bu dönemde eylemle propaganda rastgele hedef belirleme ve kendini adanmışlık özelliklerine sahip olmakla birlikte amaçları açısından ulusal, eylemleri açısından yerel ölçekte hareket eden özelliktedir (Gökçe, 2018).

İkinci dünya savaşı sonrasında terörizm, devrimci özelliğinden sıyrılarak devletlerin dış politika aracı haline gelmiştir. Soğuk Savaş’ın sona ermesiyle birlikte ulaşım, bilişim, iletişim ve teknolojiye gelişmeler küreselleşmeyi hızlandırdığı gibi terör örgütleri de gelişen imkanları kullanarak bir nevi küreselleşmiştir. 11 Eylül 2001 saldırısı ile birlikte terörizm yeni bir boyut kazanmıştır. Bu çağda gelişen imkanlar, yerel veya ulusal düzeyde değil terör örgütleri tarafından küresel boyutta etki oluşturacak eylemlerin yapılmasını sağlamıştır. Terör örgütlerinin teknik imkan ve kabiliyetleri artmış, insan kaynağı küreselleşmiştir. Post modern terörizm döneminde devletler ya da devlet dışı yapılar, uluslararası siyasetin gayri resmi ve ahlaki bir aracı olarak sosyal medyayı kullanmaktadır. Terör örgütleri sosyal medya ve internet ağlarını korku ve dehşet saçmak ve bu yolla propaganda yapmak, yandaş kazanmak, ticaret yapmak amacıyla araç olarak kullanmaktadır (Gökçe, 2018).

Geleneksel propaganda türünde bireylerin tutum ve eylemlerini değiştirmek amaçlanmışken modern propaganda türünde bireylerin tutum ve eylemlerini değiştirmenin yanında yapılan propagandaya dair bir inancın yerleşmesi ve bu uğurda aktif olarak eyleme geçmesi amaçlanmaktadır. Bireylerin kendi dost ve düşman tanımlamasına göre hareket etmesi amaçlanmaktadır. Terör örgütleri, propaganda yaparken kendilerine göre kutsal veya değerli gördükleri bazı semboller ve betimlemeler kullanabilir, bilgileri çarpıtabilir, terör örgütünün ideolojik eğitim verirken kullandığı kendilerine has bazı kelimeleri, ideolojik beyin yıkama amacıyla sıkça kullanabilmektedir. Örnek olarak Deaş terör örgütü Suriye’de dini sembollerini kullanarak dini bilgilerin kendi amaçlarına uygun olacak şekilde yorumlayıp çarpıtması, kendinden olmayanı ötekileştirebilmesi ve bu inanca uygun olarak kişileri eğitebilmesi, bireyleri radikalize edip terör eylemlerinde kullanabilmesi gösterilebilir (Kartal,2020, s.64).

Sosyal medya üzerinden propaganda yapan terör örgütlerinin paylaşımları, aldıkları etkileşimle beraber salgın hastalıklarının hızlı yayılması ve bir virüs gibi insanları enfekte etmesine benzetilmektedir (Ferrara, 2017, s.2). Bireylerin çevrimiçi sosyal ağlarda propaganda faaliyetlerine maruz kalmasıyla başlayan süreçte enfekte olan kullanıcıların etkileşime girmesiyle devam etmesiyle propagandanın yalnızca tek taraflı bir iletişim olmadığını ağ yapısı içinde devamlı yeniden üretme sürecinde olunan ve ağdaki ilişkinin güçlenerek devam ettiği bir ilişki süreci olarak görülmektedir (Ferrara, 2017, s.5).

Ferrara’nın çalışmasında özellikle propaganda faaliyetine başlatan ve yayan kullanıcıların profillerinin dikey (yüksek takipçi sayısına sahip, merkezi aktörler) ve yatay (küçük ölçeğe sahip yoğun etkileşime sahip profiller) etkileri olanlar birlikte çalıştıklarında hem geniş kitlelere ulaştığı hem de küçük, kapalı gruplarda kalıcı olarak yer edinmesini mümkün kılmakta ve analizler bu tür içeriklerin sosyal medyada çok daha hızlı ve yüksek bulaşıcı katsayısına sahip olduğu anlaşılmaktadır (Ferrara, 2017 s.8). Bu yaklaşıma göre radikalleşme süreci sadece ideolojik içeriklere maruz kalma yoluyla olmadığı, ağlar arası etkileşimin içerik akışı ve gizli gruplara girme yoluyla ilişkilerin güçlendirilmesi kısımlarının da önemli olduğu vurgulanmaktadır.

Duhaime’ye göre DEAŞ terör Örgütü’nün dijital alandaki terör stratejisi 4 maddeden oluşmaktadır.

1. Yalnız kurtları harekete geçirmek, tek başına yapılan eylemleri arttırmak, istihdam sağlamak
2. Dünya ile çevrimiçi yollarla agresif iletişim kurmak ve bu yolla gençlerin beyinlerini yıkamak amacıyla sosyal gerçeklik alanından koparmak
3. Vahşi eylemleri video kaydına alarak dijital alanda yaymak, korku ve dehşet oluşturmak bu yolla DEAŞ'ı finansörlerine kanıt sunma
4. Sosyal medya platformları aracılığıyla bağış, fon gibi yöntemlerle finansman sağlama (Duhaime, 2015, s. 1'den aktaran Taşdemir, 2025, s. 739).

Terörün bir diğer biçimi ise uluslararası terördür. Uluslararası terör ile devlet terörü, yurt dışında gerçekleştirdikleri şiddet eylemleri veya destek faaliyetleri bakımından birbirini tamamlayan niteliktedir. Ülkeler, kendi coğrafyalarında güçlerini korumak veya küresel kaynakları ekonomik açıdan kontrol altında tutmak amacıyla, hedef ülkelerde iç karışıklık ve çatışma ortamı yaratmayı amaçlayabilmektedir. Bu amaç doğrultusunda, hedef ülkelerdeki mevcut farklılıkları sahte manipülasyon yöntemleriyle meşru otoriteye ve ülke halkına karşı şiddete yönlendirebilmekte; söz konusu gruplara para, eğitim, silah, patlayıcı madde, gizlenme yeri, istihbarat bilgisi, seyahat belgeleri ve lojistik malzeme sağlayarak destek olabilmektedirler (Gökçe, 2016).

2.3.2. Radikalleşme Sürecinde Sosyal Medyanın Rolü

Terör örgütleri, radikalleştirme faaliyeti ve ardından eleman devşirme faaliyeti için sosyal medya platformlarını kullanmaktadır. Radikalleşme sürecinde İstismar, etkileşim, risk ve azaltmadan oluşan dört boyut bulunmaktadır. Buna göre sosyal medya aracılığıyla bireylerin radikalleştirilmesindeki etkisinin çok boyutlu olduğu anlaşılmaktadır. İstismar boyutu, şiddet yanlısı radikal aktörlerin ideolojik mesajlarla sosyal medya kullanıcısı bireylerin maruz bırakılması, bu platformları bağış toplama, eleman devşirme ve taktik paylaşma amacıyla kullanması olarak tanımlanmaktadır. Etkileşim boyutu kullanıcıların radikal örgütlerin propaganda amaçlı paylaştığı içeriklere maruz kalarak tüketme, onay arayışı, benzer düşünceli bireylerle bağlantı kurarak şiddet niyetinin açığa vurulması olarak tanımlanmaktadır. Risk boyutu ise hangi bireylerin daha yüksek düzeyde radikalleşme sürecinde tehdit altında olduğu ifade edilmektedir. Azaltma boyutu ise radikalleşme sürecini engellemek veya etkisini sınırlandırmak amacıyla geliştirmiş olduğu strateji ve

uygulamaları ifade etmektedir (Aryaeinejad ve Scherer, 2024). Buna yönelik olarak çevrimiçi nefret içeriklerine insanların nasıl maruz kaldığını ve nasıl tepkiler verdiklerini ölçmek amacıyla Arkansas Eyalet Üniversitesi araştırma ekibi 3.000 Amerikalı üzerinde yapılan anket çalışması gerçekleştirmiştir. Buna göre Buna göre gençlerin Youtube, Reddit ve Snapchat gibi platformlarda nefret içeriklerine daha çok maruz kaldığı, buna karşın Instagram’da daha düşük bir riskin bulunduğu, Google+, Twitter ve Facebook ile anlamlı bir bağlantı kurulmadığı görülmüştür. Aynı zamanda bu çalışmada çevrimiçi nefret içeriklerine maruz kalma ile hükümete güvensizlik, politikacılara olan güvensizlik, ABD politikalarından memnuniyetsizlik arasında pozitif ilişki kurulmuştur. İnternette geçirilen sürelerin artması, bireylerin radikal içeriklere maruz kalma riskini de arttırdığı görülmüştür. Bu açıdan risk boyutunda ideolojik eğilimlerin yanı sıra çevrimiçi kullanım süreleri ve kullanılan platformlar ve bireyin siyasal görüşüyle doğrudan ilişkili olduğu görülmektedir (Costello vd., 2020).

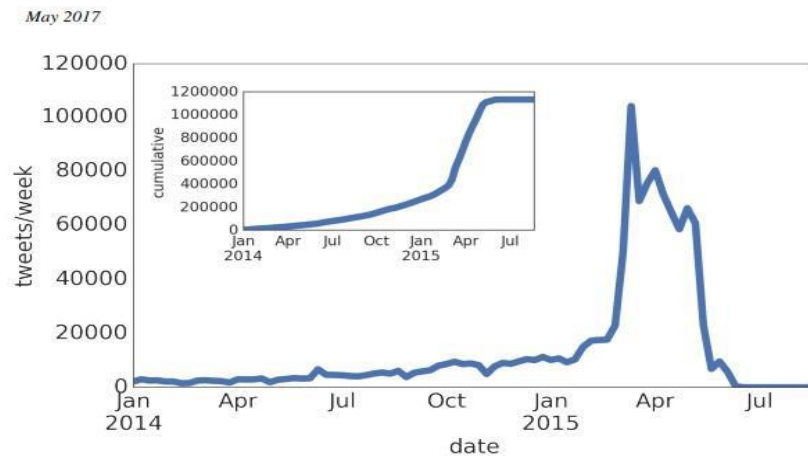
Örnek olarak 8 Eylül 2025 tarihinde sosyal medya üzerinden radikalleşen ve terör örgütü DAESH ile irtibatı tespit edilen 16 yaşındaki E.B. isimli bir şahsın İzmir’deki bir polis merkezine silahlı saldırı yapması gösterilebilir. Nitekim ailesinin beyanında çocuklarının saldırı öncesinde radikal sitelere girdiğini ve vakitlerini burada harcadığını söylemektedir. Yine saldırı öncesinde kendi Instagram hesabından eylem öncesinde “Ey Muvahhitler! Artık bugün Türkiye, eylemlerinizin çerçevesine ve cihadınızın kapsamına girmiştir. Allah’tan yardım dileyin ve oraya saldırın! Güvenliğini korkuya, rahatlığını dehşete çevirin! Sonra orayı ateşli mücadelenizin mıntıklarına katın. Müminlerin emiri ve Müslümanların halifesi Şeyh Ebu Bekir el-Bağdadi “Allah onu korusun.” şeklinde paylaşımı bulunmaktadır. Bu çocuk şahsın terör örgütü DEAS’ın propagandalarına maruz kaldığını, etkileşime geçtiğini ve eylemini gerçekleştirdiğini göstermektedir. (Demir, 2025).

2.3.3. Deaş Terör Örgütünün Sosyal Medya ve Dijital Alan Kullanımı

Bireylerin çevrimiçi sosyal ağlarda propaganda faaliyetlerine maruz kalmasıyla başlayan süreçte enfekte olan kullanıcıların etkileşime girmeye devam etmesiyle propagandanın yalnızca tek taraflı bir iletişim olmadığını ağ yapısı içinde devamlı yeniden üretme sürecinde olunan ve ağdaki ilişkinin güçlenerek devam ettiği bir ilişki süreci olarak görülmektedir (Ferrara,2017).

Ferrara'nın çalışmasında özellikle propaganda faaliyetine başlatan ve yayan kullanıcıların profillerinin dikey(yüksek takipçi sayısına sahip, merkezi aktörler) ve yatay (küçük ölçeğe sahip yoğun etkileşime sahip profiller) etkileri olanlar birlikte çalıştıklarında hem geniş kitlelere ulaştığı hem de küçük, kapalı gruplarda kalıcı olarak yer edinmesini mümkün kılmakta ve analizler bu tür içeriklerin sosyal Medya'da çok daha hızlı ve yüksek bulaşıcı katsayısına sahip olduğu anlaşılmaktadır (Ferrara, 2017). Bu yaklaşıma göre radikalleşme süreci sadece ideolojik içeriklere maruz kalma yoluyla olmadığı, ağlar arası etkileşimin içerik akışı ve gizli gruplara girme yoluyla ilişkilerin güçlendirilmesi kısımlarının da önemli olduğu vurgulanmaktadır.

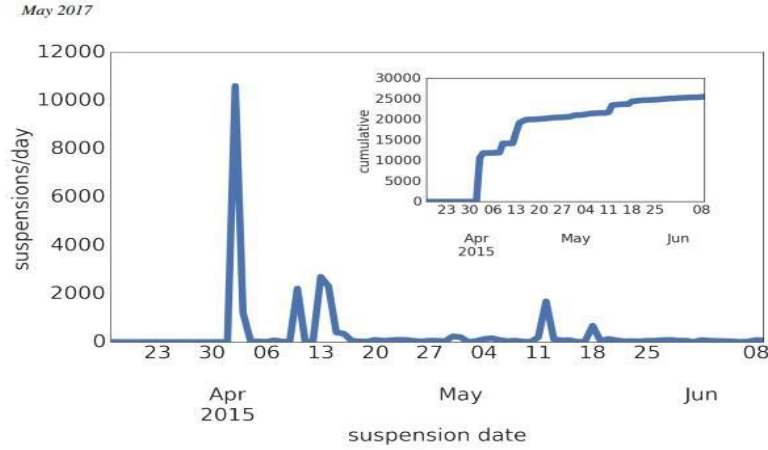
Buna göre çevrimiçi platformlarda yapılan propaganda amaçlı içeriklerin bulaşma süreci gibi bilinçli veya bilinçsiz kullanıcıların etkileşime girerek enfekte olmasını ve hiçbir şekilde örgüte sempatisi olmayan hatta bilgisi dahi olmayan kişilerin maruz kalarak kamu istismara uğramasını, etkileşime girmesi ve örgüte sempati kazanması ve diğer örgüte katılım aşamasındaki süreçlerde güvenliği açısından sosyal medya üzerinde bu tür içeriklerin yayılım hızını azaltmak amacıyla algoritmik müdahaleler, sosyal medya yasaları ve diğer müdahaleci yöntemlerin etkili olabileceği görülmektedir.



Şekil 14. Deaş destekçilerinin oluşturduğu tweet sayısının zaman içindeki dağılımı. (Ferrara, 2017) s.7).

Bu tabloya göre Deaş destekçilerinin haftalık ve kümülatif toplamda ürettiği tweetleri göstermektedir. Çalışmadaki bulgularda haftalık tweetlerde artışın olması, bazı zamanlarda yüksek artışın olması, örgüt destekçilerinin bazı önemli olaylar sonrasında yoğun tweet çalışmasıyla propaganda faaliyetine hız verdiği anlaşılmaktadır. Kümülatif toplamda artarak devam eden artışın olması ise örgütün

uzun vadeli olarak sosyal medyayı propaganda faaliyetlerini yürüteceği stratejik bir alan olarak gördüğü anlaşılmaktadır (Ferrara, 2017).



Şekil 15. Deaş destekçi hesaplarının günlük askıya alınma sayılarının zaman çizelgesi (Ferrara, 2017 s.5).

Bu tablodaki bulgulara göre terör örgütü Deaş'ın ana grafikte gösterildiği günlük askıya alınma sayılarında bazı zamanlarda artış olduğu, ek grafikte kümülatif toplamda sürekli bir artışın olduğu, bu artışın sürekli artan bir hızda devam ettiği anlaşılmaktadır. Bazı önemli olaylar sonrası propaganda içeren içeriklerin dolaşıma sokularak etkileşim alınması sonrasında çalışmadaki örnek site olan X platformu, bu tür içerikler paylaşan profilleri tespit ederek askıya aldığı görülmekte ve yine devamlı olarak askıya alınan profillerin artış halinde olduğu radikalleşme ve terör örgütü propagandasıyla mücadele edilmeye çalışıldığı görülmektedir.



Şekil 16. Deaş terör örgütü'nün militan toplamak amacıyla kurduğu birçok X hesaplarından bir tanesi (Süleyev, Medya ve Terör İlişkisi, 2019, s.47).



Şekil 17. Deaş terör örgütü'nün militan toplamak için kurmuş olduğu Facebook hesaplarından bir tanesi (Süleyev, Medya ve Terör İlişkisi, 2019, s.49).

İnsanlar üzerinde haber niteliği taşıyan ve gündemi yoğun olarak işgal eden, en çok takip edilen konulardan biri olan terör ve terörizm eylemleri, reyting sağlamak için medya şirketlerinin gündemde tutmak istediği konulardan biridir. Bu noktada her iki tarafın da bilerek veya bilmeyerek bir menfaat ilişkisine sahip olduğu söylenebilir. Geleneksel medya yayıncılığı yapan kuruluşlardan bazıları aynı zamanda sosyal medya hesapları üzerinden de yayın yapmaktadırlar. Bu anlamda yapılacak olan terör haberlerinde kullanacakları kavramlar konusunda dikkatli olmaları gerekmektedir. Örnek olarak BBC kanalının 23 Ağustos 2016 yılında PKK terör örgütünden bahsederken ‘‘Kürt asi grupları’’ olarak nitelendirmesi ve yine aynı haberde YPG terör Örgütü’nün PKK’nın devamı olarak değil de IŞİD’e karşı savaşılan özgürlük savaşçısı, Türk ordusunun da savaşçılara topçu atışı yaptığı şeklinde kavramların üzerinde oynama yaparak haberin sunulmasından kaçınılması gerekmektedir (Kartal, 2020, s.60).

Sosyal medya platformları, terör örgütlerinin propaganda faaliyetlerini sürdürdüğü, eleman temin ettiği alan olmasının yanı sıra bağış ve fon toplama adı altında finansman sağladığı alanlar olması yönünden ön plana çıkmaktadır. Örgütler bu mecralarda propaganda yoluyla sempati toplamaktadır. Oluşturulan sempatileri

eleman temin etme ve bağış linkleri yoluyla finansal destek sağlamaktadırlar (FATF, 2023).

Terör örgütleri geleneksel yöntemler olan broşür dağıtma, dergi yayınları, toplantılar düzenleme gibi etkinliklerin yanında çevrimiçi dergiler (Dabiq , Inspire) videolar, video oyunları gibi modern araçları da eleman devşirme faaliyetleri olarak kullanmaktadır. Bu faaliyetlerin üretilmesi belli bir profesyonellik ve altyapı gerektirdiğinden belli bir mali ayak izi oluşturmaktadır (FATF, 2018).

DEAŞ terör örgütü, propaganda faaliyetleri için X ve Facebook gibi platformları kullandığı gibi YouTube kanallarında da kendi tanıtımını yapma, halka korku ve panik oluşturma, kendi popülerliğini arttırma gibi birçok amacını gerçekleştirmek için kullanmaktadır. Örnek olarak 2012 yılında Işid terör örgütü, Amerikan gazeteci James Foley'nin kafasının kesilerek infaz edildiği videosunu yayınlamış, kısa sürede dünyanın birçok ülkesinde izlenmiştir (Süleyev,2019 s.50).



Şekil 18. İngiliz gazeteci James Foley'nin kafasının kesildiği videonun Youtube platformu'nda haber olması (https://www.youtube.com/watch?v=9kj9Sja7768&ab_channel=ABC7News-WJLA.)

Terör örgütleri, sosyal medyayı propaganda yoluyla devşirilen elamanların eğitimi için de kullanmaktadır. Youtube ve Facebook gönderilerinde patlayıcı yapımı, takipçileri kendi aralarında kurmuş oldukları gizli topluluklar üzerinden eğitim

materyallerinin sunulduğu sitelere yönlendirme gibi hem ideolojik ve hem de eylemde kullanılacak bilgilerin verilmesinde sosyal medya kullanılabilir. (Weimann, 2014, ss 3-4).

Sosyal medya, terör örgütlerinin finansman sağlama kanallarından biridir. Propaganda yoluyla eleman devşirme faaliyetleri, çoğu kez bağış toplama çağrılarıyla doğrudan bağlantılıdır. Şifreli web siteleri, kapalı sohbet gruplarını ideoloji yayma ve eleman devşirme amacıyla kullanmasının yanı sıra, banka hesap bilgileri, e-cüzdan adresleri, görünürdeki hayır amaçlı bağışların tespit edilmesinin önlenmesi amacıyla kullanılmaktadır (FATF, 2023).

Rapordaki Avustralya örneğinde sosyal medya platformlarından Facebook üzerinden toplanan fonların radikal ideolojilerin yayılması amacıyla çalışan kayıt dışı hayır kurumları adı altında faaliyet gösteren yapılara aktarıldığı görülmektedir (FATF, 2018, ss.14-15). Bu raporda Deaş terör örgütünün propaganda yapmak için kurduğu web sitesinin teknik hizmetleri ve diğer masraflarını karşılamak için kripto paralar üzerinden bağış topladığı tespit edilmiştir (FATF, 2018 S.20). Bu durumda sosyal medyayı daha az izlenebilir, gizli ve basit propaganda ve eleman devşirme kanalı olarak seçen terör örgütleri için bağış toplaması , devşirilen, kişilerin ayrıca bağış toplayan ve organize eden kişilerin gizli kalmasının sağlanması açısından terör örgütleri için kritik bir yapıdadır.

Financial Action Task Force (Finansal Eylem Görev Gücü Terör Amaçlı Eleman Temin Etmenin Finansmanı adlı 2018 yılındaki rapordaki vaka analizlerinde sosyal medya üzerinden toplanan bağışların devşirilen elamanların seyahat ve lojistik giderlerinde kullanıldığı görülmektedir. Mali soruşturmalar, Türkiye'ye giden M kişinin Rusya ve Orta Asya ülkesi vatandaşlarını DEAS'a katılmasını sağlamak için sosyal medyayı kullandığı bir vakada bağış çağrısı yapan bir M kişisi olan devşiricinin banka hesabına 21.000 dolar para yatırılmış, bu fonların Türkiye üzerinden Suriye'ye geçirilecek elemanların konaklama, gıda ve seyahat giderlerinin karşılanmasında kullandığı görülmektedir (FATF, 2018, s.22).

Sosyal medya platformları ve diğer medya kuruluşlarında yapılan terör haberlerinde aşırı derecede eylem görüntüleri, terör örgütünün propagandasının yapılmasını sağlayacak nitelikte haberlerin videoların, ses ve görüntülerin dolaşması, halk içinde hem korku ve paniğe hem de devlete karşı güvensizlik duygusuna yol

açabilir. Her an terör saldırısına maruz kalınabileceği düşüncesiyle insanların psikolojileri bozulabilir. Bu noktada devlet ve kamu güvenliğinin sağlanması açısından devlet kurumlarının da aktif olarak sosyal Medyayı kullanması, yapılan dezenformasyonlara hızlı bir şekilde yalanlama yapılarak cevap verilmesi gerekmektedir. Engelleme faaliyetleri medya üzerinden yapılmalıdır (Zengin vd., s.32).

2.4. Sosyal Medya İstihbaratı(Socmint)

Sosyal medya platformları, doğası gereği istihbarat teşkilatlarına hedef bireylerin tercihlerini, inançlarını, davranış kalıplarını ve faaliyetlerini toplama, birleştirme ve analiz etme konusunda geniş bir veri alanı sunmaktadır. Bu platformlar, istihbarat birimlerine eğilimleri belirleme, potansiyel tehditleri erken tespit etme, arşiv taraması yapma ve operasyonel iyileştirmeler gerçekleştirebilme imkânı sağlamaktadır. Kullanıcıların büyük çoğunluğu, biyografilerinde kişisel bilgilerini gönüllü olarak paylaşmakta, kendileri ve çevreleri hakkında zengin bir “meta veri” havuzu oluşturmaktadır. Fotoğraf, video, multimedya içerikler ve coğrafi konum verileri de sıklıkla açıkça paylaşılmaktadır. Günümüzde birçok sosyal medya uygulaması, kimlik doğrulama amacıyla kimlik numarası, telefon numarası gibi kişisel bilgileri de talep etmektedir (Dover, 2019, s. 10).

Sosyal medya platformlarından elde edilen bilgiler, günümüzde doğrudan istihbarat kaynağı olarak kullanılabilmektedir. Bu veriler, bir kişinin sosyal çevresini, son dönemdeki faaliyetlerini, genel tutumunu, siyasi eğilimlerini ve potansiyel radikalleşme belirtilerini tespit etmede önemli ipuçları sunmaktadır. Özellikle soruşturma süreçlerinde, hedef bireyin düşünce yapısını, davranış örüntülerini ve olası eylemlerini profillemek açısından değerli bir araç haline gelmiştir (Shipley ve Bowker, 2014, s. 325).

Sosyal medya istihbaratında (SOCMINT) veriler genellikle beş ana kategoride toplanmaktadır:

1. Kullanıcıların kendi paylaşımları,
2. Bu paylaşımlara diğer kullanıcılar tarafından verilen yorumlar ve tepkiler,
3. Fotoğraf, video, ses kaydı, GIF gibi multimedya içerikler,

4. Paylaşımların üst verileri (metadata) – yani paylaşımın yapıldığı konum, tarih-saat, IP adresi ve profil bilgileri,

5. Kullanıcının takipçi ve takip edilenleriyle gerçekleştirdiği etkileşim verileri (Hassan ve Hijazi, 2018, s. 206-207).

Dover'ın (2019) çalışması, sosyal medya platformlarının yaygınlığının hükümetlere ufuk taraması, erken uyarı, soruşturma ve kriz durumlarında durumsal farkındalık açısından önemli içgörüler sağladığını ortaya koymuştur. Ancak aynı çalışma, sosyal medya istihbaratının özellikle erken uyarı ve durumsal farkındalık boyutlarında sınırlı değere sahip olabileceğini de vurgulamaktadır.

Sosyal medya istihbaratının operasyonel değeri, terör örgütlerinin bu platformları yoğun şekilde kullanmasıyla daha da belirginleşmiştir. Kelly ve Rizvi'nin (2015) araştırması, 2008 Mumbai Taj Mahal Oteli saldırısında terörist grupların kamuya açık GPS verileri, Google Earth, kameralı telefonlar ve sosyal medya araçlarını etkin biçimde kullandığını göstermektedir. Teröristler, saldırı öncesi Mumbai'ye beş kez giderek önemli noktaların fotoğraflarını, videolarını ve koordinatlarını toplamış, Google Earth üzerinden işaretlemeler yapmışlardır. Saldırı sırasında otel resepsiyon görevlilerinin oda numaralarını vermemesi üzerine, teröristler otel sistemini ve sosyal medyayı kullanarak hedef kişileri tespit etmişlerdir. Bu saldırı sonucunda 172 kişi hayatını kaybetmiş, 308 kişi yaralanmıştır (Kelly ve Rizvi, 2015, s. 1-10).

Benzer şekilde, 2012 Londra Olimpiyatları sırasında Londra Polisi, sosyal medya platformu Flickr üzerinden yüklenen fotoğrafları ve yüz tanıma teknolojisini kullanarak potansiyel tehdit unsurlarını tespit etmiştir. Irak'ta ise SOMİS (Social Media Intelligence System) sistemiyle şüphelilerin sosyal medya paylaşımları analiz edilerek terör ağlarının bağlantı düğümleri ve olası saldırı planları önceden belirlenmiştir. Bu örnekler, sosyal medya istihbaratının terörle mücadelede değerli veriler sağlayabileceğini açıkça göstermektedir (Neuringer, 2019, s. 140).

Sosyal medya istihbaratı, uzman kişiler tarafından doğru yöntemlerle kullanıldığında hızlı, düşük maliyetli ve etkili bir istihbarat kaynağıdır. Veriler açık kaynaklardan elde edildiği için erişim nispeten kolaydır. Ancak verilerin karmaşıklığı, yüksek hacmi ve dinamik yapısı hem erişim hem de anlamlandırma aşamasında önemli zorluklar yaratmaktadır. İstatistiksel analiz yöntemleri, verilerin arkasındaki normları

ve davranış örüntülerini tam olarak yorumlayamamaktadır. Bu nedenle sosyal medya istihbaratında eğitimli analistlere ve uzmanlara büyük ihtiyaç duyulmaktadır. Ayrıca verilerin düzenlenmesi, saklanması ve dağıtımı konusunda ciddi güvenlik ve gizlilik sorunları bulunmaktadır. Dağınık ve kontrolsüz veri yayılımı, kamuoyunun istihbarat teşkilatlarına olan güvenini zedeleyebilmektedir (Omand vd., 2012, s. 812-814).

Askerî personelin sosyal medya üzerinden yaptığı video ve fotoğraf paylaşımları, sosyal medya istihbaratı (SOCMINT) açısından ciddi güvenlik zafiyetleri oluşturmaktadır. Özellikle operasyon bölgelerinden, üslerden veya harekât alanlarından çekilen özçekimler, birlik fotoğrafları, teçhizat görüntüleri ve konum bilgisi içeren videolar, hasım unsurlar tarafından kolayca analiz edilerek açık kaynak istihbaratına dönüştürülebilmektedir. Bu paylaşımlar; askerlerin bulunduğu konumun, birlik yapısının, kullanılan silah ve elektronik sistemlerin (termal kamera, radar, haberleşme cihazları vb.), harekât zamanlaması ve lojistik durumunun tespit edilmesine imkân tanımakta, böylece düşman unsurların hedefleme ve saldırı planlaması yapmasını kolaylaştırmaktadır (Bural, 2024).

Gerçek hayatta birçok örnekte görüldüğü üzere, askerlerin üniformalı veya operasyon sırasında çektiği görüntüler coğrafi etiketleme, arka plan analizi, yüz tanıma ve metaveri gibi tekniklerle konum ve hareket tespiti için kullanılmaktadır. Bu tür paylaşımlar sadece harekât güvenliğini ihlal etmekle kalmamakta, aynı zamanda siber istihbarat operasyonlarında “dijital ayak izi” oluşturarak askerlerin ve ailelerinin hedef alınmasına, şantaj veya psikolojik harp faaliyetlerine zemin hazırlamaktadır. Türkiye’de de çeşitli operasyonlarda sosyal medyada artan paylaşım trafiğinin hasım unsurlar tarafından izlenerek istihbari avantaj sağladığı tespit edilmiştir. Bu nedenle askerî personelin sosyal medya kullanımı, sadece bireysel bir tercih değil, doğrudan devlet ve kamu güvenliğini ilgilendiren stratejik bir risk unsuru haline gelmiştir (Bural, 2024).

2.4.1. Dijital Ayak İzi ve Profesyonel Ağların Rolü

Dijital ayak izi (digital footprint), bireylerin internet ve dijital platformlar üzerinde gerçekleştirdiği tüm işlemlerin, etkileşimlerin ve paylaşımların bir veri bütünü olarak kaydedilmesi ve izlenebilir hale gelmesidir. Bireyin dijital ortamda ürettiği veya bıraktığı her türlü kişisel veri, zaman içinde birikir ve kişi hakkında kapsamlı bir veri bankası oluşturulmasına imkân tanır. Günümüzde dijital

teknolojilerin günlük yaşamın neredeyse her alanına nüfuz etmesiyle birlikte, yalnızca gündelik pratikler değil, iş süreçleri, finansal işlemler ve sosyal etkileşimler de büyük ölçüde internet tabanlı uygulamalar üzerinden yürütülmektedir. Bankacılık işlemleri, online alışveriş, kamu hizmetleri ve profesyonel iletişim gibi faaliyetler, bireylerin farkında olmadan veya gönüllü olarak kişisel verilerini paylaşmasına yol açmaktadır. Cep telefonu, bilgisayar, akıllı cihazlar ve diğer teknolojiler arasındaki yakınsama (convergence), kişisel verilerin hızla yayılmasını ve biriktirilmesini kolaylaştırmaktadır. Sosyal medya hesapları üzerinden açılan profiller, paylaşılan fotoğraflar, videolar, konum bilgileri, beğeniler ve yorumlar da bu dijital ayak izinin önemli bileşenleri arasında yer almaktadır. İnternete bağlı her cihaz, büyük veri toplama ve analiz sürecinin bir parçası haline gelmiştir. Telefonun açık konum verisi, gönderilen e-postalar, arama motoru sorguları, ziyaret edilen web sayfaları, üye olunan platformlar ve sosyal medya etkileşimleri, bireye ait geniş ve kalıcı bir dijital ayak izi oluşturmaktadır (Polat ve Öcal, 2020).

Sosyal medya ve sosyal ağ siteleri, günümüz dijital ekosisteminin vazgeçilmez unsurları haline gelmiştir. We Are Social'ın 2020 verilerine göre dünyada dijital alanda aktif olan toplam kullanıcı sayısı 7,75 milyara ulaşmış; mobil kullanıcı sayısı 5,19 milyar, internet kullanıcısı sayısı ise 4,5 milyarın üzerine çıkmıştır. Sosyal medya kullanıcılarının sayısı da 3,8 milyarı aşmıştır. Sosyal medya platformları, etkileşimli yapısı sayesinde bireyler arasında sosyal etkileşimi dönüştürmüş ve gündelik yaşamın ayrılmaz bir parçası olmuştur. Kullanıcılar, oluşturdukları çevrimiçi profiller aracılığıyla kendilerini dünyaya tanıtırken, düşüncelerini, duygularını, inançlarını ve günlük deneyimlerini milyonlarca kişiyle paylaşmaktadır. Bu yoğun etkileşim sonucunda ortaya çıkan çevrimiçi insan etkinlikleri, arkasında muazzam bir veri kümesi bırakmaktadır. Yaş, cinsiyet, ikamet yeri, eğitim seviyesi, siyasi yönelim, paylaşılan metinler, fotoğraflar, videolar ve beğeniler gibi unsurlar, bireyin dijital ayak izini oluşturan temel verilerdir (Azucar vd., 2018, s. 150).

Kullanıcılar sosyal medya platformlarını sosyal topluluk etkileşimi, sosyal ticaret, sosyal yayıncılık ve sosyal eğlence gibi farklı amaçlarla kullanırken, her işlemde yeni bir dijital iz bırakmaktadır. Yaptıkları yorumlar, yükledikleri görseller, paylaştıkları konum bilgileri, derecelendirmeler, sosyal alışveriş davranışları ve hükümet uygulamalarıyla olan etkileşimleri, bireyin “dijital DNA”sını oluşturur. Bu dijital ayak izleri, örgütlere ve istihbarat birimlerine kullanıcıların ilgi alanları, sosyal

ve kültürel kimlikleri, mesleki bağlantıları, coğrafi aidiyetleri ve davranış örüntüleri hakkında zengin ve çok katmanlı bilgiler sağlamaktadır (Arya vd., 2019, s. 144-145). Bu noktada büyük veri analitiği (big data analytics), dijital ayak izlerinden anlamlı istihbarat üretmede kritik bir rol üstlenmektedir.

2.4.2. "Honeypot" (Bal Tuzağı) ve Sahte Profil Operasyonları

Honeypot terimi, Türkçe literatürde “bal küpü” olarak karşılık bulmuştur. Kavram, geleneksel olarak ayıları tuzağa çekmek için bal dolu kapların kullanıldığı av yöntemlerinden esinlenilmiştir (Arıkan ve Benzer, 2018). Bilişim güvenliği alanında ise bal küpü sistemleri, saldırganları bilinçli olarak tuzağa çekmek amacıyla tasarlanmış özel sistemlerdir. Bu sistemler, kötü amaçlı faaliyetleri aktif olarak engelleme rolü üstlenmez. Aksine, bal küpü üzerinde normal şartlarda herhangi bir ağ trafiği veya kullanıcı etkileşimi olmaması beklenir. Dolayısıyla bal küpü ile herhangi bir etkileşim tespit edildiğinde, bunun büyük olasılıkla bir saldırgan tarafından gerçekleştirildiği değerlendirilir (Dal, 2019).

Bal küpü sistemlerinde kasıtlı olarak güvenlik açıkları ve zayıf noktalar bırakılır. Bu açıklıklar, saldırganların dikkatini çekerek onları sisteme girmeye teşvik eder. Saldırgan, bal küpü üzerinde farklı saldırı teknikleri ve araçlar deneyebilir. Bu süreçte saldırganın kullandığı yöntemler, araçlar, taktikleri ve davranış kalıpları detaylı biçimde kaydedilir. Elde edilen bu veriler, istihbarat analizi, saldırı tekniklerinin anlaşılması ve gelecekteki saldırıları önleme stratejilerinin geliştirilmesi amacıyla kullanılır (Dal, 2019).

Honeypot kavramının daha gelişmiş bir versiyonu olan Honeynet (Bal Ağı), Türkçe’de “bal ağı” olarak ifade edilmektedir. Bal ağları, yüksek etkileşimli bal küplerinin bir araya getirildiği kolektif sistemlerdir. Tek bir bal küpü tasarlamak bile oldukça zor ve karmaşık bir süreçken, bal ağı birden fazla yüksek etkileşimli bal küpünün sıkı denetim altında birleştirilmesiyle oluşturulur. Bu sistemler genellikle bir güvenlik duvarı veya erişim kontrol cihazının arkasına yerleştirilir ve tüm ağ trafiği titizlikle izlenir (Arıkan ve Benzer, 2018).

Honeynet yapısında hiçbir hizmet simüle edilmez veya taklit edilmez. Sistemler, gerçek işletim sistemleri ve gerçek uygulamalardan oluşur. Saldırganlar, bal ağı içindeki herhangi bir sisteme erişebilir, inceleme yapabilir, saldırı gerçekleştirebilir ve sistemleri istismar edebilir. Bu sayede saldırganlara, sanki gerçek bir üretim

ortamıyla karşı karşıyaymış gibi tam etkileşim imkânı sunulur. Bal ağı, saldırganın davranışlarını, kullandığı exploit'leri ve taktiklerini en gerçekçi şekilde gözlemleme fırsatı sağlar (Hoopes, 2009).

Sosyal medya platformlarında sahte profiller kullanılarak kamu görevlilerinin tuzağa düşürülmesi, yalnızca kişisel şantaj amacıyla sınırlı kalmamakta, stratejik bilgi sızdırma faaliyetlerinde de etkili bir yöntem olarak karşımıza çıkmaktadır. Bir tapu müdürlüğünde tekniker olarak görev yapan kamu personeli, sosyal medya üzerinden tanıştığı bir kişiyle arkadaşlık kurmuştur. Bu kişi, teknikerin duygusal ilişki kurduğu bir profil aracılığıyla kendisini yönlendirerek Adalet Bakanı'na ait tapu kayıtlarının usulsüz sorgulanmasını sağlamış ve sorgu sonuçlarını kendisine göndertmiştir. Tekniker, ifadesinde bu sorgulamayı söz konusu kişinin ısrarı ve kandırması sonucu yaptığını belirtmiştir. Olayın ortaya çıkması üzerine tekniker gözaltına alınarak tutuklanmıştır. Şüpheli kişi de Antalya'da yakalanarak soruşturma için ilgili ilçeye sevk edilmiştir. Aynı usulsüz sorgulama nedeniyle farklı illerdeki iki tapu müdürü de gözaltına alınmıştır (Cnnturk, 2026).

Bu olay, sosyal medyada oluşturulan cazip ve sahte profillerle kamu görevlilerinin göre geleneksel bilişim güvenliği alanında kullanılan bal küpü yöntemine benzer şekilde sahte profil operasyonları ile duygusal ilişki tuzağına (bal tuzağı / honeypot) düşürüldüğü ve hassas resmi bilgilere erişim sağlandığı önemli bir örnektir. Özellikle resmi kayıtlara erişim yetkisi bulunan personelin sosyal medya üzerinden manipüle edilmesi, hem bireysel güvenlik risklerini hem de devlet veri güvenliği açısından ciddi zafiyetler oluşturabileceğini göstermektedir.

2.5. Hibrit Savaş ve Stratejik İletişim

Hibrit savaş kavramı, uluslararası literatürde henüz tam bir uzlaşıya varılamamış tartışmalı bir konudur. Kavramın doğasında yer alan belirsizlik ve çok boyutluluğu, onun net bir şekilde tanımlanmasını güçleştirmektedir. Patrick J. Cullen, bu durumu şu sözlerle özetlemiştir: “Uluslararası alanda hibrit savaş konusunda herkesin üzerinde anlaştığı tek nokta, kimsenin onu tam olarak anlamadığıdır. Ancak NATO ve Birleşmiş Milletler gibi çokuluslu yapılar dâhil olmak üzere herkes, hibrit savaşın ciddi bir tehdit oluşturduğu konusunda hemfikirdir” (Cullen, 2017, s. 3).

Batı literatüründe hibrit savaş kavramının kapsamlı biçimde ele alındığı öncü çalışmalardan biri, 2005 yılında General James N. Mattis ve Yarbay Frank G. Hoffman

tarafından kaleme alınan “Future Warfare: The Rise of Hybrid Wars” başlıklı analizdir. Bu çalışmada “hibrit savaş” terimi ilk kez Hoffman tarafından kullanılmıştır.

Hoffman’a göre sosyal ve teknolojik gelişmeler savaşın “karakterini” dönüştürmüş, ancak savaşın “doğası” değişmemiştir. Asıl değişim, savaşın yürütülme biçiminde yaşanmaktadır. Bu yeni dönemde en olası tehdit, savaşın tarafları arasına düzensiz aktörlerin girmesidir. Terörizm, isyan, gerilla taktikleri, sınırsız savaş ve narkotik suçlar gibi yöntemler, bu düzensiz aktörlerin sıkça başvurduğu araçlar arasında yer almaktadır. Düşman, kendi belirlediği zaman ve mekânda bu yöntemleri kullanırken, karşı tarafın kurallarına bağlı kalmak zorunda değildir ve bu sayede stratejik üstünlük elde etmeye çalışır. 2005 tarihli ABD Ulusal Savunma Stratejisi, tehditleri geleneksel, düzensiz, yıkıcı ve felaket niteliğinde olmak üzere dört kategoride sınıflandırmıştır. Ancak Hoffman’a göre gerçek tehdit, bu dört kategorinin ayrı ayrı varlığı değil, tüm bu savaş türlerinin ve araçlarının bütüncül bir yaklaşımla harmanlandığı yeni bir savaş stratejisidir. İşte bu strateji “hibrit savaş” olarak adlandırılmaktadır (Hoffman ve Mattis, 2005, s. 1-2).

Batı’da hibrit savaşın en yaygın kabul gören tanımları, büyük ölçüde Hoffman’ın çizdiği kavramsal çerçeveye örtüşmektedir. Nitekim 2018 yılında Brüksel’de düzenlenen NATO Zirvesi’nin nihai bildirisinde hibrit savaş şu şekilde tanımlanmıştır: “Dezenformasyon, siber saldırılar, yönlendirilmiş göç hareketleri, casusluk, uluslararası hukukun manipülasyonu, güç tehdidi (hem düzensiz silahlı gruplar hem de konvansiyonel kuvvetler aracılığıyla), siyasi yıkıcılık, sabotaj, terörizm, ekonomik baskı ve enerji bağımlılığı gibi çok çeşitli yöntem, araç ve tekniklerin bir arada kullanıldığı savaş stratejisi.” Bu tanım, Hoffman’ın analizleriyle önemli ölçüde paralellik göstermektedir. Bu durum, Batı hibrit savaş literatürünün büyük oranda Hoffman’ın çalışmalarından beslendiğini ortaya koymaktadır (NATO StratCom COE, 2019, s. 8).

Rusya Genelkurmay Başkanı Valery Gerasimov’un 2013 yılında yayımladığı “The Value of Science Is in the Foresight” (Bilimin Değeri Öngörüsündedir) başlıklı makalesi, aslında bir doktrin metni olmaktan ziyade, savaşın değişen doğasına dair analitik bir değerlendirmeydi. Ancak Batılı stratejistler ve uzmanlar bu makaleyi “Gerasimov Doktrini” olarak nitelendirmiş ve literatüre bu isimle yerleşmiştir. Gerasimov makalesinde “hibrit savaş” kavramını doğrudan kullanmasa da, tarif ettiği

yöntem ve taktiklerin hibrit savaş konseptiyle derin bir uyum göstermesi, çalışmayı hibrit savaşın teorik temellerini oluşturan önemli metinlerden biri haline getirmiştir.

Gerasimov, günümüzde savaş ile barış arasındaki sınırların giderek bulanıklaştığını vurgulamaktadır. Klasik savaşlarda olduğu gibi ilan edilerek başlayan çatışmaların yerini, ne zaman başladığı belirsiz olan ve alışılmadık yöntemlerin hâkim olduğu yeni nesil savaşlar almıştır. Arap Baharı sürecinde Tunus, Mısır, Libya ve Suriye’de yaşanan olaylar, bu yeni savaş biçiminin somut örnekleri olarak gösterilebilir. En istikrarlı görünen rejimlerin bile kısa sürede iç savaş, dış müdahale ve siyasi kaosla karşı karşıya kalabildiğini gösteren bu vakalar, 21. yüzyıl savaşlarının karakteristiğini yansıtmaktadır (Gerasimov, 2016, s. 24).

Hibrit savaş, savaş ile barış arasındaki “gri bölgede” yürütülür. En belirgin özelliği, failin kimliğinin kasıtlı olarak belirsiz bırakılması ve eylemlerin kolayca inkâr edilebilmesidir. Bu yönüyle hibrit savaş, doğası gereği bir belirsizlik stratejisidir (Akgül, 2021, s. 417). Hibrit tehditler, saldırıya uğrayan tarafın eylemi tanımlamakta, faili tespit etmekte ve kamuoyuyla paylaşmakta zorlandığı yeni nesil tehditlerdir. Çoğu durumda saldırının arkasındaki aktör ya bilinmez ya da kasıtlı olarak gizlenir. Bu durum, hükümetlerin tehdit değerlendirmelerini kendi politik önceliklerine ve çıkar analizlerine dayandırmasına yol açar (NATO StratCom COE, 2019, s. 8).

Bu belirsizlik, hibrit savaşın temel unsurlarından biridir ve özellikle “küçük yeşil adamlar” (Kırım ilhakı sırasında kullanılan kimliği belirsiz askerler), kaynağı tespit edilemeyen siber saldırılar ve vekil güçlerin (proxy) kullanımı gibi yöntemlerle somutlaşır. Bu taktikler, failin kimliğini gizlerken aynı zamanda uluslararası hukuku ihlal eden eylemler için “makul inkâr edilebilirlik” (plausible deniability) perdesi sağlar (Reichborn-Kjennerud ve Cullen, 2016, s. 2).

Sun Tzu’nun “vurabilecekken vuramayacakmış gibi görünmek” veya “yaklaşırken uzaklaşıyormuş gibi yapmak” taktikleri, düşmanın algısını yöneterek onu hataya sevk eden klasik aldatmaca yöntemleridir. Benzer şekilde “kargaşa yarat ve ele geçir” ilkesi, hedef ülkede toplumsal kaos ve siyasi istikrarsızlık yaratarak zayıflatma stratejisinin antik çağdaki karşılığıdır (Tzu, 2022, s. 2).

NATO Stratejik İletişim Mükemmeliyet Merkezi (StratCom), 2014 yılında Letonya’nın başkenti Riga’da kurulmuş uluslararası bir güvenlik kurumudur. Merkez, “savaşların insanların zihninde başladığı ve savunmanın da zihinde başlaması

gerektiği” anlayışına dayanmaktadır. Estonya, Almanya, İtalya, Letonya, Litvanya, Polonya ve Birleşik Krallık tarafından imzalanan mutabakat zaptıyla kurulan StratCom, 1 Eylül 2014’te NATO akreditasyonunu almıştır. Kurum, NATO’nun komuta yapısının dışında yer almakla birlikte, NATO’nun hedefleri, rolleri ve misyonları konusunda uygun, zamanında, doğru ve etkili iletişim kurulmasına katkı sağlamayı amaçlamaktadır. StratCom, sivil ve askeri, özel sektör ve akademik alanlardan çok uluslu uzmanların katılımıyla çalışmakta ve modern analiz, araştırma ile karar destek araçlarını kullanmaktadır. Merkezin faaliyetleri dezenformasyonla mücadeleden daha geniş bir yelpazeyi kapsasa da, son yıllarda yayınlarının önemli bir bölümünü dezenformasyon tehdidi oluşturmaktadır. Bu durum, dezenformasyonun günümüzde ne kadar ciddi bir güvenlik sorunu haline geldiğinin de bir göstergesidir (Arslan, 2025).

2.5.1. Psikolojik Savaş ve Etki Operasyonları

Psikolojik savaş, bir topluluğun veya devletin, diğer toplulukların bakış açılarını, duygularını, düşüncelerini ve davranışlarını kendi çıkarları doğrultusunda etkilemek ve yönlendirmek amacıyla çeşitli güç unsurlarını kullandığı stratejik bir yaklaşımdır. Bu kavram, hedef kitlenin zihinsel ve duygusal yapısını belirli amaçlar doğrultusunda değiştirmeye yönelik politik, askeri, ekonomik, sosyolojik ve teknolojik araçların tümünü kapsar (Toker ve Dilmaç, 1992). Temel amacı, askeri güç kullanmadan hedef alınan bireylerin, grupların veya toplumların düşünce yapılarını, duygusal durumlarını ve davranış kalıplarını etkilemektir.

Psikolojik savaş genellikle propaganda, manipülasyon, bilgi kontrolü ve duygusal baskı gibi yöntemleri içerir. Bu stratejinin çekirdeğini oluşturan propaganda, yanıltıcı bilgi yayma, duygusal manipülasyon ve psikolojik baskı unsurlarından oluşur. Genel olarak, toplumların algılarını kontrol etmek ve karar alma süreçlerini istenilen yönde şekillendirmek amacıyla uygulanır. Psikolojik savaş, bir düşman topluluğunu veya ordusunu etkisiz hale getirmeyi, onları uyumlu veya bağımlı kılmayı ya da yok etmeyi hedefleyen eylemler olarak da tanımlanabilir (Özdağ, 2008). Daha geniş bir perspektiften bakıldığında ise psikolojik harekât, savaş veya barış zamanlarında dost veya düşman hedef kitlelerin davranışlarını etkileyerek politik ve askeri hedeflere ulaşmayı desteklemek üzere ekonomik, sosyal, kültürel, siyasi, askeri ve teknolojik güç unsurlarının planlı ve koordineli biçimde kullanılmasını ifade eder. Bu bağlamda

propaganda, belirli bir grubun düşünce, duygu ve eylemlerini istenen amaçlar doğrultusunda etkileme çabası olarak öne çıkmaktadır (Yılmaz, 2008).

Bilgi manipülasyonu ve algı yönetimi, psikolojik savaşın en önemli araçları arasında yer alır. Bu süreçte medya, iletişim teknolojileri ve dijital platformlar kritik rol oynar. Hedef kitlenin duygusal tepkilerini yönlendirmek, belirli görüşleri güçlendirmek veya zayıflatmak amacıyla duygusal baskı teknikleri sıkça kullanılır. Psikolojik savaşın bir diğer temel unsuru ise dezenformasyon ve manipülasyon teknikleridir. Gerçek olmayan bilgilerin yayılması veya gerçek bilgilerin kasıtlı olarak çarpıtılması, hedef kitlenin güvenini sarsabilir ve istenilen toplumsal atmosferi yaratabilir (Ölçekçi, 2018). Bu stratejiler, askeri müdahale olmaksızın güç kullanımını hedef alır ve bireylerin, grupların veya toplumların düşünsel ve duygusal süreçlerini kontrol altına alarak belirli amaçlar doğrultusunda yönlendirmeyi amaçlar.

Psikolojik savaş faaliyetleri, yalnızca kısa vadeli tepkiler yaratmakla sınırlı değildir. Uzun vadeli stratejilerle hedef toplumun sosyal güç dayanaklarını sistematik olarak zayıflatmayı veya ortadan kaldırmayı da içerebilir. Çağlayan'a (2017, s. 59-60) göre, bu tür uzun soluklu girişimler şu unsurları hedef alır:

- Birey-ahlak yabancılaşması
- Toplum-değerler yabancılaşması
- Aydın-halk yabancılaşması
- Toplum-devlet yabancılaşması
- Alt kimlik yabancılaşmaları
- Bölgesel yabancılaşmalar
- Dayanışma ve uzlaşma kültürünün yok edilmesi
- Yeni ulusal, etnik ve dini kimlikler inşası yoluyla dışlama, ayrıştırma ve çatışma kültürünün geliştirilmesi

Psikolojik olarak savunmasız hale getirilen bir toplum, birlik ve düzen duygusundan uzaklaşır; devlet ve diğer sosyal kurumlara olan güvenini kaybeder; geçmişine ve geleceğine karşı sorumluluk hissinden yoksun kalır. Bu durumun nihai amacı, hedef toplumun düşünce, tutum ve davranışlarını psikolojik savaş uygulayan tarafın kontrolü altına almaktır (Toker ve Dilmaç, 1992).

Kandel’e göre (2020, s. 281), insanlar doğru ile yanlış ayırt edebilen en zeki varlıklar olmasına rağmen, bilgi bozukluklarından (information disorder) bilinçli veya bilinçsiz olarak etkilenebilmektedir. Bu etkilenmenin arkasında ekonomik, siyasi ve psikolojik motivasyonlar yattığı belirtilmektedir. Bradshaw (2020, s. 44-45), bilgi ve iletişim teknolojilerinin toplumsal ve politik dönüşümü mümkün kılan güçlü bir araç olduğunu vurgulamakta ve bu teknolojilerin aktörlere geleneksel olmayan savaş yöntemleri için yeni fırsatlar sunduğunu ifade etmektedir. Teknolojideki her ilerleme, propaganda ve dezenformasyonun etki alanını da genişletmekte ve dönüştürmektedir.

RAND Corporation’ın “Foundations of Effective Influence Operations” başlıklı raporunda (Larson vd., 2009, s. 2), etki operasyonları şu şekilde tanımlanmaktadır: “Etki operasyonları; barış zamanında, kriz anlarında, çatışma sürecinde ve çatışma sonrasında yabancı hedef kitlelerin, ABD’nin ulusal çıkarlarını ve hedeflerini destekleyen tutum, davranış veya kararlar almasını teşvik etmek amacıyla diplomatik, enformasyonel, askeri, ekonomik ve diğer ulusal kabiliyetlerin koordineli, entegre ve senkronize biçimde uygulanmasıdır.”

2.5.2. Siber Operasyonlar ve Zararlı Yazılım Yayılımı (Malware)

Siber operasyonların uluslararası hukuk açısından incelenmesinde, literatürde “siber muharebe”, “bilgi operasyonu” (information operation), “bilgisayar ağı saldırısı” (computer network attack – CNA) ve “siber saldırı” (cyber attack) gibi farklı terimler sıklıkla kullanılmaktadır (Nguyen, 2013). Bu terimlerin her biri, konuya farklı açılardan yaklaşırsa da, çalışmanın amacı açısından bazı sınırlılıklar taşımaktadır.

“Siber muharebe” kavramı, teknik olarak yalnızca silahlı çatışma sırasında siber teknolojilerin kullanıldığı düşmanca eylemleri çağrıştırdığı için daha dar kapsamlıdır ve bu çalışmada tercih edilmemiştir (Roscini, 2014). “Bilgi operasyonu” ise bilgisayar ağı operasyonlarının yanı sıra psikolojik operasyonlar, askeri aldatma, operasyon güvenliği ve elektronik harp gibi geniş bir yelpazeyi içerdiğinden, çalışmanın odaklandığı siber alandaki saldırgan operasyonları ifade etmek için fazla geniş bir kavramdır (Schreier, 2015). “Bilgisayar ağı saldırısı” kavramı ise bilgisayar ağı operasyonları doktriniyle sıkı bir ilişki içinde olması nedeniyle zamanla yerini “siber saldırı” terimine bırakmıştır (Cartwright, 2011). Ancak “siber saldırı” ifadesi de genellikle kuvvet kullanma eşiğine ulaşan veya özellikle düşman bilgisayar sistemlerini ve verilerini aksatmayı, engellemeyi, manipüle etmeyi ya da yok etmeyi

amaçlayan operasyonları tanımlamaktadır. Bu nedenle, tartışmalı hususların geniş bir perspektiften değerlendirilebilmesi amacıyla çalışmada daha kapsayıcı olan “siber operasyon” kavramı tercih edilmiştir.

Siber operasyon, genel olarak “belirli amaçlara ulaşmak üzere çeşitli siber araçların kullanıldığı ve siber alanda veya siber alan aracılığıyla gerçekleştirilen operasyonlar” şeklinde tanımlanabilir (Roscini, 2014). Bu kavram, siber alanda yürütülen eylemlerin tamamını kapsayan geniş ve tarafsız bir terminoloji sunmaktadır.

Zararlı yazılımlar (malware), siber saldırganlar tarafından belirli kötü amaçlı eylemleri gerçekleştirmek üzere geliştirilen yazılımlardır. Bu yazılımlar doğrudan bir hedef olabileceği gibi, daha büyük bir amaca hizmet eden yardımcı araç olarak da kullanılabilir. Zararlı yazılımlar genel olarak şu işlevleri yerine getirmektedir:

- Sistemin normal çalışmasını bozma,
- Sistem güvenliğini riske atma,
- Sistemlere yetkisiz erişim sağlama,
- Reklam yayma,
- İstenmeyen e-posta (spam) gönderme,
- Dosyaları şifreleyerek fidye talep etme (ransomware),
- Hassas bilgileri (kredi kartı bilgileri, bankacılık şifreleri vb.) ele geçirme,
- Büyük ölçekli servis dışı bırakma saldırıları (DDoS) düzenleme,
- Devletler arası istihbari ve stratejik bilgi toplama.

Bu tür yazılımlar, siber saldırganların en sık başvurduğu ve en etkili araçlardan biri konumundadır (Wood vd., 2016).

2.5.3. Terör Örgütleri(PKK/DEAŞ/FETÖ) ve Devletlerin Dezenformasyon Faaliyetleri

Günümüzde sosyal medya, yalnızca bireylerin iletişim kurduğu bir mecra olmaktan çıkıp sosyalleşme, kendini ifade etme ve farklı örgütlü yapılara katılım sağlama gibi işlevleri de üstlenmeye başlamıştır. Ancak teknolojinin sunduğu kolaylıklar, beraberinde bilgi kirliliği, sahte haberler ve dezenformasyon gibi karmaşaları da getirmiştir. Özellikle siyasal iletişimde, hedef kitle üzerinde istenilen

algıyı oluşturma amacıyla dezenformasyonun yaygın biçimde kullanıldığı görülmektedir (Ayhan ve Erkan, 2018) Sosyal Medyada yapılan dezenformasyon ve türleri kitleleri yönlendirme gücünden dolayı tüm ülkeleri ilgilendirmektedir. Toplumu manipüle ederek yayılan yanlış bilgiler toplumu yanlış yönlendirebilmektedir (Aydın,2023).

Dezenformasyon olgusunu incelerken, demokratik olmayan rejimleri otoriter ve totaliter sistemler olarak ayırmak büyük önem taşımaktadır. Zira devletin yapısı, siyasal felsefesi ve yönetici elitlerin devlete yükledikleri misyon, dezenformasyon faaliyetlerinin kapsamını, derinliğini ve yoğunluğunu doğrudan belirlemektedir.

Otoriter sistemlerde devlet, genellikle modernleştirici, kalkınmacı ve uluslaştırıcı bir güç olarak konumlandırılır. Bu tür rejimler dezenformasyona başvurmakla birlikte, yeni bir insan tipi veya yeni bir toplum yaratma gibi aşırı iddialı ve totaliter hedeflere sahip olmadıkları için dezenformasyon faaliyetleri görece daha sınırlı ve “masum” bir nitelik taşır (Yayla, 2014).

Totaliter sistemlerde ise dezenformasyon, devletin temel dayanaklarından ve rutin faaliyetlerinden biri haline gelmektedir (Kolakowski, 1999). Bu rejimler, bilinen dezenformasyon yöntemlerini sürekli mükemmelleştirmekle kalmaz, aynı zamanda yeni teknikler de geliştirir. Bu amaçla özel devlet organları kurulur ve dezenformasyon konusunda uzmanlaşmış kadrolar yetiştirilir. Bu organlar ve uzmanlar, hem kendi ülkelerindeki halkı hem de dış dünyada rakip gördükleri toplumları ve devletleri hedef alır. Yeni bir insan ve toplum yaratma hırsı ile hasım ülkeyi zayıflatma veya dünyaya hâkim olma ideali, totaliter rejimlerin dezenformasyon faaliyetlerine olağanüstü bir enerji ve sistematiklik kazandırır (Yayla, 2020).

Dezenformasyonun bir diğer önemli aktörü ise terör örgütleridir. Türkiye, uzun yıllardır PKK ve DEAŞ gibi terör örgütleriyle mücadele etmekteyken, son dönemde bunlara bir de din istismarı üzerine kurulu Fethullahçı Terör Örgütü (FETÖ) eklenmiştir. FETÖ, uzun yıllar boyunca “ışık evleri” adı verilen gizli yapılarda “altın nesil” olarak nitelendirdiği radikal militanlar yetiştirmiş ve bu kadroları devletin kritik kurumlarına sızdırarak önemli güç merkezlerini ele geçirmiştir (Arslan, 2016, s. 86). Güç zehirlenmesine kapılan örgüt ele başı Fethullah Gülen, bağlı olduğu odakların yönlendirmesiyle önce 17-25 Aralık 2013’te bürokratik-sivil darbe girişiminde bulunmuş, bu girişim başarısız olunca 15 Temmuz 2016’da askeri darbe teşebbüsüne

kalkışmıştır (Arslan, 2016, s. 256). Her iki teşebbüs de Türk milletinin ve meşru iktidarın kararlı direnişi sayesinde engellenmiştir.

Darbe girişimlerinin başarısız olmasının ardından FETÖ, strateji değiştirerek PKK ve DEAŞ gibi terör örgütlerinin sıkça kullandığı yönteme başvurmuştur. Sosyal medya üzerinden yoğun dezenformasyon, manipülasyon ve karalama kampanyaları yürütmeye başlamıştır. Bu faaliyetlerin temel amacı, Türkiye’de kamu düzenini ve toplumsal güvenliğı bozmak, halk sağlığını tehlikeye atmak ve Türkiye’yi uluslararası alanda yalnızlaştırmaktır. Örgüt, bu doğrultuda Türkiye’nin tüm dış düşmanlarıyla işbirliğı yapmaktan çekinmemekte ve Türkiye aleyhine yürütülen her türlü propaganda, algı operasyonu ve kumpasta aktif rol almaktadır (Arslan, 2022).

Terör örgütlerinin Türkiye karşıtlığı uzun yıllardır bilinen ve kanıksanmış bir olgudur. Ancak daha kaygı verici olan husus, bazı sorumluluk sahibi kişilerin ve makam sahiplerinin, zaman zaman bu örgütlerin yaydığı yalan ve yanlış bilgileri sorgulamadan paylaşmasıdır. Bu tür paylaşımlar, terör örgütlerinin ekmeğine yağ sürmekte ve onların dezenformasyon faaliyetlerini güçlendirmektedir. Özellikle sosyal medyada post-truth (hakikat-ötesi) söylemler, dezenformasyon, algı yönetimi, propaganda ve manipülasyon içeren mesajlar, kamu düzenini, toplumsal güvenliğı ve halk sağlığını ciddi biçimde tehdit edebilecek sonuçlar doğurabilmektedir. Bu nedenle hem hukuki yaptırımlardan kaçınmak hem de toplumsal kaos ve kriz ortamı yaratmamak açısından, sosyal medyada paylaşılan bilgilere karşı azami dikkat ve eleştirel yaklaşım gösterilmesi büyük önem taşımaktadır (Arslan, 2022).

2.6. Sosyal Medya İle İlgili Yasal Düzenlemeler: Ülke Örnekleri

Günümüz dijital çağında sosyal medya platformları, hem ifade özgürlüğünün en önemli alanlarından biri hem de kamu düzenini, ulusal güvenliğı ve bireysel hakları tehdit edebilecek risklerin yoğunlaştığı bir ortam haline gelmiştir. Bu ikili yapı, birçok devleti sosyal medya içeriklerini düzenleyen özel yasal çerçeveler oluşturmaya yöneltmiştir. Ülkeler, bu düzenlemelerde kendi siyasi, kültürel ve güvenlik önceliklerine göre farklı yaklaşımlar benimsemektedir. Tezin bu bölümünde farklı ülkelerin sosyal medya yasal düzenlemeleri ele alınacaktır.

2.6.1. Almanya ve AB: Dijital Hizmet Yasası

Almanya’da internet ortamındaki faaliyetleri, bu faaliyetleri yürüten aktörlerin sorumluluklarını ve erişim engelleme konularını düzenleyen temel yasal

metin, 1 Mart 2007 tarihli Tele medya Kanunu'dur. Ancak sosyal ağlarda hukuka aykırı içeriklerin hızlı ve etkili biçimde engellenmesinde bu Kanun'un yetersiz kaldığının anlaşılması üzerine, 1 Eylül 2017 tarihinde Sosyal Ağ Kanunu (Netzwerkdurchsetzungsgesetz – NetzDG) yürürlüğe konulmuştur. Bu Kanun'da öncelikle “sosyal ağ” kavramı tanımlanmış, ancak tüm sosyal ağlar kapsam dışında bırakılmamıştır. Gazetecilik veya yayıncılık faaliyeti yürüten platformlar, bireysel iletişim amaçlı kullanılan platformlar, belirli bir içeriğin yayılmasını sağlayan platformlar ve Almanya'da iki milyonun altında kayıtlı kullanıcıya sahip platformlar Kanun kapsamı dışında tutulmuştur.

Almanya'daki Sosyal Ağ Kanunu, hukuka aykırı içeriklere karşı şeffaf ve etkili bir şikâyet mekanizması kurulmasını öngörmektedir. Bu ülkede şikâyet sistemi, hukuka aykırı içeriklerin kaldırılması veya erişimin engellenmesinde temel rol oynamaktadır. Türkiye'de ise bu konuda sulh ceza hâkimlikleri belirleyici konumdadır. Almanya'da uygulanan şikâyet sistemi, Türkiye'deki “uyar-kaldır” mekanizmasına büyük ölçüde benzemektedir. Bu sisteme göre, hakkı ihlal edilen kişi veya kamu kurumları, yargı yoluna başvurmadan önce doğrudan sosyal ağ işletmecisine başvurarak içeriğin kaldırılmasını veya engellenmesini talep edebilmektedir. 5651 sayılı Kanun'da “uyar-kaldır” sisteminden bahsedilmesine rağmen, bu sistemin etkili biçimde işletilebilmesi için sosyal ağ işletmecilerine düşen yükümlülükler ve alınması gereken tedbirler yeterince düzenlenmemiştir. Bu nedenle uyar-kaldır mekanizmasının işleyişini ayrıntılı biçimde düzenleyen ek düzenlemelere ihtiyaç duyulmaktadır. Avrupa Birliği düzeyinde sosyal medya düzenlemelerinin en kapsamlısı, Dijital Hizmetler Yasası (Digital Services Act – DSA) olarak kabul edilmektedir. DSA, sosyal ağlar, içerik paylaşım platformları ve diğer çevrimiçi aracı hizmet sağlayıcılarının çalışma prensiplerini düzenlemek amacıyla hazırlanmıştır. Yasanın temel amacı, AB üyesi ülkelerin vatandaşlarının temel haklarını ve tüketicilerin çıkarlarını dijital ortamda korumaktır. Bunun yanı sıra, ticari kuruluşların büyüme ve rekabet gücünü destekleyen hükümler de içermektedir. DSA kapsamında toplumun geneli ve bireyler için sistemik platformlarda daha fazla demokratik denetim ve gözetim, temel hakların korunması, manipülasyon ve dezenformasyon gibi sistemik risklerin azaltılması, çevrimiçi ortamda daha fazla şeffaflık ve kullanıcı tercihi, çocukların daha güçlü korunması ve yasa dışı içeriklere maruz kalma riskinin düşürülmesi hedeflenmiştir. Yasada şirketler, internet servis sağlayıcıları, önbellek servis sağlayıcıları,

hosting/depolama hizmeti sağlayıcıları, çevrimiçi platformlar ve çok büyük çevrimiçi platformlar (Very Large Online Platforms) olarak sınıflandırılmış ve her bir kademeye farklı yükümlülükler getirilmiştir. En ağır düzenlemeler ve yaptırımlar ise “çok büyük çevrim içi platformlar” olarak tanımlanan dünyanın önde gelen sosyal medya şirketlerine yönelik olarak öngörülmüştür (eur-lex.europa.eu, 2022).

2.6.2. Çin ve Rusya Uygulamaları

İnternet içeriklerini denetlemek amacıyla çıkarılan yasalar ve yönetmelikler, birçok devletin dijital sansür politikalarının temelini oluşturmaktadır. Bu yasal çerçeve, hangi içeriklerin yasaklanacağını, kısıtlanacağını veya erişime engelleneceğini belirleyen temel araç niteliğindedir.

Çin, dijital denetim konusunda dünyanın en kapsamlı ve sistematik modelini uygulamaktadır. “Büyük Güvenlik Duvarı” (Great Firewall) olarak bilinen ileri düzey filtreleme ve engelleme sistemiyle hükümet, istenmeyen içerikleri ülke genelinde etkili biçimde bloke etmektedir. Yabancı sosyal medya platformları (Facebook, X, Instagram, YouTube vb.) büyük ölçüde erişime kapatılmış olup, bunların yerine devlet denetimindeki yerli alternatifler (WeChat, Weibo, Douyin/TikTok vb.) teşvik edilmektedir. Bu platformlar üzerinden yürütülen dijital iletişim, sıkı içerik denetimi, gerçek isim politikası ve gelişmiş gözetim teknolojileriyle yakından takip edilmektedir. Böylece Çin hükümeti, dijital ekosistem üzerindeki mutlak kontrolünü sürdürmektedir (Creemers, 2015).

Rusya’da da internet içerikleri üzerinde giderek artan bir denetim mekanizması kurulmuştur. Özellikle hükümeti eleştiren blog yazarları, gazeteciler ve muhalif aktivistler üzerinde yoğun baskılar uygulanmaktadır. “Yabancı ajan” yasası, veri yerelleştirme zorunluluğu ve çeşitli internet kısıtlama düzenlemeleriyle Rusya, yabancı platformları hedef almakta ve yerli alternatifleri (VK, RuTube vb.) desteklemektedir. Bu düzenlemeler, muhalif sesleri susturma ve kamuoyunu istenilen yönde şekillendirme amacını taşımaktadır. Her iki ülkede de devlet, interneti yalnızca bir iletişim aracı olarak değil, aynı zamanda toplumsal kontrol, siyasi istikrarı koruma ve ulusal güvenlik aracı olarak görmektedir. Bu yaklaşım, dijital özgürlükler ile devlet egemenliği arasındaki gerilimi en keskin biçimde ortaya koymaktadır (Yalınız, 2025).

2.6.3. Türkiye’deki Mevcut Yasal Düzenlemeler ve Sosyal Medya Yasası

Türkiye’de sosyal medya platformlarına yönelik yasal düzenlemeler, son yıllarda hem akademik çalışmalarda hem de kamuoyunda sıkça tartışılan önemli bir konu haline gelmiştir. Özellikle kullanıcıların veri güvenliği, içerik denetimi, ifade özgürlüğü ve platformların sorumlulukları gibi hususlar, düzenleyici otoritelerin öncelikli gündem maddeleri arasında yer almaktadır.

7253 sayılı Sosyal Medya Yasası ile getirilen temsilci bulundurma zorunluluğu, içerik kaldırma yükümlülükleri, veri saklama kuralları ve dezenformasyonla mücadele mekanizmaları gibi düzenlemelerin uygulanması, merkezi ve etkili bir politika koordinasyonunu gerektirmektedir. Politika kurullarının bu alandaki rolü, sosyal medya kaynaklı güvenlik tehditlerine karşı hızlı ve bütüncül yanıt geliştirilmesini sağlayacak stratejik bir araç niteliğindedir.

Sosyal medya düzenlemelerinin temel amacı, kullanıcıların kişisel verilerinin korunması, hukuka aykırı içeriklerin yayılmasının önlenmesi ve platformların Türkiye’de daha sorumlu ve şeffaf bir şekilde faaliyet göstermelerini sağlamaktır. Bu düzenlemeler, sosyal medya şirketlerini belirli kriterlere tabi tutarak kullanıcılar için önemli güvenceler oluşturmayı hedeflemektedir (Dülger ve Özkan, 2021).

Bu alandaki en önemli adım, 2020 yılında yürürlüğe giren ve kamuoyunda “Sosyal Medya Kanunu” olarak bilinen düzenlemedir. Bu düzenleme ile sosyal medya platformlarına önemli yükümlülükler getirilmiştir. Bunların başında, Türkiye’de belirli bir kullanıcı sayısını aşan platformların Türkiye’de temsilci bulundurma zorunluluğu gelmektedir. Ayrıca kullanıcı verilerinin Türkiye sınırları içinde saklanması zorunluluğu da getirilmiştir. Bu sayede yetkili makamların erişimi ve denetimi kolaylaştırılmış, kullanıcı verilerinin korunması açısından önemli bir adım atılmıştır (Dülger ve Özkan, 2021).

Türkiye’de sosyal medya düzenlemeleri uzun süredir tartışılmaktadır. Bu düzenlemeler, kullanıcıların kişisel verilerinin korunması, içerik denetimi ve iletişim özgürlüğü gibi kritik konuları kapsamaktadır. Platformların faaliyetlerini ve kullanıcı deneyimlerini doğrudan etkileyen bu kurallar, hem bireysel hakların korunması hem de toplumsal güvenlik açısından büyük önem taşımaktadır (Arslan ve Özel, 2021, s. 259-265).

Genel olarak Türkiye’deki sosyal medya düzenlemeleri, kullanıcı haklarını korumayı ve platformların daha sorumlu davranmasını sağlamayı amaçlamaktadır. Bu düzenlemeler, hem kullanıcılar hem de sosyal medya şirketleri açısından önemli değişiklikler getirerek Türk hukuku çerçevesinde daha etkin ve denetlenebilir bir dijital ortam oluşturmayı hedeflemektedir (Oymak, 2022).

2020 yılında yürürlüğe giren Sosyal Medya Kanunu’nun getirdiği başlıca yükümlülükler şu şekilde özetlenebilir (Oymak, 2022, s. 507-509):

- **Temsilci Atama Zorunluluğu:** Günlük erişim sayısı belirli bir eşiği aşan sosyal medya platformlarının Türkiye’de temsilci bulundurması zorunlu kılınmıştır. Bu temsilci, yasal taleplere hızlı yanıt verme ve iletişimi kolaylaştırma görevini üstlenmektedir.
- **Veri Saklama Zorunluluğu:** Kullanıcı verilerinin Türkiye sınırları içinde saklanması zorunluluğu getirilmiştir. Böylece yetkili makamların erişimi ve denetimi önemli ölçüde kolaylaştırılmıştır.
- **Şikâyet ve İçerik Kaldırma Yükümlülüğü:** Platformlar, kişilik haklarına saldırı, suç unsuru taşıyan içerikler veya kişisel verilerin hukuka aykırı paylaşımı gibi durumlarda şikâyetleri hızlı bir şekilde değerlendirmek ve gerekli tedbirleri almakla yükümlüdür.
- **Reklam ve Tanıtım Yükümlülükleri:** Reklam verenlerin ve tanıtım yapanların kimliklerinin doğrulanması ile reklam içeriklerinin şeffaflık kurallarına uygun olması zorunlu hale getirilmiştir.

Bu düzenlemeler, Türkiye’de sosyal medya ekosisteminin daha sorumlu, şeffaf ve hukuka uygun bir yapıya kavuşması yönünde atılmış önemli adımlar olarak değerlendirilmektedir.

Son dönemde Türkiye’de sosyal medya alanında atılan en önemli adımlardan biri, çocukları dijital risklerden koruma amacıyla yapılan düzenlemedir. Aile ve Sosyal Hizmetler Bakanı Mahinur Özdemir Göktaş, 15 yaşın altındaki çocukların sosyal medya kullanımı konusunda yeni bir yasa teklifinin hazırlandığını açıklamıştır. Bakan Göktaş, kabine toplantısı sonrası yaptığı açıklamada, “15 yaş altına yönelik sosyal medya düzenlemesini de içeren torba yasa taslağımızı bu ay sonunda mecliste ilgili komisyona sevk ediyoruz” demiştir (BBC, 2026).

Bu düzenleme ile sosyal medya platformlarına, 15 yaşından küçük çocuklara hiçbir şekilde hizmet sunmama, hesap açtırmama ve zararlı içeriklere karşı etkili filtreleme sistemleri kurma yükümlülüğü getirilmesi hedeflenmektedir. Bakan Göktaş, “Çocuklarımızı her türlü risk ve tehditten, zararlı içeriklerden korumak en önemli önceliğimizdir” diyerek, platformlara daha fazla sorumluluk yüklenmesinin amaçlandığını vurgulamıştır (BBC, 2026).

Bu gelişme, dünyada da benzer tartışmaların yaşandığı bir dönemde gerçekleşmektedir. Avustralya Kasım 2025’te 16 yaş altına yönelik dünyanın en kapsamlı sosyal medya yasağını hayata geçirmiş, İngiltere’de ise küçük yaştakilere sosyal medya ve cep telefonu kullanımının kısıtlanması yoğun biçimde tartışılmaktadır. Türkiye’nin bu alandaki adımı, çocuk ve gençlerin dijital güvenliklerini koruma konusunda uluslararası eğilimle uyumlu bir adım olarak değerlendirilmektedir (BBC, 2026).

III. BÖLÜM

SOSYAL MEDYANIN DEVLET VE KAMU GÜVENLİĞİNE ETKİSİ: UYGULAMA VE VAKA ANALİZLERİ

Güvenlik, canlı ya da cansız varlıklara yönelen korku, tehdit veya saldırılara karşı korunma ve savunma mekanizması olarak tanımlanabilir. Olası riskler karşısında bireysel veya kurumsal düzeyde engelleme, önleme ya da karşı tepki geliştirme şeklinde kendini gösterir. Bu tepki, temel olarak kendini koruma ve hayatta kalma içgüdüsünden kaynaklandığı için doğal bir davranış biçimi olarak değerlendirilir. Kamu düzeni ve güvenliğin sürdürülmesi amacıyla yasama organları tarafından oluşturulan anayasa ve kanunlar gibi maddi yaptırımlar da bu ihtiyacın kurumsal yansımasıdır. Türk Dil Kurumu'na göre güvenlik, "toplum yaşamında yasal düzenin kesintisiz devam etmesi ve bireylerin korkusuzca yaşayabilmesi durumu" ya da kısaca "emniyetli olma halidir. Milli güvenlik ise daha özel bir kavram olarak devletin iç ve dış her türlü tehdide karşı korunmasını ifade eder (Güvenlik Terimleri Sözlüğü, 2017, s. 386).

Devlet, vatandaşları için koruyucu ve kollayıcı bir otorite olarak görülür; bireylerin huzur içinde, hayati endişelerden uzak ve korkusuzca yaşamasını sağlayan denetim mekanizmasıdır (Acar ve Urhal, 2007, ss. 76-77). Devletler açısından güvenlik, beslenme ve barınma gibi temel bir ihtiyaçtır ve iç ile dış tehditler bir bütün olarak ele alınmalıdır (Acar ve Urhal, 2007, ss. 128-129). İç sorunların çözümsüz kalması halinde dış tehdit boyutuna evrilmesi oldukça olasıdır. Tarihimizde buna örnek olarak Osmanlı'da yaşanan Cem Sultan olayı gösterilebilir: Başlangıçta iç mesele olan

bu durum, zamanında çözülemeyince dış aktörlerin müdahalesine zemin hazırlamış, devleti itibarsızlaştırmış ve güç kaybına yol açmıştır.

Teknolojinin gelişmesiyle güvenlik olgusu da dönüşüme uğramıştır. Korunma isteğinin kurumsallaşmasıyla devletler, bilgi ve verilerini dış tehditlere karşı korumak için özel birimler ve kurumlar oluşturmuştur. Kamu güvenliği ise ulusal güvenliğin bir parçası olarak, devletin iç ve dış her türlü tehdide karşı sürekli korunma halini kapsar. Bu ihtiyaç günümüzde yeni teknolojik trendlerle daha fazla önem kazanmıştır (Ateş, 2012, ss. 14-15).

Ülkeler fiziki sınırlarını korusa da çevrimiçi dünyanın sınırları belirsizdir ve her geçen gün genişlemektedir. Enerji santrallerinden barajlara, sanayi tesislerinden iletişim ağlarına kadar dijital altyapıya bağımlılık arttıkça, bireyler fiziki geçişlerdeki güvenlik standartlarının çevrimiçi ortamda aynı düzeyde sağlanmadığını fark etmektedir. Güvenlik yazılımlarına ayrılan bütçeler sürekli artmasına rağmen, İsrail Teknoloji Enstitüsü'nden genç araştırmacıların 82 yeni bilgisayar virüsünü test ettiği bir çalışmada, bilinen anti-virüs programlarının ilk tehdit algılama oranı yalnızca %5 düzeyinde kalmıştır (Goodman, 2017, s. 28).

2014 verilerine göre günlük yaklaşık 684 bin Facebook paylaşımı, 34 milyon WhatsApp mesajı, 100 bin Twitter paylaşımı ve 36 bin Instagram fotoğrafı yüklenirken, Zuckerberg ve Eric Schmidt'in ifadeleriyle "çağı yönetenler" artık bireylerin bıraktığı dijital ayak izlerinin verisine sahip olanlardır. Zamanla bu platformlarda paylaşılan bilgiler, insan davranışlarını analiz ederek reklam, pazarlama, gözetim, şantaj veya siyasi baskı gibi amaçlarla kullanılabilir. Bu nedenle kişisel veriler, doğal kaynaklar gibi yüksek hassasiyetle korunmayı gerektiren stratejik bir değere dönüşmüştür (Goodman, 2017, s. 126).

3.1.Siyasi İstikrar ve Rejim Güvenliği Odaklı Vakalar

Siyasal istikrar, ekonomik, siyasi ve sosyal karar alma süreçlerinde toplumun beklentilerinin karşılanmasında sürekli başarı sağlanması olarak tanımlanabilir. Bu istikrarın sürdürülebilmesi, yalnızca hükümete değil; siyasi sistemin yapısına, seçim mekanizmalarına, seçmenlerin sosyo-kültürel ve ekonomik özelliklerine, ülkenin genel mali durumuna gibi pek çok unsura bağlıdır. İstikrar kavramı, uzun vadede aynı düzen içinde tutarlılık ve süreklilik gösterebilme kapasitesini ifade eder; sistemin hedeflerine ulaşma kararlılığını ve düzen içindeki tutarlılığını açıklar. Siyaset

biliminde kullanılan siyasal istikrar terimi, hem siyasi sistemin genel sürekliliğini hem de sürece katılan aktörlerin (seçmenler, partiler, baskı grupları vb.) tutum ve eylemlerindeki istikrarı kapsar. Ancak toplumda tüm kararların ayrıcalıklı bir sınıf ya da diktatör tarafından alındığı otoriter veya teokratik modellerde gerçek anlamda siyasal istikrardan söz etmek mümkün değildir; çünkü bu sistemlerde halk katılımı ve temsil mekanizması bulunmaz (Ertekin, 2006, s. 99). Özetle, demokrasi ilkelerine dayanmayan yönetim biçimlerinde istikrar kavramı işlevsel olamaz. Toplumsal ve siyasal kurumların, toplumun ekonomik, siyasi ve sosyal taleplerini karşılamakta yetersiz kalması ise siyasal istikrarsızlığın temel nedenlerinden biri olarak kabul edilir (Lemco, 1991, s. 26).

Rejim güvenliği yaklaşımı, iç güvenlik tehditlerinin devletin güvenlik stratejilerini şekillendirmedeki belirleyici rolünü vurgular. Bu yaklaşımda analiz birimi devlet değil, rejimin kendisidir. Rejim güvenliği, iktidardaki seçkinlerin kendi yönetimlerine yönelik şiddet içeren iç tehditlerden korunması olarak tanımlanabilir (Jackson, 2007). Özellikle demokratik olmayan yollarla iktidarı elinde tutan hükümetlerde meşruiyet eksikliği, siyasi kırılganlık, sosyal uyum yetersizliği, temel konularda uzlaşmazlık, kurumsal zayıflıklar ve yerel istikrarsızlıklar gibi faktörler rejimleri ciddi güvenlik riskleriyle karşı karşıya bırakır (Ayoob, 1995).

Rejim güvenliği kavramı, Batılı devletlerin geleneksel ulusal güvenlik anlayışıyla (dış saldırılardan korunma odaklı) tam bir karşıtlık oluşturur (Job, 1992). Bu yaklaşım, otoriter rejim liderlerinin iç ve dış tehditleri minimize etmek üzere kendi yönetimlerini önceliklendiren güvenlik stratejileri benimseyeceğini öngörür. Rejim güvenliği ilkeleri, farklı güvenlik politikası alanlarına uyarlanarak çeşitli teorilere temel oluşturmuştur. Örneğin Steven David'in (1991) Soğuk Savaş dönemi ittifak davranışlarını açıklamak için geliştirdiği “çok yönlü dengeleme” (omni-balancing) teorisi, bu yaklaşımlardan biridir. Geleneksel güç dengesi veya tehdit dengesi teorilerinin dış tehditleri merkeze almasına karşın, çok yönlü dengeleme, yoğun iç tehditlerle yüzleşen liderlerin bu tehditlere karşı en etkili desteği sağlayabilecek veya en istekli müttefikleri tercih edeceğini savunur (Koblentz, 2013).

3.1.1.Arap Baharı Bağlamında Sosyal Medyanın Etkisi: Dijital Aktivizm

2010 yılının sonlarında Tunus'ta seyyar satıcılık yapan Muhammed Buazizi'nin kendini ateşe vermesiyle başlayan olaylar, kısa sürede "Arap Baharı"

olarak adlandırılan geniş çaplı protestolara dönüşmüştür. Bu eylem, halkın yönetime ve ekonomi politikalarına karşı birikmiş tepkisini tetiklemiş; yaşam kalitesinin düşüklüğü, yoksulluk ve yönetim zaafları gibi iç dinamikler protestoların temel itici gücü olmuştur. Tunus'ta başlayan eylemler sonucunda Zeynel Abidin Bin Ali'nin uzun süreli iktidarı sona ermiş, yerine Nahda Partisi ağırlıklı bir yönetim gelmiştir. Protestolar hızla bölgeye yayılmış ve farklı ülkelerde kendi iç dinamikleriyle şekillenmiştir (Şahin, 2011, s. 86).

Geleneksel kitle iletişim araçlarındaki baskı ve sansür ortamı nedeniyle Arap Baharı, ağırlıklı olarak sosyal medya platformlarında hayat bulmuştur. Muhalif gruplar, basın-yayın organlarında yer bulamayan görüşlerini, görüntülerini ve düşüncelerini internet üzerinden dünyaya duyurabilmişlerdir. Özellikle anonimlik imkânı sunan sosyal ağlar, kullanıcıların iktidar baskısından uzak bir şekilde fikirlerini ifade etmesine olanak tanımıştır. Ancak bu özgürlük algısı yanıltıcıdır; sosyal paylaşım ağlarının altyapısı ve kontrolü büyük ölçüde bu platformları geliştiren ülkelerin ve şirketlerin elindedir. Yeni iletişim teknolojileri, onları üreten ve ticarileştiren aktörlerin denetiminde gelişmekte olup, tam bir bağımsızlık veya tarafsızlık ilkesinden söz etmek zordur (Kırık, 2012).

Sonuç olarak sosyal medya, sınırsız özgürlük alanı gibi görünse de gerçekte iktidar ve güç dengelerinden bağımsız değildir; sınırları önceden belirlenmiş, tüketiciye bu sınırlar içinde hareket alanı sunan kontrollü mecralardır. Bu platformlar, sermaye güdümlü reklamların ve siyasal propagandanın en önemli hedeflerinden biri haline gelmiştir. “İnternet ve yeni iletişim teknolojileri, ticari medyanın hedeflerini genişleten bir büyüme alanı yaratmıştır. Bu durum, sosyal medyanın özgürlük aracı olmanın ötesinde, manipülasyon ve kontrol mekanizması olarak da işlev gördüğünü göstermektedir.

3.1.2. 6 Ocak ABD Kongre Baskını: Sosyal Medyada Radikalleşmenin Fiziksel Şiddete Dönüşümü

ABD'nin 46. başkanını belirleyen seçimler 3 Kasım 2020'de gerçekleştirilmiş; sonuçlara göre Demokrat aday Joe Biden zafer kazanmış, Cumhuriyetçi aday Donald Trump ise yenilgiyi kabul etmemiştir. Seçim sonuçlarının onay sürecinde Trump, 6 Ocak 2021 tarihinde destekçilerini eyleme davet etmiştir. O gün Kongre binası önünde toplanan kalabalık, polis barikatlarını aşarak binaya girmiş

ve başkanlık oylamasının ertelenmesine neden olmuştur. Bu olay sırasında 5 kişi hayatını kaybetmiş, 14 kişi yaralanmıştır. Trump'ın "geri çekilin" çağrısından sonra eylemciler dağılmıştır (Koyuncu, 2022).

6 Ocak olaylarında Trump'ın paylaştığı tweetler, oldukça riskli ve tehlikeli bir söylem yapısını net biçimde ortaya koymaktadır. İlk tweetinde Trump, 20 Ocak'ta başkanlığı Biden'a devrederken Washington'a gitmeyeceğini belirterek kitlesiyle bu kararı paylaşmakta ve eylemini meşrulaştırmaktadır. İkinci tweette ise kendisine oy veren 75 milyon kişiyi "Amerikalı vatanseverler" olarak tanımlamakta; oy vermeyenleri zımnen vatansever olmayan –yani "öteki"– konumuna yerleştirmektedir. "Önce Amerika" ve "Amerika'yı Yeniden Büyük Yapalım" sloganlarıyla kitlesinin duygularına güçlü bir şekilde seslenen Trump, kendi grubuyla izole bir anlam dünyası oluştururken "öteki"ne yönelik öfke biriktirme potansiyeli taşımaktadır. Capitol baskını sırasında gelen üçüncü tweette Trump, "ABD Capitol'deki herkesin barışçıl kalmasını istiyorum. Şiddete hayır! Unutmayın, BİZ Kanun ve Düzen Partisiyiz" ifadesini kullanmıştır (Tunçay vd., 2023).

Burada "BİZ" kelimesini büyük harfle vurgulayarak hem kendisi hem partisi hem de kitlesi adına sisteme bağlılık ve kanun-düzen vurgusu yapmakta, eylemcileri sükunete davet etmektedir. Bu büyük harf kullanımı, kitlesiyle arasındaki aidiyet duygusunu pekiştirirken aynı zamanda onları durdurma çabası olarak okunabilmektedir. Son tweetinde ise "Lütfen Capitol Polisimizi ve Emniyet Teşkilatımızı destekleyin. Onlar gerçekten ülkemizin yanındalar. Barışçıl kalın!" diyerek doğrudan kitlesine seslenmekte ve baskını sonlandırmaya çalışmaktadır. Özellikle "destekleyin" ve "gerçekten ülkemizin yanındalar" ifadeleri dikkat çekicidir; çünkü emniyet mensupları "öteki olmayan" ve "bizimle" kategorisine yerleştirilmekte, böylece öfkeli kitle "bizimle" addedilen bir grupta uzlaşma zemini bulabilmektedir. Bu söylem, kitlenin "bizimle" olan üzerinden kanun sınırlarına çekilmesini sağlamakta ve liderin kitleler üzerindeki durdurma gücünü göstermektedir. Barışçıl kalma çağrısı "öteki olmayan" için geçerliyken, "öteki"ne karşı fiili baskın ve şiddet zaten devam edebilmektedir. Bu tür söylemler, fanatizm dinamiklerinde liderin kitleyi durdurma sürecindeki mantık ve retorik örneklerinden biri olarak değerlendirilebilir (Tunçay vd., 2023)

3.2. Kamu Düzeni ve Toplumsal Barış Odaklı Vakalar

Kolluk güçleri, kamu düzeninin kurulması, korunması ve bozulması halinde yeniden sağlanması amacıyla faaliyet gösterir. Kolluğun temel görevi, kamu düzenini hem önleyici hem de onarıcı yönde sürdürmektir. Kanunla verilen yetkiler kolluk faaliyetinin çerçevesini belirler; ancak bu yetkiler yetersiz kaldığında veya detaylandırma gerektiğinde idare (kolluk), kanun sınırları içinde kendi düzenlemelerini yaparak kamu düzenini tesis eder ve sonrasında bunu koruma altına alır. Düzen bozulduğunda ise kolluk yeniden müdahale ederek düzeni geri getirir (Günday, 2011).

Kamu düzeni, bozulduğunda kamu yararını zedeleyen, korunduğunda ise kamu yararının gerçekleşmesini sağlayan bir yapıdır. Kamu düzenini tehdit eden davranışlar kamu yararına aykırı iken, bu düzeni koruyan faaliyetler doğrudan kamu yararına hizmet eder. Ancak kolluğun faaliyetlerinin kamu yararına olması tek başına yeterli değildir; eylemlerin amacı mutlaka kamu düzenini sağlamak ve korumak olmalıdır. Eğer kolluk, örneğin yalnızca gelir elde etmeyi hedeflerse, bu faaliyet hukuka aykırı hale gelir (Akyılmaz vd., 2018).

Kişinin uzlaşmacı ve barışsever tutumu, hem bireysel hem de toplumsal düzeyde gerginlikleri azaltır ve ciddi bir rahatlama sağlar. Birey, aile, iş ve sosyal ilişkilerinde barış içinde olduğunda çatışma yerine çözüm odaklı davranabilir. Uzlaşma, insanın hedeflerine ulaşmasında temel bir araçtır; çatışmak ya da kaçınmak yerine farklılıkları yöneterek benzerliklere odaklanmayı mümkün kılar. Bu tutum, bireyin varoluş düzeyini yükseltir ve daha sağlıklı ilişkiler kurmasına zemin hazırlar (Tarhan, 2018; Dökmen, 2010). Toplumsal düzeyde de uzlaşmacı yaklaşım, tarafların ortak değerlere yoğunlaşmasını sağlar.

Hoşgörü odaklı toplumlar genellikle çoğulculuk ve katılımcılık ilkelerini benimser; bu değerler demokrasinin temel taşlarıdır ve birbirlerinin varlığını güvence altına alır. Demokratik sistemlerde eleştiri hoşgörüyle karşılanır, çokseslilikten yararlanılır. Farklı görüşlerle yüzleşmeye cesaret eden toplumlarda düşünceler dış etkilerle harmanlanarak yenilikçi fikirler doğar; bu da hızlı bir gelişim ve ilerleme sağlar (Arıcan ve Türer, 2015).

3.2.1. Myanmar Vaka Analizi: Etnik Çatışmalar

Myanmar, Asya'nın güneydoğusunda 676.578 km²'lik yüzölçümüyle yer alan bir ülkedir. Hindistan, Bangladeş, Laos ve Tayland ile kara sınırı paylaşırken, Bengal Körfezi ve Andaman Denizi'ne kıyısı sayesinde enerji transferi ve uluslararası ticaret açısından stratejik bir konumdadır (Tüysüzoglu, 2012, s. 2). Daha önce Burma (veya Birmanya) olarak bilinen ülkenin adı, 1989 yılında Myanmar Birliği Cumhuriyeti olarak değiştirilmiştir. Her iki isim de esasen Bamar etnik grubunu ifade eder (Bayram ve Yaylar, 2016).

Yaklaşık 51 milyon nüfusa sahip ülkede 135 farklı etnik grup bulunmakta olup, nüfusun %68'ini Bamarlar oluşturur. Diğer önemli gruplar arasında Şanlar, Karenler, Rakhineler, Rohingyalar, Çinliler, Monlar, Kaçiler, Kayinler, Kayalar ve Hintliler yer alır. Resmi verilere göre nüfusun %89'u Budist, %4'ü Hristiyan, %4'ü Müslüman ve %1'i Hindu'dur. Müslüman nüfusun büyük kısmı, Bangladeş sınırına yakın Arakan dağlık bölgesinde yoğunlaşmıştır (Bayram ve Yaylar, 2016).

1989'daki isim değişikliği, ülkenin çok etnikli yapısını daha kapsayıcı bir biçimde yansıtmaya amacıyla yapılmıştır. "Burma" terimi, çoğunluğu oluşturan Bamar grubunun hâkimiyetini çağrıştırırken, "Myanmar" daha geniş bir kapsayıcılık hedeflemiştir. Ancak özellikle Rohingyalar gibi bazı etnik gruplar bu değişikliği kabul etmemiş ve geleneksel "Burma" adını kullanmayı sürdürmüştür. Myanmar, tarihsel olarak derin etnik çeşitliliğe sahip bir ülkedir; başlıca gruplar arasında Bamar, Rohingya, Kachin, Shan, Karen, Chin ve Mon öne çıkar. 1962 askeri darbesi sonrasında etnik gruplara yönelik baskılar artmış; Rohingyalar özellikle vatandaşlık hakkı başta olmak üzere temel haklardan uzun süre mahrum bırakılmıştır. Bu durum, isim değişikliğine rağmen etnik eşitsizliklerin ve çatışmaların devam ettiğini göstermektedir (Jabbari, 2025).

Myanmar'da Müslümanlara yönelik saldırıların tetikleyicilerinden biri, Budist rahip Ashin Wirathu'nun provokatif söylemleridir. 2003'te dinî nefret kışkırtıcılığından hapis cezası alan Wirathu, kendisini "Budist bin Ladin" olarak tanımlamaktadır. Bu tür rahipler, halk nezdinde yüksek meşruiyet gördükleri için yöneticiler tarafından sıklıkla desteklenmekte ve korunmaktadır. Myanmar liderleri, tarih boyunca Budizm'i milli kimliğin temel unsurlarından biri olarak konumlandırmış ve bu din adına şiddeti meşrulaştırmıştır. Müslüman karşıtı söylemler, halkın belirli

kesimlerinde karşılık bulmaya başlamış; çoğunlukta olmalarına rağmen Budistler kendi dinlerinin ve milli birliklerinin tehdit altında olduğuna inanmaktadır. Küresel ölçekte İslam ile şiddet arasında kurulan bağların etkisiyle Budistler de benzer bir "savunma" refleksi geliştirmişlerdir. Bu süreç, pasifist öğretilere dayandığı düşünülen Budizm'in şiddet eylemlerine gerekçe sunan bir ideolojiye dönüştürülmesi anlamına gelmektedir (Bayram ve Yaylar, 2016).

Myanmar'da yaşanan etnik çatışmalar, sosyal medyanın şiddet ve nefret söyleminin yayılmasındaki rolünü çarpıcı biçimde ortaya koymuştur. Özellikle Facebook platformu, ülkedeki en yaygın haber kaynağı olarak kullanılmış ve bu durum, platformun şiddet içeren içeriklerin kontrolünde yetersiz kaldığını göstermiştir. Bağımsız bir kurum tarafından hazırlanan raporda, Facebook'un Myanmar'da insan hakları ihlallerinin yaygınlaşmasına zemin hazırlayan bir ortam oluşturduğu açıkça belirtilmiştir. Facebook da bu rapora katıldığını ifade ederek, platformun nefret söylemini önleme konusunda yeterli önlemleri alamadığını kabul etmiştir (BBC, 2018).

Birleşmiş Milletler'in "soykırım boyutuna ulaşabilecek" nitelikte tanımladığı Arakan Müslümanlarına (Rohingya) yönelik şiddet olaylarında, sosyal medya üzerinden yayılan dezenformasyon ve kışkırtıcı paylaşımların önemli rol oynadığı tespit edilmiştir. Raporda, özellikle 2020 seçimleri öncesinde Facebook'un bu sorunu çözmesi gerektiği vurgulanmış, aksi takdirde platformun etnik gerilimi daha da derinleştirebileceği uyarısı yapılmıştır. Myanmar'da yaklaşık 18 milyon kullanıcısı bulunan Facebook, birçok kişi için haber alma ve bilgi paylaşımının neredeyse tek kanalı haline gelmiştir. Bu durum, platformun hem olumlu hem de olumsuz etkilerini aynı anda artırmıştır (BBC, 2018).

Sonuç olarak, Myanmar deneyimi sosyal medyanın kamu düzenini ve toplumsal barışı tehdit eden bir araç haline gelebileceğini gösteren kritik örneklerden biridir. Facebook'un nefret söylemini yayılmasını engellemede yavaş ve yetersiz kalması, BM tarafından da eleştirilmiştir. Bu vaka, sosyal medya platformlarının özellikle etnik çeşitliliğin yüksek olduğu toplumlarda sorumluluklarının ne kadar büyük olduğunu ve etkili içerik denetim mekanizmalarının önemini bir kez daha ortaya koymaktadır (BBC, 2018).

3.2.2. Covid-19 Pandemisi ve İnfodemi: Kamu Sağlığı Güvenliğine Yönelik Dijital Tehditler

2019 yılında Çin'in Wuhan kentinde ortaya çıkan koronavirüs salgını (COVID-19), kısa sürede küresel ölçeğe yayılarak yaklaşık iki yıl boyunca toplumsal yaşamın neredeyse tüm alanlarını derinden etkilemiştir. Salgın, ağır sağlık sonuçlarının yanı sıra ciddi toplumsal ve ekonomik dönüşümlere de yol açan geniş kapsamlı bir kriz niteliği taşımaktadır. Salgın döneminde üretimdeki aksamalar, alım gücünün azalması, daralan ekonomiler, tedarik zincirlerinde yaşanan kopmalar, yavaşlayan büyüme oranları ve toplumsal kalkınmada gözlenen gerilemeler gibi makro düzeydeki sorunların yanı sıra, bireysel düzeyde kaygı, stres, tahammül kaybı ve psikolojik travmalar da yaygın biçimde ortaya çıkmıştır. Bu süreçte ekonomik ve psiko-sosyal değişimler, toplumun tüketim alışkanlıklarından eğitim ve çalışma modellerine, hayata bakış açısına kadar birçok temel dinamiğini kökten etkilemiş ve yeni biçimler kazanmasına neden olmuştur (Bulut ve Aslan, 2021).

Dünya Sağlık Örgütü (DSÖ) Genel Direktörü Dr. Tedros'un Şubat 2020'de yaptığı “Biz yalnızca bir pandemiyle değil, aynı zamanda bir infodemiyle de mücadele ediyoruz” açıklaması, COVID-19 salgını sırasında “infodemi” kavramını küresel ölçekte yeniden gündeme taşımıştır. Bu terim, “information” (bilgi) ve “pandemic” (salgın) sözcüklerinin birleşiminden türetilmiş olup, salgınla ilgili gerçek dışı, hatalı veya yanıltıcı bilgilerin aşırı yük oluşturarak yayılması anlamına gelir. DSÖ, bu fenomeni “aşırı bilgi yükünün kaçınılmaz olarak beraberinde yanlış veya güvenilir olmayan bilgileri getirmesi” ve “yanlış bilgi epidemisi” olarak tanımlamakta; söz konusu durumun toplumlarda panik ve korku yaratabildiğini, hastalıkla mücadeleyi zorlaştırdığını ve damgalamayı artırabildiğini vurgulamaktadır (Dünya Sağlık Örgütü, 2020).

Tarih boyunca aşılar, antihipertansif ilaçlar gibi sağlık konularında bilimsel çevrelerin de zaman zaman dahil olduğu yanlış bilgi yayılım senaryoları yaşanmıştır. Ancak bulaşıcı hastalık salgınları gibi öngörülemez ve hızlı gelişen durumlarda yanlış bilginin ve buna bağlı davranışların yayılımı, belirsizliği bir an önce giderme ihtiyacı nedeniyle çok daha süratli ve yıkıcı olabilmektedir (Gölbaşı ve Metinbaş, 2020).

Son dönemde sosyal medya ağlarının yaygınlaşmasıyla birlikte her salgın kendi infodemisini beraberinde getirmiş; Covid-19 pandemisinde bu olgu en önemli

engelleyici faktörlerden biri haline gelmiştir. DSÖ ile aynı iletişim kanallarını kullanan politika aktörleri, doğru sağlık bilgisini ulaştırmak için ayrı bir mücadele alanı oluşturmuştur. DSÖ öncülüğünde infodemi yönetimi, “risk iletişimi ve toplum katılımı” çerçevesinde çeşitli uygulamalarla desteklenmiştir. Pandemi süreci, topluluklara doğru bilgi aktarımı için esnek ve dayanıklı sistemlerin kurulması gereğini net biçimde ortaya koymuştur. Çevrim içi ve çevrim dışı söylentilerin ile yanlış bilgilerin tespit edilip görünür kılınması, ardından toplulukların değer yapılarını da dikkate alarak aşamalı müdahale edilmesi kritik önem taşımaktadır (Gölbaşı ve Metinbaş, 2020).

3.2.3. İngiltere (2011) Londra İsyanları ve Yağma

2011 yazında Londra'da siyahi bir vatandaş olan 29 yaşındaki Mark Duggan'ın polis tarafından öldürülmesi, kısa sürede ülke çapında büyük çaplı isyanlara yol açmıştır. Bu olay sosyoekonomik nedenlerle hızla yayılmış; farklı kesimlerden insanlar sosyal ağlar üzerinden haberdar olup örgütlenerek sokaklara dökülmüştür (Türk, 2013).

Ayaklanmalar Londra'da başlayıp ülke geneline sıçramış, özellikle kundaklama ve yaygın yağmalama eylemleriyle dikkat çekici bir boyut kazanmıştır. Başbakan David Cameron, kamu düzenini yeniden tesis etmek üzere gerekli tüm yasal ve operasyonel adımların atılacağını açıklamış; tatilini yarıda keserek acilen Londra'ya dönmüş ve güvenlik kabinesi toplantısı toplamıştır. BBC'nin aktardığına göre olayların başlangıcından itibaren ilk ölüm vakası kayıtlara geçmiş; Croydon bölgesinde arabasında vurularak öldürülen 26 yaşındaki bir erkek kurban olarak belirlenmiştir. Londra Emniyeti, tutuklanan kişi sayısının 525'e ulaştığını duyurmuştur (T24, 2011).

Güvenlik güçlerine yönelik takviye kararları kapsamında, önceki gece 6.000 polis memurunun görev yaptığı belirtilirken, o gece bu sayı 16.000'e çıkarılmış ve 10.000 ek personel bölgeye sevk edilmiştir. Başbakan, parlamentonun Perşembe günü olağanüstü toplanacağını ilan etmiştir. İsyanların tetikleyicisi, dört çocuk babası Duggan'ın polis tarafından öldürülmesini protesto eden barışçıl gösterilerin kontrolden çıkması olarak değerlendirilmektedir. Ülke genelinde 525'ten fazla kişinin gözaltına alındığı resmi verilerle doğrulanmıştır. Olaylar Londra ile sınırlı kalmamış; Birmingham, Liverpool, Nottingham ve Bristol gibi kentlerde de ciddi boyutlara ulaşmıştır. Bu şehirlerde çok sayıda araç ve iş yeri ateşe verilmiş, mağazalar sistematik

yağmalanmıştır. Özellikle Türkiye kökenli göçmenlerin yoğun yaşadığı semtlerde Türk ve Kürt vatandaşların kendi dükkânlarını yağmalamaya çalışan kalabalıkları başarıyla püskürttüğü gözlemlenmiştir. Ana arterler trafiğe kapatılmış, saldırı korkusuyla birçok iş yeri kapanmak zorunda kalmıştır. Birmingham kent merkezinde vitrinlere yönelik saldırılar, Manchester'da polis karakolunun kundaklanması, otomobillerin yakılması, Liverpool'da maskeli grupların dükkânları hedef alması ve Bristol'da yaklaşık 150 kişilik kalabalığın çıkardığı olaylar medyada geniş yer bulmuştur. Bu gelişmeler üzerine İngiltere-Hollanda milli takımlarının Çarşamba günü oynanması planlanan futbol maçı da iptal edilmiştir (T24, 2011).

İngiltere medyasında olaylara ilişkin yorumlar ağırlıklı olarak polis ve siyasilerin yetersizliğine odaklanmış; sokakların çetelere terk edildiği ve "orman kanunu"nın egemen olduğu eleştirileri öne çıkmıştır. Önde gelen gazeteler, kundaklama ve yağmalama eylemlerini bu çerçevede değerlendirmiştir (T24, 2011).

Bir grup akademisyen tarafından gerçekleştirilen kapsamlı analiz, 2,6 milyondan fazla tweet incelenerek Twitter'ın gerçek rolünü ortaya koymuştur. Araştırmacılar, #EnglandRiots ve #BirminghamRiots gibi hashtag'ler üzerinden toplanan verileri değerlendirerek, Twitter'ın isyanı teşvik etmekten ziyade, özellikle "temizlik kampanyası" (#riotcleanup) gibi sivil girişimleri güçlendirdiğini tespit etmiştir. Prof. Rob Procter'in de yer aldığı çalışma, isyan sırasında atılan tweetlerin büyük çoğunluğunun şiddet çağrısı içermediğini, aksine kamu düzeninin yeniden sağlanması ve toplumun kendi kendini toparlaması yönünde mesajlar taşıdığını göstermiştir (Tamir, 2018).

Öte yandan, isyancıların asıl iletişim aracı olarak kapalı ve daha gizli bir uygulama olan BlackBerry Messenger'ı (BBM) tercih ettikleri belirlenmiştir. Twitter'da isyanı açıkça teşvik eden tweet sayısı oldukça sınırlı kalmış ve bunlar da genellikle istenen etkiyi yaratamamıştır. Sonuç olarak, en yoğun etkileşim temizlik ve dayanışma çağrıları etrafında oluşmuş, #riotcleanup etiketi binlerce kişi tarafından paylaşılmış ve milyonlarca kullanıcıya ulaşmıştır. Bu durum, sosyal medyanın toplumsal olaylarda hem kaos yaratma hem de toplumsal iyileşmeyi destekleme potansiyelini aynı anda taşıdığını gösteren önemli bir örnek olarak literatürde yerini almıştır (Tamir, 2018).

3.3. Siber Güvenlik, İstihbarat ve Hibrit Savaş Odaklı vakalar

Siber güvenlik, internet ortamındaki varlığımızın güvenliği ve gizliliğinin korunması olarak ifade edilebilir. Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı'nda bu kavram, “siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunması, bu ortamda işlenen bilgi ve verilerin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, bu tespitlere karşı tepki mekanizmalarının devreye sokulması ve sistemlerin olay öncesi duruma geri döndürülmesi” şeklinde tanımlanmıştır. Kısaca siber güvenlik, dijital sistemleri ve verileri saldırılara karşı korumak için kullanılan teknoloji, süreç ve yöntemlerin tümünü kapsar (BTK, 2016).

Siber güvenlik, dijital sistemleri ve verileri tehditlerden korumaya yönelik çeşitli süreçler, stratejiler ve teknolojik çözümlerin bütünüdür. Verilerin hızla çoğaldığı, bireylerin her yerden bağlandığı ve uzaktan çalıştığı günümüzde kötü niyetli aktörler, kaynaklara erişmek, veri çalmak, sabotaj yapmak veya fidye talep etmek amacıyla daha karmaşık yöntemler geliştirmektedir. Saldırıların sayısı her yıl artmakta, saldırganlar algılanmadan kaçmak için yeni teknikler üretmektedir. Etkili bir siber güvenlik yaklaşımı, insanlar, süreçler ve teknolojinin bir arada çalışarak iş kesintisi, finansal kayıp ve itibar zararı gibi risklerle başa çıkabilmesini gerektirir (Cyberarts, 2024).

Milli güvenliğin bir parçası olarak ele alınan siber güvenlik, erişilebilirlik, gizlilik ve bütünlük ilkeleri üzerine kuruludur. Erişilebilirlik, yetkili kişilerin istedikleri anda bilgiye ulaşabilmesini; gizlilik, bilginin yalnızca yetkili kişilerce erişilebilir olmasını; bütünlük ise bilginin herhangi bir değişiklik veya bozulma olmadan korunmasını ifade eder. Bu üç unsur arasında doğal bir denge vardır: Erişilebilirlik düzeyinin artması gizlilik ve bütünlükte kısmi düşüşe yol açabilirken, gizlilik ve bütünlük önceliği erişilebilirliği sınırlayabilir (Halisdemir, 2021). Bu dengeyi korumak amacıyla geliştirilen standartlardan biri ISO 27001 Bilgi Güvenliği Yönetim Sistemi'dir; bu standart, kurumların kurulum, sistem yönetimi ve sürekli iyileştirme süreçlerini kapsar. ISO 27002 ise bu sistemde uygulanacak önlemleri ve tehditlere karşı alınacak tedbirleri detaylandıran bir rehber niteliğindedir (Çiftçi, 2024).

Avrupa Birliği'nde siber güvenlik politikalarının kurumsal yapısı, 2004 yılında kurulan AB Siber Güvenlik Ajansı (ENISA) ile şekillenmiştir. ENISA, iki veya daha fazla üye ülkeyi eşzamanlı etkileyen sınır ötesi siber olaylara müdahale kapasitesini artırmak üzere tasarlanmış özerk bir Birlik organıdır. Avrupa Parlamentosu ve Bakanlar Konseyi kararıyla kurulan ENISA, üye ülkelerle yakın iş birliği içinde siber suçların ve hibrit tehditlerin aracı olarak kullanılmasına karşı mücadele kapasitesini güçlendirmekte, tavsiye ve çözüm önerileri üretmekte ve uygulamaların takibini yapmaktadır (ENISA, 2023). Kuruluş döneminde hibrit tehdit kavramı henüz literatürde yer almasa da, 2007 sonrası dönemde ENISA kademeli olarak bu alandaki politikaların yürütülmesinde aktif rol üstlenmiştir.

Hibrit tehdit kavramının 2007'de literatüre girmesinin ardından AB, 2009 yılında Kritik Bilgi Yapılarının Korunması Üzerine Bildirim (CIIP) ile siber güvenlik politikalarını güncellemiştir. CIIP, AB'yi geniş çaplı siber saldırılardan ve yıkımlardan korumayı hedefleyen bir politika çerçevesidir; güvenliği, hazır bulunurluğu ve hibrit tehditlere karşı toplum direncini artırmayı amaçlar. Bildirim, kritik bilgi ve iletişim teknolojisi yapılarının korunmasına odaklanmakta; bu yapılara yönelik suç ve terör faaliyetlerini önleme, mücadele etme ve yargıya taşıma mekanizmalarını görmektedir (Commission of the European Communities, 2009).

3.3.1. Stuxnet ve Sonrası: Nükleer Tesislere Yönelik Keşif Aşamasında Sosyal Medyanın Rolü

21.yüzyılın en yıkıcı siber saldırılarından biri olarak kabul edilen Stuxnet, İran'ın nükleer tesislerini hedef alarak insanlık tarihinde sabotaj amaçlı geliştirilen ilk "süper bilgisayar virüsü" özelliğini taşımaktadır. Bu solucan tipi kötü amaçlı yazılım (worm), 2010 yılında tespit edilmiş ve kendi kendini kopyalama yeteneği sayesinde içine yerleştiği ağlarda hızla yayılarak sistemi kullanılamaz hale getirebilen bir "yazılım bombası" işlevi görmüştür. Stuxnet, uzaktan erişimle büyük ölçekli bir sisteme yönelik gerçekleştirilen ilk kapsamlı saldırı olması bakımından da dönüm noktası niteliğindedir. Bu saldırı, siber terörün kurallarını ve dinamiklerini kökten değiştirmiş, devlet destekli siber operasyonların yeni bir çağını başlatmıştır (Holat, 2021).

Stuxnet saldırısının ABD tarafından 2009 yılında İran'ın Natanz uranyum zenginleştirme tesislerine karşı düzenlendiği öne sürülmektedir. Saldırıları iki ayrı

tarihte gerçekleşmiş; ilki 22 Haziran 2009 yerel saatle 16:30'da ikincisi ise 7 Temmuz 2009 yerel saatle 17:00'de meydana gelmiştir. Virüs, özellikle SCADA (Supervisory Control and Data Acquisition) sistemlerini hedef almak üzere tasarlanmış en karmaşık yazılımlardan biri olarak öne çıkar. Nükleer tesislerde SCADA sistemleri tüm saha operasyonlarını izleyen ve kontrol eden merkezi yapıyı oluşturduğundan, bu saldırıların önemi daha da artmaktadır (Kara ve Çelikkol, 2011, s. 145).

Virüs, büyük olasılıkla bir USB bellek aracılığıyla tesisin yerel ağına sızmış ve buradan Programlanabilir Mantık Denetleyicisi (PLC) kontrol devrelerini ele geçirmiştir. Bu sayede komuta-kontrol merkezine bağlanarak saldırıyı düzenleyene hareket serbestliği sağlamış ve sisteme ek kötücül kod yüklemelerine imkân tanımıştır (Bıçakçı, 2016, s. 116). Kontrol yazılımı bozulmaya başlayınca santrifüjlerin dönme hızı kontrolden çıkmış, makineler parçalanmaya başlamıştır. Stuxnet'in en sofistike yanı, merkez bilgisayarlara her şeyin normal görüldüğü izlenimini vermesiydi; bu nedenle verilen zarar uzun süre fark edilmemiştir (Kara ve Çelikkol, 2011, s. 34).

Virüs, her 100 milisaniyede bir komut göndererek santrifüjlerin frekansını olağanüstü hızla değiştirmiş; bu da uranyum zenginleştirme sürecini sekteye uğratmayı amaçlamıştır. Saldırının amacı tesisleri tamamen yok etmekten ziyade çalışmaları yavaşlatmak ve geciktirmek olarak değerlendirilmektedir (Çelik, 2013, s. 148). Sonuçta Natanz tesisindeki yaklaşık 1000 santrifüj tahrip edilmiş, tesisin kapasitesinin beşte biri işlevsiz hale gelmiştir. Bu hasar, tamiri aylar sürecektir boyutta olmuş ve İran'ın nükleer programını yaklaşık iki yıl geriye atmıştır. Virüsün küresel yayılımında İran %58.85 oranla ilk sırada yer alırken, Endonezya (%18.22), Hindistan (%8.31), Azerbaycan (%2.57), ABD (%1.56) ve Pakistan (%1.28) gibi ülkeler de etkilenmiştir (Wikipedia, 2020). Bu yayılım, saldırının yalnızca İran'ı değil, çok sayıda ülkeyi de hedef aldığını veya dolaylı etkilediğini ortaya koymuştur. Stuxnet vakası, siber ortamda küresel iş birliğinin ve ortak savunma mekanizmalarının zorunluluğunu bir kez daha vurgulamıştır.

Devletlerin siber alandaki hâkimiyeti, bilişim sistemlerindeki teknolojik üstünlüklerine, yeni medya araçlarını yönetebilme kapasitelerine ve genel dijital gelişmişliklerine bağlıdır. Bu hâkimiyet, ulusal güvenliğin korunmasında kritik rol oynar. Dolayısıyla siber güvenlik stratejileri için etkili mücadele yöntemleri geliştirilmesi ve bu alana azami önemin verilmesi bir zorunluluk haline gelmiştir (Holat, 2021).

3.3.2. Ukrayna- Rusya Savaşı: Sosyal Medya Cephesi (Dijital Savaş)

21 Şubat 2022'de Rusya Devlet Başkanı Vladimir Putin, Donetsk ve Luhansk'taki ayrılıkçı yönetimleri bağımsız devletler olarak tanıdığını duyurmuş; bu adım, Ukrayna ve Batı tarafından reddedilse de büyük çaplı bir askeri harekâtın habercisi olmuştur. 24 Şubat 2022'de Putin'in emriyle yaklaşık 200.000 askerden oluşan Rus kuvvetleri Kiev'i hedef alarak Ukrayna'ya kapsamlı bir saldırı başlatmıştır (Fix ve Keil, 2022, s. 4).

Rusya, bu harekâtı tam ölçekli savaş yerine “özel askeri operasyon” olarak nitelendirmiş ve uluslararası tepkileri yumuşatmak amacıyla belirli gerekçeler öne sürmüştür. Bu söylemde Ukrayna ve Rusya halklarının “kardeş” olduğu vurgusu öne çıkmış; Putin'in 2021 tarihli makalesinde de bu kardeşlik teması belirgindir (Park, 2022, s. 143). Putin, operasyonun dostane niyetlerle çerçevelendiğini savunurken, bu tür açıklamalar Avrupa'da İkinci Dünya Savaşı'ndan bu yana en büyük saldırının “özel operasyon” olarak sunulması nedeniyle yoğun eleştirilere yol açmıştır (Koşar, 2024, s. 71).

Rusya, harekâtın hedefleri arasında Ukrayna'yı askeri unsurlardan ve “Nazi ideolojisinden” arındırmayı göstermiş; ülkeyi işgal etme niyeti olmadığını ifade etmiştir (Libman, 2022, s. 150). Bu söylemde Ukrayna'nın “milliyetçi ve radikal gruplardan” temizlenmesi ve halkın “zorbalık ile soykırımdan” korunması vurgulanmıştır. 2014'te Yanukoviç'in devrilmesi, Kırım'ın ilhakı ve Donbas çatışmaları da Rusya'nın müdahale gerekçeleri arasında yer almıştır (Safranchuk, 2022, s. 5). Bu gelişmeler, Rusya'nın bölgedeki nüfuzunu artırma ve Ukrayna'daki mevcut durumu değiştirme çabaları olarak değerlendirilebilir.

21.yüzyılın dijital dönüşümü, savaşların ve krizlerin artık yalnızca sahada değil, çevrim içi platformlarda da yoğun biçimde yürütüldüğünü göstermektedir. Dijital savaş, askerî harekâtın ötesinde kamuoyunu yönlendirme, dezenformasyon yayma ve psikolojik üstünlük sağlama gibi unsurları içerir. Sosyal medya bu savaşın en kritik alanı haline gelmiştir; devletler, hükümet dışı aktörler ve bireyler Twitter, Facebook, Instagram ve TikTok gibi mecralar üzerinden kitleleri etkileme mücadelesi vermektedir. Kamuoyu yönetimi, askeri başarı kadar stratejik öneme sahiptir. Ukrayna-Rusya Savaşı, dijital savaşın kamuoyu yönetimindeki rolünü gösteren çarpıcı bir örnektir. Ukrayna yönetimi, savaşın ilk günlerinden itibaren sosyal medyayı etkin

kullanarak Batılı kamuoyunu yanına çekmiş; dramatik görseller, duygusal videolar ve lider açıklamalarıyla küresel sempati toplamayı başarmıştır (Sütçü, 2022).

Kamuoyu yönetimi yalnızca dış hedeflere değil, iç kamuoyuna da yöneliktir. Taraflar kendi halklarının moralini yüksek tutmak ve birlik duygusunu güçlendirmek için sosyal medyada pozitif söylemler üretmekte, kahramanlık hikâyeleri paylaşmakta ve ulusal kimliği ön plana çıkarmaktadır. Ukrayna, asker direniş görüntüleri, sivil dayanışması ve ulusal sembollerle halkını motive ederken; Rusya kendi kamuoyuna Batı'nın tehdit oluşturduğu ve operasyonun “savunma amaçlı” olduğu mesajını iletmektedir (Hoskins ve O’Loughlin, 2010).

Rusya-Ukrayna Savaşı'nda Ukrayna'nın propaganda faaliyetlerinde modern iletişim teknolojilerini yenilikçi biçimde kullanması dikkat çekicidir. 2022 Şubat'ında başlayan işgal sürecinden itibaren Ukrayna, klasik diplomatik kanalların ötesine geçerek sosyal medya üzerinden küresel kamuoyuyla doğrudan iletişim kurmuştur. Bu yaklaşım, Ukrayna'yı yalnızca askeri değil, enformasyon savaşı alanında da güçlü bir aktör haline getirmiştir. Twitter, Facebook, TikTok ve Instagram gibi platformlarda yürütülen dijital kampanyalar, Batı toplumlarında kamuoyu algısını şekillendirerek hükümetlerin silah ve mali yardım kararlarını hızlandırmıştır (Alieva, 2025).

Alternatif iletişim araçları etkileşimi zenginleştirse de, her aracın olumsuz yönleri de vardır. Kullanıcılar bu yönleri fark etmeli ve dikkatli davranmalıdır. Devletler, görevliler ve çıkar grupları sosyal medyayı propaganda aracı olarak kullanmaktadır. Botlar, sahte hesaplar ve troller, doğrudan takip edilebilen hesapların dışında yanlış, kışkırtıcı veya manipülatif içerikler yayabilmektedir. Sosyal platformların algoritmik yapıları yankı odaları (echo chambers) ve filtre balonları (filter bubble) oluşturarak kullanıcıları benzer görüşlere hapsedmekte, farklı fikirlerin temsilini kısıtlamakta veya ortadan kaldırmaktadır. Özellikle savaş ve kitle hareketleri gibi olağanüstü dönemlerde kullanıcılar karşılaştıkları içeriklerin güvenilirliğini sorgulamalı, kesin yargıya varmadan önce doğruluğunu teyit etmelidir (Durmuş, 2023).

3.4. Türkiye Özelinde Sosyal Medya ve Güvenlik Vakaları

Bu bölümde öncelikle 2013 Gezi Parkı Olaylarının sosyal medyanın mobilize edici ve koordinasyon gücü üzerinden nasıl bir dönüm noktası oluşturduğu, ardından 2024 yılındaki Kayseri göçmen karşıtı olaylarının dezenformasyon ve nefret söylemi

yayılımı bağlamında nasıl hızlı bir şekilde ülke geneline sıçradığı ve son olarak terör örgütlerinin (özellikle PKK ve DAESH gibi yapılar) güncel sosyal medya operasyonlarının psikolojik harp ve istihbarat boyutu ele alınacaktır. Bu vakalar, sosyal medyanın çift yönlü doğasını yani hem demokratik katılımı artıran hem de güvenlik risklerini çoğaltan bir araç olduğunu somut biçimde ortaya koymaktadır.

3.4.1. Gezi Parkı Olayları: Kitle Hareketlerinde Sosyal Medyanın Dönüştürücü Rolü

İstanbul Büyükşehir Belediyesi'nin Taksim yayalaştırma projesi kapsamında, Topçu Kışlası'nın bulunduğu alanın revize edilerek yeni bir kentsel dönüşüm çalışması yapılması planlanmıştır. Bu proje, İBB'nin 16 Eylül 2011 tarihli ve 2111 sayılı kararıyla, Beyoğlu İlçesi Taksim Meydanı Yayalaştırma Projesi'ne ilişkin 1/5000 ve 1/1000 ölçekli Koruma Amaçlı İmar Planı Tadilatı olarak kabul edilmişti. Ancak çeşitli sivil toplum kuruluşlarının ve vatandaşların itirazları nedeniyle proje durdurulmuş ve uygulamaya geçilememiştir (ibb.gov.tr, e.t. 14.06.2016). Bu itirazlar zamanla kitlesel bir tepki haline gelmiş ve Taksim Dayanışması Platformu'nun öncülüğünde bir toplumsal harekete dönüşmüştür.

Gezi Parkı Olayları, hükümetin 11 yıldır sürdürdüğü kalkınma odaklı neoliberal politikalara karşı bir tepki olarak değerlendirilmekte; iktidarı hedef alan ve rejim değişikliği talep eden eylemler şeklinde yorumlanmaktadır. Bazı analizlerde olaylar, dünya genelinde 2013'ten itibaren görülen küresel isyan dalgasının Türkiye uzantısı olarak görülmüştür. Gezi Parkı'nı diğer toplumsal hareketlerden ayıran başlıca özellikler, geniş toplumsal kesimlerden destek görmesi ve polis ile eylemciler arasında yaşanan yoğun çatışmalardır (Bilim Akademisi Derneği, 2013, s. 2).

Türkiye Barolar Birliği'nin raporuna göre olaylar öncelikle çevresel ve kentsel hakların korunması mücadelesi olarak başlamış, ancak zamanla barınma, yaşama ve konut hakkı gibi daha geniş boyutlar kazanmıştır. Dolayısıyla mesele yalnızca "3-5 ağaç" meselesi olmaktan çıkmış, demokrasinin adil işleyişi ve çevresel hakların savunulmasıyla ilgili kapsamlı bir mücadele haline gelmiştir (Türkiye Barolar Birliği, 2014, s. 51).

Ete ve Taştan'a göre Gezi Parkı Olayları üç aşamalı bir toplumsal hareket olarak gelişmiştir: Başlangıç aşaması sınırlı sayıda aktivistin çevre duyarlılığı söylemiyle bir araya gelmesi; siyasallaşma aşaması 1-15 Haziran arası yaşanan

gelişmelerle olayların siyasal alana taşınması; zayıflama aşaması ise hükümetin kararlı tutumuyla 15 Haziran'dan itibaren hareketin durağanlaşmasıdır (Ete ve Taştan, 2014, ss. 25-26).

Olayların başlangıcında geleneksel medyanın sessiz kalması, Türkiye'de 30 milyonu aşkın kullanıcıya sahip Facebook'ta fotoğrafların hızla yayılmasına ve İstanbul dışındaki bireylerin olaylardan sosyal medya üzerinden haberdar olmasına yol açmıştır. Bu durum sosyal medyanın kendi içinde bir kamusal alan işlevi görmesini sağlamış; fikirlerin özgürce tartışıldığı, örgütlenmenin ve eylemlerin koordine edildiği bir mecra haline gelmiştir (Yeniçikti, 2014).

Bireyler Facebook grupları ve Twitter'da #direngeziparkı, #occupygezi gibi hashtagler üzerinden iletişim kurarak örgütlenmişlerdir. Sosyal medya, olayların anlık paylaşımı, yardımlaşma, gelişmelerden haberdar olma gibi konularda ana akım medyanın önüne geçmiştir. Ancak hem eylemciler hem de iktidar yanlıları tarafından paylaşılan içeriklerde yanlı tutumlar sergilenmiş, bu da olayların amacından sapmasına neden olabilmıştır (Yeniçikti, 2014).

Başlangıçta 27 Mayıs 2013 gecesi protesto eden kişi sayısı 40-50 civarındayken, sosyal medya sayfaları ve gruplar sayesinde çok sayıda kişi olaylardan haberdar olup katılım sağlamıştır. Araştırmalara göre olayları sosyal medya üzerinden takip edenlerin oranı %69, protestocuların %84,6'sının anlık paylaşım yaptığı tespit edilmiştir. Bu yüksek etkileşim, hareketin etkisini artırmış ve ulusal/uluslararası düzeyde tartışılmasını sağlamıştır. 40-50 kişiyle başlayan süreç, sosyal medya üzerinden sürekli propaganda ve uluslararası düzeyde paylaşımlar sayesinde küresel bir görünürlük kazanmıştır. Özellikle Twitter'da #direngezi hashtag'inin trendtopic listelerinde üst sıralarda yer alması olayların tüm dünyaya servis edilmesine ve taraflı haberdarlığa yol açmıştır (Aslan, S, 2017).

3.4.2. Kayseri Göçmen Olayları (2024): Dezenformasyonun Toplumsal Şiddeti Tetiklemesi

Bu bölüm, yapay zekâ GROK tarafından Kayseri olayları (2024) bağlamında X platformunda (eski adıyla Twitter) dolaşıma giren paylaşımların nitel ve nicel unsurlarını analiz ederek hazırlanmıştır. Analiz, resmi açıklamalar, haber kaynakları ve doğrudan platformdan elde edilen örnek tweetler temel alınarak yapılmış olup,

sosyal medyanın devlet ve kamu güvenliği açısından taşıdığı riskleri somutlaştırmayı amaçlamaktadır.

30 Haziran 2024 akşamı Kayseri'nin Melikgazi ilçesinde bir Suriyeli şahsın 5-6 yaşlarındaki bir çocuğa yönelik cinsel istismar iddiası, kısa sürede X platformunda yoğun bir dezenformasyon ve provokasyon dalgasına dönüştü. İçişleri Bakanı Ali Yerlikaya'nın resmi açıklamasına göre olaylar sırasında yaklaşık 79 bin hesaptan 343 bin paylaşım gerçekleştirildi; bu paylaşımların %37'si bot hesaplar tarafından üretildi ve %68'i provokatif ile negatif nitelik taşıyordu. Bu veriler, sosyal medyanın gerçek bir adli olayı hızla genelleştirerek toplumsal gerilimi ülke geneline yayma kapasitesini açıkça ortaya koymaktadır. DW Türkçe'nin yaklaşık 12 bin tweet üzerinden yaptığı bağımsız analizde de benzer sonuçlara ulaşılmış, bot ve trol hesapların %20-24 oranında tweet trafiğini domine ettiği, görüntülenmelerin %39'unun bu hesaplar kaynaklı olduğu belirlenmiştir. Özellikle 1 Temmuz gecesi şiddet olaylarının zirve yaptığı dönemde, yeni açılmış bot hesapların (örneğin Temmuz 2024'te açılan 39 hesap) koordineli şekilde göçmen karşıtı mesajları yaydığı tespit edilmiştir.

Paylaşımların içeriği incelendiğinde dört ana tema belirgindir. Birincisi duygusal manipülasyon ve mağduriyet anlatısıdır; örneğin olay yerinden çekilen videolarla birlikte "Suriyeli tacizci 5 yaşındaki çocuğu istismar etti! Kayseri'de halk ayaklandı" gibi başlıklar kullanılarak istismar iddiası tüm Suriyeli topluluğuna mal edilmiş, bu da kitlesel öfkeyi tetiklemiştir. İkincisi doğrudan nefret söylemi ve şiddet çağrısıdır; bazı tweetlerde "Suriyelilere ait araçları devirip iş yerlerini ateşe veriyoruz" veya "iç savaş çıkacak, sığınmacılar yarın dönmeli" ifadeleriyle açık şiddet teşviki yapılmış, bu paylaşımlar hızla binlerce etkileşim almıştır. Üçüncüsü provokasyon ve dış güç tezi olup, Cumhurbaşkanı Erdoğan'ın "aynı kaos planlandı, figüranlık yapanları biliyoruz" açıklaması binlerce kez alıntılanarak "ABD/MOSSAD/FETÖ kışkırtması" iddiaları yaygınlaştırılmıştır. Dördüncüsü ise bot koordinasyonu olup, aynı cümlelerin ("Kayseri'de 6 yaşındaki küçük Suriyeli kıza tecavüz edildi") yüzlerce hesap tarafından eş zamanlı paylaşılması, gündemi yapay biçimde şişirmiştir. Hashtag'ler (#Kayseri, #SuriyelilerSınırDışıEdilsin) 150 binin üzerinde kullanım görerek olayların Adana, Hatay, Gaziantep gibi illere sıçramasını hızlandırmıştır.

Bu dinamikler, kamu güvenliği açısından doğrudan tehdit oluşturmuştur. Olaylar sırasında yüzlerce iş yeri ve araç tahrip edilmiş, 474 kişi gözaltına alınmış, 285'inin adli sicil kaydı (göçmen kaçakçılığı, yaralama, mala zarar verme vb.)

bulunduğu açıklanmıştır. Yayın yasağı getirilmesi ve sosyal medya kısıtlamaları uygulanmasına rağmen, platformdaki nefret söylemi ve dezenformasyon döngüsü toplumsal fay hatlarını tetiklemiş, kısa süreli bir güvenlik krizi yaratmıştır. Devlet SOCMINT birimleri aracılığıyla bot hesapları ve provokatörleri tespit ederek müdahale etse de dijital okuryazarlık eksikliği nedeniyle kamuoyunun manipülasyona açıklığı belirginleşmiştir.

Sonuç olarak Kayseri olayları, sosyal medyanın devlet ve kamu güvenliği bağlamında çift yönlü bir araç olduğunu vurgulamaktadır. Bir yandan gerçek suç iddialarını hızla görünür kılarak adalet talebini güçlendirirken, diğer yandan bot ağları, trol hesaplar ve provokatif içeriklerle kitlesel şiddeti körükleyebilmektedir. Bu vaka, 5651 sayılı Kanun ve ilgili düzenlemelerin yetersiz kaldığını, makine öğrenmesi tabanlı erken uyarı sistemleri ile karşı-narratif stratejilerinin acil geliştirilmesi gerektiğini göstermektedir. Gelecekte benzer krizlerin yönetilmesinde X platformunun gerçek zamanlı izlenmesi ve uluslararası işbirliği, ulusal güvenlik politikalarının vazgeçilmez unsuru haline gelmelidir (Grok, 2026).

3.4.3. Terör Örgütlerinin (PKK/FETÖ/DEAŞ) Güncel Sosyal Medya Operasyonları

Terör eylemleri günümüzün özgün sorunu olmaktan uzak olsa da, tarih boyunca hem tanımlama hem de çeşitlilik açısından köklü değişimler geçirmiştir. İlk terör örnekleri bazı çalışmalarda MÖ dönemdeki hükümdarların muhaliflere yönelik eylemleri olarak gösterilse de, modern terör algısı genellikle 1789 Fransız İhtilali sonrası gelişmelerle ilişkilendirilir. Ancak “modern” kavramı da zamanla evrilmiştir. Ulrich Beck’in “Risk Toplumu” ve “Refleksif Modernleşme” yaklaşımları, modernitenin dönüşümünü ve terörün bu süreçteki değişimini açıklamakta güçlü bir çerçeve sunar (Kürkçü ve Erendor, 2022).

Suriye İç Savaşı sırasında güney sınırında oluşturulmaya çalışılan olası terör yapılanmasına karşı Türkiye, Şah Fırat Operasyonu, Fırat Kalkanı, Zeytin Dalı, Barış Pınarı ve Bahar Kalkanı gibi harekâtlarla mücadele etmiştir. Bu operasyonlarda karşılaşılan en büyük zorluklardan biri, terör örgütü mensuplarının sosyal medya üzerinden yürüttüğü online provokasyon ve algı yönetimi faaliyetleridir. Örneğin TSK operasyonlarında “TSK hastaneyi vurdu” gibi yalan haberler hızla yayılmış, dünya medyasında geniş yer bulmuş ve Türkiye uluslararası eleştirilere maruz kalmıştır.

Ancak TSK'nın canlı görüntüler ve doğrulamalarla dezenformasyonu dakikalar içinde çürütmesi etkili olsa da, bu tür haberlerin sürekli üretilmesi hem internet hem de sosyal medya platformlarında daha sıkı engelleyici önlemler gerektirmektedir. Yakın gelecekte bu tür kısıtlamaların uluslararası düzeyde uygulanması ise oldukça zor görünmektedir. Sonuçta terör, geleneksel veya modern yöntemlerle uygulansın, bireylerin ve devletlerin varlığına yönelik ciddi tehditler yaratmaya devam eder (Kürkçü ve Erendor, 2022).

Dijital medya üzerinden algı operasyonlarının boyutunu ortaya koymak amacıyla yapılan bu çalışmada, özellikle sosyal medya hesapları ve bazı haber siteleri üzerinden hedef kitlelerin algısını yönlendirmek için yoğun fotoğraf ve içerik paylaşımı tespit edilmiştir. Göstergebilimsel analizler, bu paylaşımların terör örgütleri ve yandaşları tarafından Türkiye Cumhuriyeti'nin politik ve askeri kararlarını haksız göstermek, itibarını zedelemek amacıyla yapıldığını ortaya koymuştur. Gerçekmiş gibi sunulan kara propaganda niteliğindeki içerikler, zamansal ve mekânsal olarak Türkiye ile ilgisiz olmasına rağmen yalan ve iftiralarla servis edilerek algı yönetimi yapılmıştır. Suriye, Irak, Filistin, Mısır ve Ukrayna gibi farklı coğrafyalardaki saldırılar PKK/PYD, DAESH, Esad güçleri, Rusya veya İsrail gibi aktörlere atken, Türkiye'ye mal edilmiş; Türk askeri, polisi ve vatandaşları sorumlu tutulmaya çalışılmıştır. Bu operasyonlar bazen doğrudan, bazen ters algı yöntemiyle üretilmiş profesyonel görseller, sahte hesaplar üzerinden kamuoyu önderi gibi görünen profiller veya milyonlarca izleyiciye sahip filmlerin dramatik sahnelerinden alıntılarla gerçekleştirilmekte; yaptırımlarla karşılaşmaksızın yoğun biçimde kullanılmaktadır (Ayhan ve Çakmak, 2018).

17-25 Aralık 2013 yolsuzluk operasyonları, FETÖ medyasının algı operasyonlarıyla devam etmiştir. Örgütün yayın organları ve etki altındaki medya, soruşturmaları yargı süreci olmaktan çıkarıp medya üzerinden algı operasyonu haline getirmiştir. 2014 Ocak ayından itibaren dönemin Başbakanı'na ait olduğu iddia edilen ses kayıtlarının medyaya servis edilmesiyle itibarsızlaştırma ve istifaya zorlama hedeflenmiştir. Amacın, seçilmiş meşru hükümeti devirmek olduğu açıktır. Yolsuzluk üzerinden başarı elde edilemeyince, önceden hazırlanan "terör örgütlerine yardım" iddiası güçlendirilmiş; MİT tırları hadisesi gündeme taşınmıştır. FETÖ'nün sızdığı güvenlik birimlerinin 1 Ocak 2014 Kırıkkale ve 19 Ocak 2014 Adana'da MİT tırlarını durdurması ve görüntülerin medyaya servis edilmesiyle Türkiye ağır ithamlarla karşı

karşıya bırakılmıştır. Bu kumpasta her aşamada FETÖ yapılanmasının ve medyasının propagandası görülmüş; Türk ve dünya kamuoyunda ciddi imaj kaybına yol açılmıştır (Ölçekçi, 2018).

DAEŞ, yeni medya araçlarının özelliklerini ustalıkla kullanarak yaklaşık 100 ülkeye propaganda yapmış, on binlerce kişiyi safına katmış ve çok daha fazlasına kendini tanıtmıştır. Video paylaşım siteleriyle mücadele görüntülerini dünyaya ulaştırmış, sosyal medya üzerinden paylaşımlar yapmış, mobil uygulamalarla sempaticanlarına hizmet sunmuş, dergilerle düşüncesini meşrulaştırmaya çalışmıştır. Geleneksel medya araçlarıyla bu ölçekte etki yaratması mümkün olmazken, internetin bireysel özgürlük ve ifade özgürlüğü vurgusuyla tanımlanması DAEŞ'in işini kolaylaştırmıştır. Twitter, YouTube ve Telegram gibi platformlar belirli bir süre ifade özgürlüğü ve gizlilik gerekçesiyle DAEŞ hesaplarını kapatmada isteksiz davranmıştır. Zamanla tutum değişse de internetin temsil ettiği değerler değişmemiştir (Karakaş, 2017)

SONUÇLAR VE ÖNERİLER

4.1. Sonuçlar

Sosyal Medya Web2.0 teknolojisinin getirdiği yeniliklerle beraber ortaya çıkmış ve gelişimini devam ettirmiştir. 5 milyar kullanıcı sayısını geçen bu platformlar dünya üzerinde en geniş dijital kamusal alan haline gelmesine yol açmıştır. Sosyal Medya ilk bakışta devlet ve kamu üzerinde devletin açık istihbarat elde etmesi, afet zamanlarında hızlı iletişim sağlanması ve vatandaşların yönlendirilmesi, kriz ve kaos zamanlarında oluşan bilgi kirliliğinin önlenmesi gibi olumlu etkilerinin olduğu aynı zamanda kamu üzerinde ise ifade özgürlüğü, hızlı bilgi akışı, demokratik katılım gibi birçok olumlu etkilerinin bulunduğu görülse de tez boyunca ayrıntılı olarak üzerinde durulduğu gibi sosyal medya devlet ve kamu güvenliği üzerinde ciddi asimetrik tehditleri de beraberinde getirmektedir.

Çalışmanın temel bulgusu şudur: Sosyal Medyanın denetlenmesi güç yapısı, hiyerarşik olmayan, hızlı bilgi akışına sahip anonim yapısı nedeniyle geleneksel güvenlik anlayışlarını yetersiz kılmaktadır. Terör örgütleri -DEAŞ ve PKK- örneklerinde açıkça görüldüğü üzere- terör örgütleri bu platformları propaganda, sempatizan kazanma, eleman devşirme, eyleme teşvik etme, dijital eğitim ve finansman sağlama, grup içi iletişim ve etkileşim gibi birçok amaç doğrultusunda etkin bir şekilde kullanmaktadır. DEAŞ terör örgütünün profesyonel video prodüksiyonlarıyla yapmış olduğu propaganda faaliyetleri, PKK terör örgütünün bu platformlar aracılığıyla yapmaya çalıştığı algı yönetimi faaliyetleri, bu mecraların terör örgütleri açısından düşük maliyetli ancak yüksek etkili bir araca dönüştüğünü göstermektedir. Ortadoğu bölgesindeki birçok ülkedeki sokak hareketlerinin domino etkisi oluşturarak yayıldığı Arap Baharı isimli Halk hareketleri, Türkiye’de ortaya

çıkan Gezi Olayları isimli sokak hareketlerinde görüldüğü üzere sosyal medya kitleleri harekete geçirmede dönüştürücü rol oynamaktadır. Sosyal medyanın mobilizasyonunun bazı durumlarda kamu düzenini bozucu, siyasi istikrarsızlığa yol açıcı sonuçları doğurduğu görülmüştür.

Nitelikli dolandırıcılık, tehdit, şantaj, halkı kin ve nefrete teşvik gibi birçok suç, sosyal medya mecralarında işlenmektedir. Bu durumda bireyden topluma ve devlete doğru giden güvenlik riskleri oluşmaktadır.

Dezenformasyon ve algı yönetimi tezin kritik başlıklarından birini oluşturmaktadır. Sosyal Medyada yanlış bilgilerin ne kadar hızlı yayıldığını ve toplumsal şiddeti körükleyebileceğini Myanmar Olaylarında, Türkiye'deki Kayseri Olaylarında görmekteyiz. Yanlış bilginin hızla yayılarak toplum sağlığına ne derece zarar verebileceği Covid-19 infodemisinden anlaşılmaktadır. 6 Ocak ABD Kongre Baskınında sosyal medya aracılığıyla toplumun yönlendirilebileceği ve toplumsal şiddeti körükleyebileceği görülmektedir. Sosyal Medyanın dezenformasyon aracılığıyla kamu güvenliğini doğrudan tehdit edilebildiğini göstermektedir.

Veri güvenliği ve dijital egemenlik boyutları devlet ve kamu güvenliğinin tesisi için göz ardı edilmemelidir. Nitekim Cambridge Analytica skandalıyla sosyal medya kullanıcılarının verilerinin güvende olmadığı anlaşılmıştır. 87 milyon Facebook kullanıcısının kişisel bilgilerinin rızası olmadan toplanıp siyasi amaçlar doğrultusunda kullanıldığı ortaya çıkmıştır. Tarihte en büyük veri skandalları dan biridir. Nitekim bu olayın sonucunda kişisel bilgilerin, kullanıcıların yapmış olduğu tercihlerin, kişiselleştirilmiş tercihlerin, kullanıcıların bilerek veya bilmeyerek bıraktığı dijital ayak izlerinin ticari anlamda sosyal medya platformlarının bu platformlara ait veri depolarında saklanması ilerde istihbari anlamda da kullanılabileceği görülmüş ve kamu güvenliği açısından risk teşkil ettiği anlaşılmıştır. Kamu görevlilerinin sosyal medya kullanımında sahte profil operasyonuna dikkat etmesi gerekmektedir. Tapu Müdürlüğündeki bir memurla duygusal bağ kuran sahte profile sahip birisinin devlet görevlisine ait tapu kayıtlarını incelediği görülmüştür. Askerlerin kıışlalarda veya operasyon üs bölgelerinde fotoğraf video paylaşmaması gerekmektedir. Konum bilgisi teçhizat bilgisi gibi kritik bilgiler hasım unsurlar tarafından ele geçirilebilmektedir. Reklam gelirlerinin vergilendirilmemesi, içerik telif haklarındaki belirsizlikler devletin dijital egemenliğini zayıflatarak sermaye akışının ülke dışındaki platformlara aktarmaktadır.

Savaş esnasında tüm tehdit unsurlarının beraber kullanıldığı hibrit savaş türünde vekil güçler, hedef ülkenin halkına yönelik algı yönetimi, dezenformasyon faaliyetleri ve hedef ülkenin dijital alanlarına yönelik siber saldırılar ile birlikte konvansiyonel savaşın birlikte hareket etmesi hibrit savaşın somut halini Rusya-Ukrayna savaşında görülmektedir. Bu savaşta sosyal medyanın, her iki tarafın psikolojik harp sahası ve propaganda alanı haline geldiğini göstermektedir. Siber saldırı anlamında Stuxnet olayı, hibrit savaşın en önemli örneklerinden biridir. Sosyal medya, etki operasyonları ve istihbarat toplama faaliyetlerinin ayrılmaz bir parçası haline gelmiştir. Kullanıcıların kendi isteğiyle kişisel bilgilerini paylaşmaktadır. Kullanıcılar kendi ve çevresi ile alakalı fotoğraf, video paylaşarak zengin bir meta veri havuzu sunmaktadır. Fotoğraf, video, coğrafi konum gibi bilgiler de açıkça paylaşılmaktadır. Bazı sosyal medya uygulamaları kimlik doğrulaması için kimlik numarası ve cep telefon numarası gibi kişisel bilgiler talep etmektedir. Kişisel bilgilerin açıkça paylaşılması, devletlerin istihbarat birimleri açısından eğilimleri belirleme, potansiyel tehditleri erken tespit etme, arşiv araştırması yapma gibi birçok imkan sağlamaktadır. 2012 Londra Olimpiyatları sırasında Londra Polisinin Flickr isimli sosyal medya platformunda yüklenen fotoğraflardan yüz tanıma sistemi aracılığıyla potansiyel tehditleri tespit etmesi aynı şekilde Irak'ta SOMİS (Social Media Intelligence System) ile terör ağlarının bağlantı düğümleri ve olası terör saldırılarını önceden tespit etmiştir. Terör örgütlerinin kendi istihbarat faaliyetlerinde sosyal medyayı açık kaynak olarak kullanması da söz konusudur. Bu nedenle kamu görevlilerinin özellikle askerlerin bağlı bulunduğu kışla gibi görev alanlarını belirten fotoğraf ve video paylaşımı yapmamaları gerekmektedir. 2008 Mumbai Taj Mahal Otel saldırısında teröristlerin sosyal medyayı ve dijital alanı istihbarat elde etme anlamında etkin şekilde kullandıkları görülmektedir.

Devletler sosyal medyanın ulusal güvenliğe ve bireysel haklara yönelik birtakım tehditler içerdiğini anlayarak devlet ve kamu güvenliğini artırmaya yönelik birtakım yasal tedbirler almıştır. Bu çalışmada farklı yapıları temsilen Almanya ve Avrupa Birliği, Çin ve Rusya, Türkiye'deki yasal yapılan yasal düzenlemeler ele alınmıştır.

Sonuç olarak sosyal medya tamamen eğlence ve iletişim aracı değil aynı zamanda devlet ve kamu güvenliğini tehdit eden bir araçtır. Tez boyunca incelenen vakalar ve literatür, bu mecraların çift yönlü karakteristik yapısını ortaya koymakta

olup geleneksel güvenlik anlayışı ile değil modern güvenlik anlayışı ile ele alınması gerekmekte ve güvenlik politikalarını buna göre şekillendirmek gerekmektedir.

4.2. Öneriler

1-Yasal ve kurumsal çerçeve güçlendirilmelidir. Bu noktada bot hesapların engellenmesi, tespit edilmesinde sahte profiller ve koordineli dezenformasyon kampanyalarına yönelik sosyal medya platformlarıyla devlet kurumları arasında iş birliği yapılması gerekmektedir. Buna göre Sosyal Medya platformlarına yüklenen sorumluluklar arttırılmalıdır. Bot hesaplarla dezenformasyon ürettiği tespit edilen kişilere cezai ve idari yaptırımların arttırılması gerekmektedir.

2- Henüz kendi kimlik ve benliğini oluşturamamış çocukların kimlik inşası ve karakterinin oluşması sürecinde sosyal medyadaki kötü örnek teşkil edecek içeriklere çocukların maruz kalmaması için 16 yaş altındaki çocukların sosyal medya hesabı açması yasal olarak engellenmelidir. Kimlik doğrulaması yapılmalıdır. Buna rağmen 16 yaşından küçük ve sosyal medya hesabı olduğu ve sosyal medya aracılığıyla suç işlediği tespit edilen çocukların ailesi de yasal sorumluluk altına girmelidir.

2- Dijital okuryazarlığın güçlendirilmesi gerekmektedir. Sosyal medyayı kullanan kullanıcılar, karşısına çıkan bilgilerin doğru olup olmadığını ayırt edebilmelidir. Dolandırıcılık gibi suçlara maruz kalınmaması, dezenformasyonlara kapılmaması, terör örgütleri ve kötü niyetli kişilerin ağlarına takılmamaları için toplumun dijital suçlarla mücadele kapsamında bilinçlendirilmesi gerekmektedir.

3-Kamu kurumları ve güvenlik personeli için zorunlu “sosyal medya kullanım rehberleri” hazırlanmalıdır. Sosyal medya güvenliği, sosyal medya kullanımı ve veri koruma eğitimleri verilmelidir. Kritik noktalarda ve üslerde görev yapan tüm güvenlik görevlilerine sosyal medya kullanımı ile ilgili eğitimler verilmelidir.

4-Socmınt kapasitesi güçlendirilmelidir. Emniyet, İstihbarat ve diğer güvenlik kurumları bünyesinde açık kaynak istihbaratı sağlama, konum tespiti sağlama, kullanıcıların gerçek kimliğini tespit etme olanağını sağlayan yerli yazılımların geliştirilmesi ve yeterli teknik personelin eğitilmesi gerekmektedir.

5-Dijital egemenlik ve veri politikaları gözden geçirilmelidir. Sosyal medya platformlarında paylaşılan verilerin depolandığı, üçüncü tarafla reklam ve pazarlama amacıyla kullanıldığı bilinmektedir. Kullanıcı verilerinin depolandığı, kişisel verilerin kaydedildiği, konum bilgisi gibi bilgileri elinde tutan, hatta algoritma ve yapay ve kişiselleştirilmiş desteğiyle duygu analizleri ve kişiselleştirilmiş tercihlerle kullanıcıları adeta en yakını kadar tanıyabilen sosyal medya platformları, bir ülkenin vatandaşlarının genel eğilimi, siyasi tutum ve değişkenlikleri, tercihleri gibi birçok faktörleri analiz edebilecek büyük veriye sahip olabilmektedirler. Bu nedenle yerli imkanlarla geliştirilen, verilerin ülke içinde saklandığı, devlet denetimine tamamen açık sosyal medya platformlarının geliştirilmesi teşvik edilmelidir. Reklam ve sponsorluk gelirlerinin vergilendirilmesi konusunda daha bütüncül yaklaşımlar benimsenmelidir.

6- Uluslararası İşbirliği arttırılmalıdır. Hibrit tehditler ve sınırları aşan dijital dezenformasyonla mücadelede devletlerin istihbarat birimleri ve uluslararası örgütlerle ortak çalışmalar yürütülmeli, Interpol gibi ortak birimler kurulmalı, Devletlerarası veri paylaşımları yapılmalıdır.

7-Teknolojik Gelişmelere Yönelik Güvenlik Politikaları Uygulanmalı Sosyal Medyanın etkin kullanımında devletin imkân ve kabiliyetini arttıran bir güç, etkisiz kullanımında ulusal güvenliği azaltabilen bir tehdit niteliği taşımaktadır. Bu nedenle güvenlik politikaları gelişmekte olan yapay zekâ teknolojisine yönelik olarak şekillenmelidir. Buna göre Sosyal medya platformlarının algoritmasına yönelik denetim yazılımları geliştirme, kolluk güçlerinin sosyal medya devriyelerinde terör örgütü mensuplarını tespit etmede kullandığı yüz tanıma teknolojisinin geliştirilmesi, belli suç içeren kelimelerin sıklıkla kullanıldığında uyarı verecek yazılımların geliştirilmesi, Socmint elde etmek amacıyla şüphelilere yönelik kullanıcı analizi yapan sosyal medya istihbaratı analiz programı geliştirilmeli, yapay zeka destekli dezenformasyon tespit programı geliştirilmelidir. Buna benzer programlar ve yazılımlar geliştirirken güvenlik ve özgürlük dengesi gözetilmeli bu programlar uygulanırken çerçevesi yasal olarak savcı ve hakim iznine bağlı olarak düzenlenmelidir. Buna göre güvenlik politikaları, proaktif ve bütüncül bir anlayışla teknolojik gelişmeleri takip edip uygulayan anlayışla yeniden şekillenmelidir.

Sosyal Medya platformlarının hedef ülkenin insanlarını etkileyerek siyasi, sosyal, ekonomik, hukuki olarak birçok alanda etkilemektedir. Örnek vermek

gerekirse siyasi olarak seçim sürecine etki etmek suretiyle kullanıcıların duygularının manipüle edilmesi söz konusu olabilir. Ekonomik olarak kullanıcıların ekonomi hakkındaki gelecek beklentisi kötü yönlendirilerek kitlesel beklentilerin kötüleşmesini sağlayabilir, ekonomik kriz ortamı oluşmasına destek verebilir. Sosyal olarak kişilerin kötü haberlere maruz kalarak gelecek hakkında umutsuzluğa kapılması, depresyona girmesi gibi birçok olumsuz etkilere sebep olabilir. Toplumun sosyal yapısı etki altına alınabilir. Hukuki olarak verilerinin başka amaçlar doğrultusunda kullanılabilir ve istihbarat örgütleri ve diğer devlet dışı örgütler tarafından kullanılarak güvenlik zafiyetine yol açabilir.

Bu bağlamda önemle belirtilmesi gereken husus, sosyal medyaya yönelik yasal düzenlemeler ve idari tedbirlerin kısıtlı kalabildiğidir. Bu çalışmada çeşitli önlemler ele alınmış olmakla birlikte yapay zeka teknolojisi aracılığıyla devreye girecek yazılımsal tedbirlerin en etkili, hızlı ve kalıcı tedbir olacağı değerlendirilmektedir. Bu doğrultuda; duygu analizi, yüz tanıma özelliği, birtakım seçilmiş kelimelerin sıklıkla kullanılmasının tespit ve analizi, radikalleşen insanların eylemsel faaliyet öncesinde tespit edilmesi, socmint elde etmek amacıyla şüphelilere yönelik kullanıcı analizi yapan sosyal medya istihbaratı analiz programı büyük önem taşımaktadır. Bunların yanında yapay zeka destekli dezenformasyon tespit programı geliştirilmelidir. Söz konusu programlar ve yazılımlar geliştirirken güvenlik ve özgürlük dengesi gözetilmelidir.

Sonuç olarak sosyal medya platformları ile devlet arasında yapılacak iş birliği doğrultusunda sosyal medya algoritmalarına entegre edilecek çok katmanlı yazılımsal çözümler aracılığıyla güvenlik anlayışının reaktif bir yaklaşımdan proaktif bir yaklaşıma doğru evrilmesi gerektiği değerlendirilmektedir.

KAYNAKLAR

- Acar, Ü., ve Urhal, Ö. (2007). *Devlet – güvenlik – istihbarat – terörizm*. Adalet Yayınevi.
- Adalet ve Kalkınma Partisi. (2025). @akparti – Resmî YouTube Kanalı. YouTube. <https://www.youtube.com/@akparti>
- Afyon Kocatepe Üniversitesi. (2025). *Sayfa hazırlama kılavuzu*. <https://blog.aku.edu.tr/sayfa-hazirlama-kilavuzu/>
- Akca, M. A. (2016). Sosyal mühendislik ile yapılan saldırılarının doğal dil işleme teknikleri ile engellenmesine yönelik web servis geliştirilmesi. *Selçuk Üniversitesi Mühendislik, Bilim ve Teknoloji Dergisi*, 4(2), 111–120.
- Aksoy, A., ve Türkölmez, O. (2020). Dijital çağda demokrasiyi çağırmak: Cambridge Analytica skandalı. *Journal of Political Administrative and Local Studies*, 3(1), 41-59. <https://doi.org/10.37460/j.2636-7823>
- Akyıldız, S., ve Yılmaz, K. (2020). Sosyal medya konulu araştırmaların bilim haritalama tekniği ile bibliyometrik analizi. *OPUS International Journal of Society Researches*, 16(28), 1416–1451. <https://doi.org/10.26466/opus.680835>
- Akyılmaz, B., Sezginer, M., ve Kaya, M. (2018). *Türk idare hukuku*. Seçkin Yayıncılık.
- Akyol C, Ünal E ve Aydın F (2012) Sosyal Ağlar, Ayfer Alper (ed.), Pelikan Yayıncılık, Ankara, 5-53.
- Alakoyun, B. (2025, 6 Şubat). İstanbul merkezli “panel” operasyonunda tutuklanan şüphelilerin ifadesine ulaşıldı. *Anadolu Ajansı*. <https://www.aa.com.tr/tr/gundem/istanbul-merkezli-panel-operasyonunda-tutuklanan-suphelilerin-ifadesine-ulasildi/3473643>
- Alieva, A. (2025). *Rusya–Ukrayna savaşı’nda Twitter (X) ve Facebook üzerinden yürütülen propagandaların savaşın seyrine etkileri* [Yüksek lisans tezi, Marmara Üniversitesi].
- Alpaslan, B. A., ve Delibalta, E. (2025). Algorithmic Nostalgia: How Machine Learning Curates Our Emotional Connections to the Past. *AJIT-e: Academic Journal of Information Technology*, 16(3), 187-206.
- Anderson, M., & Jiang, J. (2018). *Teens, social media & technology 2018*. Pew Research Center. <https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/>

- Arat, Y., Aycan, Z., Buğra, A., Gürkaynak, R., Kalaycıoğlu, E., & Keyder, Ç. (2013). *Siyaset ve toplum bilim perspektifinden Gezi Parkı olayları* (Çalışma Grubu Raporu). Bilim Akademisi. <https://bilimakademisi.org/wp-content/uploads/2013/08/Siyaset-ve-Toplum-Bilim-Perspektifinden-Gezi-Parki-Olaylari.pdf>
- Arena. (2025, 30 Mayıs). *The history of online chat: from the 1970s to 2025*. Arena.im <https://arena.im/group-chat/history-of-online-chat/>
- Arıcan, M. K. (2015). Birlikte yaşamının felsefi temelleri. C. Türer (Ed.), *Ortak yaşama kültürü ve felsefesi* içinde (ss. 83–105). Türk Felsefe Derneği Yayınları.
- Arık, E. (2013). Sıradan insanın yükselişi: Sosyal medya şöhretleri. *İletişim ve Diplomasi*, 1, 97–112. <https://izlik.org/JA48TH35ZW>
- Arıkan, S. M., ve Benzer, R. (2018). Bir güvenlik trendi: Bal küpü. *Acta Infologica*, 2(1), 1-11.
- Arklan, Ü. (2016). Sosyal medyanın siyasal amaçlı kullanımı: Ağ kuşağının kullanım alışkanlıkları üzerine bir araştırma. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*. <https://doi.org/10.19145/gujofoc.87504>
- Arrighi, G., Hopkins, T. K., & Wallerstein, I. (2015). *Sistem karşıtı hareketler* (3. Baskı) (C. Kanat, B. Somay, & S. Sökmen, Çev.). Metis Yayıncılık.
- Arslan, A. C. (2025). Yeni güvenlik konsepti bağlamında dezenformasyonla mücadele. *Iğdır Üniversitesi Sosyal Bilimler Dergisi*, (38), 361–380.
- Arslan, Ç., ve Özel, K. C. (2021). Dillere pelesenk bir tartışma: “Sosyal medya düzenlemeleri” (Dünü, bugünü ve yarını). *Ankara Barosu Dergisi*, 79(3), 255–284.
- Arslan, H. (2016). Farklı bir perspektiften terörizm. *OPUS Uluslararası Toplum Araştırmaları Dergisi*, 6(11), 491-520.
- Arslan, H. (2022). Sosyal medyada paylaşılan post-truth söylemlerin ve dezenformasyonların Türkiye’nin güvenliğine etkileri. *International Academic Social Resources Journal*, 7(44), 1874-1885.
- Arya, V., Sethi, D., & Paul, J. (2019). Does digital footprint act as a digital asset? Enhancing brand experience through remarketing. *International Journal of Information Management*, 49, 142-156.
- Aryaeinejad, K., ve Scherer, T. L. (2024). *The role of the Internet and social media on radicalization: What research sponsored by the National Institute of Justice tells us*. National Institute of Justice, U.S. Department of Justice, Office of Justice Programs. <https://www.ojp.gov/pdffiles1/nij/305797.pdf>
- Aslan, S. (2017). Gezi Parkı Eylemlerinin Farklı Boyutlarıyla Bir Değerlendirmesi. *Birey ve Toplum Sosyal Bilimler Dergisi*, 6(2), 153-178. <https://izlik.org/JA57DS32AM>
- Ateş, H. (2012). *Kamu güvenliğinde istihbarat sisteminin değerlendirilmesi* [Yüksek lisans tezi, Atılım Üniversitesi Sosyal Bilimler Enstitüsü]. <https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=FP4d7U0eZYoxlvnZ9rxYFw&no=uuNcm-v66kD1fzrtG2r0TQ>

- Avrupa Komisyonu. (2018). *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation*. Avrupa Birliği Yayın Ofisi.
- Aydın, A. (2015). Dijital vatandaşlık. *Türk Kütüphaneciliği*, 29(1), 142–146. <https://izlik.org/JA33PW62KZ>
- Aydın, A. F. (2023). Sosyal medyada dezenformasyon ve manipülasyon: 2023 Kahramanmaraş depremi örneği. *İnsan ve Toplum Bilimleri Araştırmaları Dergisi*, 12(5), 2603–2624.
- Aydın, A. F. (2023). Sosyal medyada dezenformasyon ve manipülasyon: 2023 Kahramanmaraş depremi örneği. *İnsan ve Toplum Bilimleri Araştırmaları Dergisi*, 12(5), 2603–2624. <https://doi.org/10.15869/itobiad.1283358>
- Aydoğan, T. (2024). Sosyal medya yalnızlığı. *Uluslararası Sosyal Bilimler Akademik Araştırmalar Dergisi*, 8(16), 35–38. <https://doi.org/10.58201/utsobilder.1591433>
- Ayhan, A. Ve Erkan, G. (2018). Siyasal iletişimde dezenformasyon ve sosyal medya: Bir doğrulama platformu olarak Teyit.Org. *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*, (30), 201–223.
- Ayhan, A., ve Çakmak, F. (2018). Türkiye’ye yönelik algı operasyonlarının dijital medyaya yansımaları. *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*, 29(Özel Sayı), 11-35.
- Ayoob, M. (1995). *The third world security predicament: State making, regional conflict, and the international system*. Lynne Rienner Publishers.
- Azucar, D., Marengo, D., ve Settanni, M. (2018). Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis. *Personality and Individual Differences*, 124, 150-159.
- Bahar, A. (2020). Polislik perspektifinden dijital 116iteratüre116yon ve dezenformasyon: Covid-19 örnek olayı bağlamında bir analiz. *OPUS Uluslararası Toplum Araştırmaları Dergisi*, 16(30), 2760–2794.
- Bakan Gürlek’in kayıtlarını sorgulayan teknikerin ifadesi ortaya çıktı: Ayşegül tarafından kandırıldım. (2026, 24 Mart). *CNN Türk*. <https://www.cnnturk.com/turkiye/bakan-gurlekin-kayitlarini-sorgulayan-teknikerin-ifadesi-ortaya-cikti-aysegul-tarafindan-kandirildim-2409574>
- Bakshy, E., Messing, S., & Adamic, L. A. (2015). Exposure to ideologically diverse news and opinion on Facebook. *Science*, 348(6239), 1130–1132. <https://doi.org/10.1126/science.aaa1160>
- Banks, J. (2014). *Countering hate speech online: Organisations and collectives*. Ashgate Publishing.
- Baş, M., Erdoğan Tarakçı, İ., ve Aslan, R. (2022). *Dijitalleşme 2*. Efe Akademi Yayınları. <https://play.google.com/books/reader?id=V56jEAAQBAJ>
- Başaran, F. (2006). Bir teknolojik yenilik olarak internetin tarihi: Ulusal yenilik sistemi, kamu politikaları ve standartlar. *Kültür ve İletişim*, 9(18), 9–32. <https://izlik.org/JA95YT75WR>
- Bayhan, V. (2014). Yeni toplumsal hareketler ve Gezi Parkı direnişi. *Birey ve Toplum*, 4(7), 23-57.

- Bayram, M., ve Yaylar, Y. (2016). Myanmar'daki Budist-Müslüman çatışmasının tarihî dinamikler. *Uluslararası Sosyal Araştırmalar Dergisi*, 9(44), 367-373.
- BBC News Türkçe. (2026, Nisan). Göktaş: 15 yaş altı sosyal medya yasa teklifi bu ay sonu Meclis'e geliyor. *BBC News Türkçe*. <https://www.bbc.com/turkce/articles/czx3k6vpyvyo>
- BBC News Türkçe. (2026, Nisan). Göktaş: 15 yaş altı sosyal medya yasa teklifi bu ay sonu Meclis'e geliyor. <https://www.bbc.com/turkce> adresinden edinilmiştir.
- BBC. (2018, 6 Kasım). Facebook admits it was used to 'incite offline violence' in Myanmar. *BBC*. <https://www.bbc.com/news/world-asia-46105934>
- Begenirbaş, M. Ve Ünver, O. C. (2021). Milli güvenlik stratejisi ve askeri güç. M. Begenirbaş, R. C. Yalçın ve S. Yenal (Ed.), *Strateji ve güvenlik alanında temel ve güncel yaklaşımlar* içinde (ss. 93-125). Nobel Akademik Yayıncılık.
- Bıçakçı, S. (2016). Nükleer tesislerin siber güvenliğine giriş. In S. Ülgen & G. Kim (Eds.), *Türkiye'de siber güvenlik ve nükleer enerji* (ss. 100-146). Ekonomi ve Dış Politika Araştırmalar Merkezi.
- Bilge, B. (2019). Şantaj suçu. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 6(1), 131-160.
- Bilgi Bilimi. (t.y.). Web 1.0 Web 2.0 Web 3.0 nedir? <https://bilgibilimi.net/web-1-0-web-2-0-web-3-0-nedir/>
- Bilim Akademisi Derneği. (2013). *Siyaset ve toplum perspektifinden Gezi Parkı olayları*. <https://bilimakademisi.org/wp-content/uploads/2013/08/Siyaset-ve-Toplum-Bilim-Perspektifinden-Gezi-Parki-Olaylari.pdf>
- Binark, M. (2007). Yeni medya çalışmalarında yeni sorunlar. M. Binark (Ed.), *Yeni medya çalışmaları* içinde (ss. 21-44). Dipnot Yayınları.
- Binark, M. Ve Bayraktutan, G. (2013). *Aydın karanlık yüzü: Yeni medya ve etik*. Kalkedon Yayınları.
- Boyd, D., & Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society*, 15(5), 662-679.
- Boyd, D., & Ellison, N. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210-230.
- Bradshaw, S. (2020). *Industrialized disinformation: 2020 global inventory of organized social media manipulation*. Oxford Internet Institute.
- Brown, A. J. (2020). Should I stay or should I leave? Exploring (dis)continued Facebook use after the Cambridge Analytica scandal. *Social Media + Society*, 6(1). <https://doi.org/10.1177/2056305120913884>
- BTK. (2016). *2016-2019 ulusal siber güvenlik stratejisi*. Bilgi Teknolojileri ve İletişim Kurumu.
- Bulunmaz, B. (2014). Yeni medya eski medyaya karşı: Savaşı kim kazandı ya da kim kazanacak? *Karadeniz Teknik Üniversitesi İletişim Araştırmaları Dergisi*, 4(1), 22-29. <https://izlik.org/JA68CW89RT>

- Bulut, Y., ve Aslan, M. M. (2021). Covid-19 pandemisinin sosyo-ekonomik etkileri ve akıllı kent uygulamaları. *Iğdır Üniversitesi Sosyal Bilimler Dergisi*, (ICOMEÖ Özel Sayısı), 261-276.
- Bural, E. B. (2024). Sosyal medya istihbaratı çerçevesinde harekât güvenliği. *İstihbarat Çalışmaları ve Araştırmaları Dergisi*, 3(1), 127–152.
- Cadwalladr, C. (2017, 7 Mayıs). The great British Brexit robbery: How our democracy was hijacked. *The Guardian*. <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy>
- Can, O., ve Ercan, M. (2022). Yargı bağımsızlığı perspektifinde ‘sosyal medya adaleti’. *Socrates Journal of Interdisciplinary Social Studies*, 15, 255–284. <https://socratesjournal.org/index.php/pub/article/view/111/101>
- Cartwright, J. E. (2011). *Memorandum for chiefs of the military services commanders of the combatant commands directors of the joint staff directorates, on joint terminology for cyberspace operations*. Joint Chiefs of Staff.
- Castells, M. (2008). *Ağ toplumun yükselişi* (2. Baskı) (E. Kılıç, Çev.). İstanbul Bilgi Üniversitesi Yayınları.
- Ceng, E. (2018). Algı yönetimi aracı olarak Twitter kullanımına ilişkin siyasal bir analiz. *Erciyes İletişim Dergisi*, 5(4), 663-689.
- CNN Türk. (2026, 21 Şubat). Tapu müdürlüğünde “sosyal medya” operasyonu: Bakanın kayıtlarını sorgulattılar. *CNN Türk*. <https://www.cnnturk.com/turkiye/bakan-gurlekin-tapu-kayitlarinin-usulsuz-sorgulanmasina-iliskin-yeni-gelisme-bir-kisi-daha-gozaltina-alindi-2410023>
- Commission of the European Communities. (2009, Mart 30). *Protecting Europe from large scale cyber-attacks and disruptions: Enhancing preparedness, security and resilience*.
- Costello, M., Barrett-Fox, R., Bernatzky, C., Hawdon, J., ve Mendes, K. (2020). Predictors of viewing online extremism among America’s youth. *Youth and Society*, 52(5), 710–727.
- Coşkun, M. B., ve Börklüoğlu, L. (2021). Türk kamu yönetiminde yapısal reform çalışmalarında “müdahale alanı” meselesi. *Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi*, 11(1), 429–440. <https://doi.org/10.30783/nevsosbilen.887144>
- Council of Europe. (2019). *Social rights and the fight against hate speech: A guide for practitioners and youth workers*. Council of Europe Publishing.
- Cozumpark. (2025, Kasım 5). MİT harekete geçti: Signal mesajları nedeniyle TÜBİTAK ve ASELSAN’da gözaltılar başladı. <https://www.cozumpark.com/mit-harekete-gecti-signal-mesajlari-nedeniyle-tubitak-ve-aselsanda-gozaltilar-basladi/>
- Creemers, R. (2015). Cyber China: Upgrading propaganda, public opinion work and social management 118iterat twenty-first century. *Journal of Contemporary China*, 24(93), 85-100.
- Cullen, P. J. (2017). Understanding hybrid warfare. Norwegian Institute of International Affairs.

- Cumhuriyet Halk Partisi. (2025). @chpgenelmerkezi – Resmî YouTube Kanalı [YouTube kanalı]. YouTube. <https://www.youtube.com/@chpgenelmerkezi>
- Cyberarts. (2024). 2024 Cyberarts siber bülten. Cyberarts.
- Çağlayan, Y. (2017). *Sosyolojik savaş*. İstanbul: Timaş Yayınları.
- Çakır, H. (2007). Geleneksel gazetecilik karşısında internet gazeteciliği. *Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 1(22), 123–149.
- Çalışkan, M., ve Mencik, Y. (2015). Değişen dünyanın yeni yüzü: Sosyal medya. *Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi*, (50), 254–277. <https://izlik.org/JA85ZL57PK>
- Çaycı, A. E. (2019). Sosyal medyada dijital yemek kültürü. *International Journal of Cultural and Social Studies*, 5(1), 120–136.
- Çelik, Ş. (2013). Stuxnet saldırısı ve ABD'nin siber savaş stratejisi: Uluslararası hukukta kuvvet kullanmaktan kaçınma ilkesi çerçevesinde bir değerlendirme. *Dokuz Eylül Hukuk Fakültesi Dergisi*, 15(1), 137–175.
- Çetin, H. (2014). Kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi. *Akdeniz İİBF Dergisi*, 14(29), 86–105.
- Çınar, B. (1997). *Devlet güvenliği, istihbarat ve terör*. SAM Yayınları.
- Çiftçi, H. (2024). Analysis of Türkiye's cybersecurity strategies: Historical developments, scope, content and objectives. *Sakarya University Journal of Science*, 28(1), 204–219.
- Çubukcu, A. (2020). Almanya'nın sosyal ağ yasasının nefret söylemi içeriklerinin kaldırılması bakımından incelenmesi: Türkiye için öneriler. *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi*, 3(2), 164–181.
- Dal, E. P., ve Erdoğan, E. (2020). *Dezenformasyonla mücadele el kitapçığı*. <https://emreerdogan.com/rdmedu/>
- Dal, F. (2019). *A case study on the analysis of attacks against Internet of Things systems with honeypot systems* [Yüksek lisans tezi, Hacettepe Üniversitesi]. <https://tez.yok.gov.tr/>
- DEMGeneMerkezi – Resmî YouTube Kanalı. (2025, Kasım 11). *DEMGeneMerkezi* [YouTube kanalı]. YouTube. <https://www.youtube.com/@DEMGeneMerkezi>
- Demir, H. (2025, Eylül 15). 16 yaşında bir çocuk nasıl IŞİD'li oldu? *Fikir Turu*. <https://fikirturu.com/toplum/16-yasinda-bir-cocuk-nasil-isisli-oldu/>
- Doğan, S., ve Çelik, R. (2023). Postmodern medyanın analizi: Sosyal medya örneği. *Journal of Economics and Political Sciences*, 3(2), 157–165.
- Dopinger Blog. (2025, Ekim 30). Sosyal imleme nedir? *Dopinger*. <https://www.dopinger.com/tr/blog/sosyal-imleme-nedir>
- Dover, R. (2019). SOCMINT: A shifting balance of opportunity. *Intelligence and National Security*, 34(1), 1-17. <https://doi.org/10.1080/02684527.2019.1694132>
- Dökmen, Ü. (2010). *Varolmak gelişmek uzlaşmak: Evrenle uyumlaşma sürecinde*. Sistem Yayıncılık.

- Durmuş, A. (2023). Sosyal medyada propaganda: Rusya-Ukrayna savaşı örneği. *AJIT-e: Academic Journal of Information Technology*, 14(52), 41–69.
- Dülger, M. V., ve Özkan, O. (2021). *Sosyal medya yasası Meclis'ten geçti: Peki, şimdi?* ResearchGate. <https://www.researchgate.net/publication/349552885>
- Dünya Sağlık Örgütü. (2020, Şubat 2). *Novel Coronavirus (2019-nCoV): Situation report – 13*. <https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf>
- Eba. (t.y.). Eğitim 3.0 – Modül 1.1 – İnternetin tarihi gelişimi – Web 3.0. <https://etwinningonline.eba.gov.tr/lesson/egitim-3-0-modul-1-1-internetin-tarihi-gelisimi-web-3-0/>
- Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Dairesi Başkanlığı. (1993–2019). *EGM-KOMDB raporları*.
- ENISA. (2023). *About ENISA: The European Union Agency for Cybersecurity*. <https://www.enisa.europa.eu/about-enisa>
- Er, H. İ. (2025, Kasım 28). Sosyal imleme nedir? *Dopinger*. <https://www.dopinger.com/tr/blog/sosyal-imleme-nedir>
- Erdal, C. (2013). Sosyal medya ve paylaşım kültürü. C. Bilgili & G. Şener (Ed.), *Sosyal medya ve ağ toplumu-2: Kültür, kimlik, siyaset içinde* (ss. 15–38). Reklam Yaratıcıları Derneği.
- Erdoğan, M., & Kaşlı, E. (2022). Sosyal medyanın arka sokakları: Gençlere karşı işlenen sanal şantaj suçu. İnce, A., Cevherli, K., Koçak, M. F., Adalar, A. A., & Kaya Aitaouri, S. (Ed.), *Uluslararası Gençlik Araştırmaları Sempozyumu 2022 tam metin bildiriler kitabı* içinde (ss. 144–150). SAÜ Gençlik Çalışmaları Uygulama ve Araştırma Merkezi.
- Erendor, M. E. (2025). *Analysis of threat perceptions: NATO and Türkiye's cyber terrorism policies*. CRC Press.
- Ersöz, B. (2020). Yeni nesil web paradigması: Web 4.0. *Bilgisayar Bilimleri ve Teknolojileri Dergisi*, 58-65.
- Ertekin, Ş. (2006). *1980 sonrası dönemde Türkiye'de siyasal istikrar-vergilendirme ilişkisi* [Doktora tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü]. <https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=baMQxME0-8zyYWmrGr65Cw&no=FHmopWXK4wmbynMNwvE-LQ>
- Ete, H., ve Taştan, C. (2014). *Kurgu ile gerçeklik arasında Gezi eylemleri*. SETA Yayınları.
- Eticaret Marketing. (2025, Ekim 30). Pinterest nedir ve nasıl kullanılır? *Eticaret Marketing*. <https://www.eticaretmarketing.com/pinterest-nedir-ve-nasil-kullanilir/>
- European Parliament & Council of the European Union. (2022, Ekim 19). *Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act)*. EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065>
- Fallis, D. (2015). What is disinformation?. *Library Trends*, 63(3), 401-426.

- FATF. (2018). *Financing of recruitment for terrorist purposes*. Financial Action Task Force. <https://www.fatf-gafi.org/publications/methodsandtrends/documents/financing-recruitment-terrorist-purposes.html>
- FATF. (2023). *Crowdfunding for terrorism financing*. Financial Action Task Force. <https://www.fatf-gafi.org/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html>
- Ferrara, E. (2017). Contagion 121iteratü of extremist propaganda in social networks. *Information Sciences*, 418–419, 1–12. <https://doi.org/10.1016/j.ins.2017.07.030>
- Fındıklı, R., & Bilgiç, V. K. (2006). *İdare hukuku*. Anadolu Yayıncılık.
- Fix, L., & Keil, S. (2022). *NATO and Russia after the invasion of Ukraine*. The German Marshall Fund of the United States. <https://www.gmfus.org/sites/default/files/2022-04/Fix%20%26%20Keil%20-%20NATO%20-%20Geopolitics%20-%20Russia%20-Brief%20-%20FINAL.pdf>
- Gerasimov, V. (2016). The value of science is in the foresight: New challenges demand rethinking the forms and methods of carrying out combat operations (R. Coalson, Çev.). *Military Review*, 96(1), 23–29.
- Goodman, M. (2017). *Geleceğin suçları: Dijital dünyanın karanlık yüzü*. Timaş Yayınları.
- Göçoğlu, V. (2019). Türkiye’de merkezi yönetimin sosyal medya kullanımı: Bakanlıkların Twitter hesapları üzerine bir analiz. *Uluslararası Yönetim Akademisi Dergisi*, 2(2), 422–444. <https://doi.org/10.33712/mana.600666>
- Gökçe, A. F. (2016). Adalet kavramı kapsamında geçmişle hesaplaşma ve uzlaşma: Türkiye. *Bilge Strateji*, 8(15), 113–142.
- Gökçe, A. F. (2018). Dijital çağın küreselleşen terörü: Postmodern terörizm. 15. *Kamu Yönetimi Formu (KAYFOR 15) bildiriler kitabı* içinde (ss. 253–267).
- Gökçe, A. F. (2021). Güvenlik anlayışında değişimler: Postmodern terörizm. O. Göksu (Ed.), *Algı yönetimi* içinde (ss. 331–354). Literatürk Academia.
- Gölbaşı, S. D., & Metinbaş, S. (2020). Kovid-19 pandemisi ve bilgi salgını. *Eskişehir Türk Dünyası Uygulama ve Araştırma Merkezi Halk Sağlığı Dergisi*, 5, 126–137.
- Gümüşbaş, A. (2016). Siber savaş hukukunda meşru müdafaa hakkı ve isnat edilebilirlik: Stuxnet ve Aramco saldırıları. R. Akkaş (Ed.), *Türk-Arap ilişkileri: Çok boyutlu güvenlik inşası* içinde (ss. 181–194). TASAM Yayınları.
- Günday, M. (2011). *İdare hukuku* (10. Baskı). Ekin Basım Yayın Dağıtım.
- Güranlıoğlu, N. (2016). *Nefret söylemi ve nefret suçunun Türkiye üzerinden örneklerle incelenmesi*. Academia.edu.
- Güzel, C. (2020). Sosyal medyanın neliği, gelişimi ve kullanım alanları üzerine kuramsal bir inceleme. *Sosyolojik Düşün*, 5(1), 93–112.
- Hafizoğulları, Z., & Özen, M. (2010). *Türk ceza hukuku özel hükümler: Kişilere karşı suçlar*. US-A Yayıncılık.

- Halisdemir, E. (2021). *National cybersecurity organisation: Turkey*. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). <https://ccdcoe.org/>
- Hassan, N. A., & Hijazi, R. (2018). *Open source intelligence methods and tools*. Apress.
- Hekim, H., & Başbüyük, O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, 4(2), 135–158.
- Holat, O. (2021). Yeni medya ve siber savaş kavramları bağlamında Stuxnet saldırısı örneğinin incelenmesi. *Abant Kültürel Araştırmalar Dergisi*, 6(11), 105–121.
- Hoopes, J. W. (2009). *Virtualization for security*. Syngress.
- Hoskins, A., & O'Loughlin, B. (2010). *War and media: The emergence of diffused war*. Polity Press.
- Hügül, H. (2011). *Algı yönetimi ve medya: İnegöl olaylarının basında sunulmasının algı yönetimi kapsamında analiz edilmesi* [Yayımlanmamış yüksek lisans tezi]. Kara Harp Okulu Savunma Bilimleri Enstitüsü.
- Ireton, C., & Posetti, J. (2018). *Journalism, fake news & disinformation: Handbook for journalism education and training*. UNESCO Publishing.
- Işık, T. (2022). 21. Yüzyılda dijital iletişim ve etik: Facebook ve YouTube örnek vaka incelemesi. *Global Media Journal: Turkish Edition*, 12(24).
- İçişleri Bakanlığı Kamu Düzeni ve Güvenliği Müsteşarlığı. (2017). *Güvenlik terimleri sözlüğü* (2. Baskı). http://metropolsavunma.com.tr/wp-content/uploads/2020/10/Guvenlik_Terimleri_Sozlugu_Mayis_2017_KD.pdf
- İhlas Haber Ajansı. (2026, Şubat 19). Zabıt katibi 'Casperlar'a bilgi sızdırmış! WhatsApp mesajları ortaya çıktı. *Türkiye Gazetesi*. <https://www.turkiyegazetesi.com.tr/gundem/zabıt-katibi-casperlara-bilgi-sizdirmis-whatsapp-mesajlari-ortaya-cikti-1771915>
- İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun, Kanun No. 7253, *Resmî Gazete* (Sayı: 31202). (2020, 31 Temmuz). <https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm>
- İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Kanun No. 5651, *Resmî Gazete* (Sayı: 26530). (2007, 23 Mayıs). <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&MevzuatTertip=5>
- İstanbul Büyükşehir Belediyesi. (2011). Meclis kararı (Karar No: 22527). <http://www.ibb.gov.tr/tr-TR/Pages/MecelisKarari.aspx?KararID=22527> Grok. (2026). *Grok*. <https://grok.com/>
- İstanbul Ticaret Üniversitesi Bilgi İşlem Daire Başkanlığı. (2025, 30 Ekim). Sosyal ağlarda güvenlik. <https://bim.ticaret.edu.tr/sosyal-aglarda-guvenlik/>
- Jabbari, N. (2025). Dil ve etnik grup temelli isim taşıyan ülkeler: Baskın ve azınlık gruplar arasında çatışma dinamikleri ve oranı üzerine bir analiz. *Ulusa: Uluslararası Çalışmalar Dergisi*, 9(2), 106-125.
- Jackson, R. (2007). Rejim güvenliği. A. Collins (Ed.) içinde, *Çağdaş güvenlik çalışmaları* (ss. 146–163). Uluslararası İlişkiler Kütüphanesi.

- Job, B. (1992). *The insecurity dilemma: National, regime, and state securities in the Third World*. Cambridge University Press.
- Kaminska, I. (2017). *A 123itera in fake news from the info-wars of ancient Rome*. Financial Times. <https://www.ft.com/content/aaf2bb08-dca2-11e6-86ac-f253db7791c6>
- Kandel, E. R. (2020). *The age of insight: The quest to understand the unconscious in art, mind, and brain*. Random House.
- Kapan, K., ve Üncel, R. (2020). Gelişen web teknolojilerinin (Web 1.0–Web 2.0–Web 3.0) Türkiye turizmine etkisi. *Safran Kültür ve Turizm Araştırmaları Dergisi*, 3(3), 276–289. <https://dergipark.org.tr/tr/download/article-file/1164473>
- Kaplan, A. M. & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, 53(1), 59–68.
- Kara, B., ve Çamur, Ö. (2024). Kamu güvenliği: Kalabalık yönetimi açısından bir değerlendirme. *Cihanşümül Akademi Sosyal Bilimler Dergisi*, 219–235. <https://dergipark.org.tr/en/download/article-file/4326887>
- Kara, M. (2024). Suç örgütlerinin sosyal medyayı bir özendirme aracı olarak kullanması: Basına yansıyan haberler eşliğinde bir inceleme. *Yeni Medya Elektronik Dergisi*, 8(3), 510–536. https://doi.org/10.17932/IAU.EJNM.25480200.2024/ejnm_v8i3005
- Kara, M., ve Çelikkol, S. (2011). Kritik altyapılar: Elektrik üretim ve dağıtım sistemleri SCADA güvenliği. *Atılım Üniversitesi 4. Ağ ve Bilgi Güvenliği*
- Karakaş, C. K. (2017). DAES propagandasında yeni medya kullanımı. *Marmara İletişim Dergisi*, 28, 33–46.
- Karlova, N. A., & Fisher, K. E. (2012). Plz RT: A social diffusion model of misinformation and disinformation for understanding human information behaviour. *Proceedings of ISIC 2012*. https://www.academia.edu/1981610/Plz_RT_A_social_diffusion_model_of_misinformation_and_disinformation_for_understanding_human_information_behaviour
- Kartal, A. B. (2018). Uluslararası terörizmin değişen yapısı ve terör örgütlerinin sosyal medyayı kullanması: Suriye’de DAES ve YPG örneği. *Güvenlik Stratejileri*, 14(27), 39–77. <https://dergipark.org.tr>
- Kaya, S. (2022). Sosyal medyada bireysel güvenlik tehditleri: Siber zorbalık ve kişisel veri ihlalleri. *Karadeniz Sosyal Bilimler Dergisi*, *cilt*, 112–130.
- Kazu, E. (2018). *Algı yönetimi perspektifinden siyasal iletişim ve lider ilişkisi: Turgut Özal dönemi analizi (1983-1989)* (Yayımlanmamış yüksek lisans tezi). İstanbul Ticaret Üniversitesi.
- Kelly, J. L., & Rizvi, S. (2015). The continued relevance of the November 2008 Mumbai terrorist attack: Countering new tactics with old lessons. *Homeland Security Affairs*, 11, 1–9.
- Kılınç, E. (2025). *Sosyal medya istihbaratı ve psikolojik savaş: Terör örgütlerinin psikolojik manipülasyon stratejileri* [Yüksek lisans tezi, Selçuk Üniversitesi].

- Kıran, S., Küçükboşancı, H., ve Emre, İ. E. (2020). Sosyal medya kullanımının kişiler üzerindeki etkilerinin incelenmesi. *Bilişim Teknolojileri Dergisi*, 13(4), 435–441. <https://doi.org/10.17671/gazibtd.693331>
- Kırık, A. M. (2012). Arap Baharı bağlamında sosyal medya-birey etkileşimi ve toplumsal dönüşüm. *21. Yüzyılda Eğitim ve Toplum*, 1(3), 87–98.
- Kızılyel, S. (2014). *Temel hak ve özgürlüklerin kısıtlanmasında kamu güvenliği ölçütü* (Doktora tezi, Polis Akademisi).
- Kietzmann, J., Hermkens, K., McCarthy, I., & Silvestre, B. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, 54(3), 241–251.
- Kim, Y., Sohn, D., & Choi, S. M. (2011). Cultural difference in motivations for using social network sites: A comparative study of American and Korean college students. *Computers in Human Behavior*, 27(1), 365–372. <https://doi.org/10.1016/j.chb.2010.08.015>
- Koblentz, G. D. (2013). Regime security: A new theory for understanding the proliferation of chemical and biological weapons. *Contemporary Security Policy*, 34(3), 501–525.
- Korkmaz, F. (2020). Dolandırıcılık suçunun bilişim sistemlerinin araç olarak kullanılması suretiyle işlenmesi. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 1(3), 1415–1436.
- Koşar, Y. (2024). *Rusya'nın Ukrayna politikalarının jeopolitik teoriler çerçevesinde incelenmesi: Vladimir Putin dönemi* (Yüksek lisans tezi, Necmettin Erbakan Üniversitesi).
- Koyuncu, S. (2022). ABD Kongre Binası baskınının Türk yazılı basınında sunumu: Göstergebilimsel bir analiz. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi*, 24(1), 146–168. <https://doi.org/10.32709/akusosbil.881347>
- Köse, T. (2024). Radikalleşme. TÜBİTAK Ansiklopedisi. <https://ansiklopedi.tubitak.gov.tr/ansiklopedi/radikallesme>
- Kurnaz, A., Kayar, İ., Güngör, M., ve Görün, M. (2019). Ulusal güvenlik ve sosyal medya: Fırsatlar ve tehditler. *Management and Political Sciences Review*, *cilt*, 75–96. <https://izlik.org/JA69BL87UZ>
- Kutup, N. (2010). İnternet ve sanat, yeni medya ve net.art. *XII. Akademik Bilişim Konferansı Bildirileri* içinde (ss. 9–15). Muğla Üniversitesi.
- Kuyucu, M. (2023, 19 Ekim). *YouTuber ekonomisi: Dijital ekonominin yıldızı parlayan video platformu YouTube'un geliştirdiği iş modelinin içerik üreticilerine sağladığı ekonomik avantajlar* [Bildiri sunumu]. 9. Uluslararası Ekonomi Yönetimi ve Pazar Araştırmaları Kongresi, İstanbul, Türkiye. <https://www.researchgate.net/publication/384665284>
- Kültür ve Yaşam. (2025, Kasım). *Türkiye'de sosyal medyanın gelişimi ve ilk yerli platform: Next Sosyal*. <https://kulturveyasam.com/turkiyede-sosyal-medyanin-gelisimi-ve-ilk-yerli-platform-next-sosyal/>

- Kürkçü, S., ve Erendor, M. E. (2022). İnternet ve sosyal medyada terör eylemleri: PKK örneği. *Terörizm ve Radikalleşme Araştırmaları Dergisi*, 1(2), 367–396.
- Larson, E. V., Darilek, R. E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, H. L., & Thurston, C. Q. (2009). *Foundations of effective influence operations*. RAND Corporation.
- Latorre, M. (2021). Web 1.0, 2.0, 3.0 ve 4.0'ın tarihi (Ö. Yılmaz, Çev.). *Maltepe Üniversitesi İletişim Fakültesi Dergisi*, 8(2), 344–350. (Orijinal çalışma basım tarihi 2018). <https://dergipark.org.tr/tr/download/article-file/2122736>
- Lemco, C. (1991). *Political stability in federal governments*. Praeger.
- Libman, A. (2022). The future of the global economy after the war in Ukraine. *Horizons: Journal of International Relations and Sustainable*, 21, 148–159.
- Lister, M., Dovey, J., Giddings, S., Grant, I., & Kelly, K. (2009). *New media: A critical introduction* (2nd ed.). Routledge.
- Lutkevich, B., & Scarpati, J. (2022, 11 Ocak). Instant messaging. *TechTarget*. <https://www.techtarget.com/searchunifiedcommunications/definition/instant-messaging>
- Manovich, L. (2003). New media from Borges to HTML. In N. Wardrip-Fruin & N. Montfort (Eds.), *The new media reader* (pp. 13–25). MIT Press.
- Marchant, E., Karatnycky, A., Puddington, A., & Walter, C. (2008). *Enabling environments for civic movements and the 125iteratü of democratic transition*. Freedom House.
- Margetts, H. (2019). Rethinking democracy with social media. *The Political Quarterly*, 90(S1), 107–123. <https://doi.org/10.1111/1467-923X.12574>
- Marshall, G. (2005). *Sosyoloji sözlüğü* (O. Akınhay ve D. Kömürçü, Çev.). Bilim ve Sanat Yayınları.
- Marwick, A., & Lewis, R. (2017). *Media manipulation and disinformation online*. Data & Society Research Institute. <https://datasociety.net/library/media-manipulation-and-disinfo-online>
- Mayfield, A. (2008). *What is social media?* iCrossing. https://crmexchange.com/uploadedFiles/White_Papers/PDF/What_is_Social_Media_iCrossing_ebook.pdf
- McIntyre, L. (2018). *Post-truth*. MIT Press.
- McLoughlin, C., & Lee, M. J. W. (2007). Social software and participatory learning: Pedagogical choices with technology affordances in the Web 2.0 era. In R. Atkinson, C. McBeath, S.-K. A. Soong, & C. Cheers (Eds.), *ICT: Providing choices for learners and learning* (pp. 664–675). Centre for Educational Development, Nanyang Technological University.
- Milliyetçi Hareket Partisi. (2025). @milliyetcihareketpartisi – Resmî YouTube Kanalı [YouTube kanalı]. YouTube. <https://www.youtube.com/@milliyetcihareketpartisi>
- Moralı, G. (2018). Yabancı dil olarak Türkçe öğretiminde blogların kullanımına yönelik kuramsal bir çalışma. *Turkophone*, 5(1), 42–44. <https://dergipark.org.tr>

- Neuringer, J. (2019). The use of special operations forces to counter terrorist networks in the megacity and urban environment. *Special Operations Journal*, 5(2), 127–142.
- Nguyen, R. (2013). Navigating jus ad bellum in the age of cyber warfare. *California Law Review*, 101(4), 1079–1129.
- Nuran, M. B. (2015). *Geleneksel medya ve yeni medya etkileşiminin Gezi Parkı gösterileri bağlamında incelenmesi* [Yayımlanmamış yüksek lisans tezi]. Beykent Üniversitesi Sosyal Bilimler Enstitüsü.
- Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, 27(6), 801–823.
- Oymak, H. (2022). Kamuoyunda dezenformasyon yasası olarak bilinen, 7418 sayılı “Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun”un getirdikleri. *Yeni Medya*, 2022(13), 504–514. <https://izlik.org/JA45ZZ63KL>
- Ölçekçi, H. (2018). Vekâlet savaşlarının bir aracı olarak medya ve 15 Temmuz sürecinde FETÖ’nün medya faaliyetleri. *Uluslararası 15 Temmuz ve Darbeler Sempozyumu Tebliğler Kitabı*.
- Özarslan, M. Z. (2014). *Kitleleri harekete geçirme aracı olarak sosyal algı yönetimi* (Yüksek lisans tezi). İstanbul Ticaret Üniversitesi.
- Özçağlayan, M. (2014). Gazetelerin gelişimi ve gazeteciliğin geleceği (Yeni teknolojiler ve medya ekonomisi açısından genel bir değerlendirme). *Marmara İletişim Dergisi*, (13), 131–141.
- Özdağ, Ü. (2008). *Algı yönetimi: Propaganda, psikolojik savaş, örtülü operasyon ve enformasyon savaşı*. Kripto Kitaplar.
- Özden, A. T. (2022). 1.0’dan 5.0’a dünya: Web, pazarlama, endüstri ve toplum. *Journal of Business in The Digital Age*, 5(1), 29–44. <https://doi.org/10.46238/jobda.1003371>
- Özkaya, E. (2017). The use of social media for terrorism. *NATO Defence Against Terrorism Review*, 9, 47–59.
- Öztekin, A. (2015). Devletin asli ve sürekli görevleri (temel kamu hizmetleri) ve özellikleri. *Akdeniz İ.İ.B.F. Dergisi*, *cilt*, [sayfa aralığı]. <https://dergipark.org.tr/en/download/article-file/372899>
- Polat, H., ve Öcal, D. (2020). Çoklu medyada ayak izlerini sürmek: Büyük veri ve yönetimi. *Dijital reklamcılık içinde* (ss. 99–130). [Yayınevi eklenmelidir].
- Reichborn-Kjennerud, E., & Cullen, P. (2016). *What is hybrid warfare?* Norwegian Institute of International Affairs. <https://nva.sikt.no/registration/0198cc7d0bf6-4f24ef7c-9045-401d-87de-46da2f39e4da>
- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
- Roscini, M. (2014). *Cyber operations and the use of force in international law*. Oxford University Press.
- Sabah. (2025, 5 Kasım). *YouTube ne zaman kuruldu, Türkiye’ye ne zaman geldi ve hangi yıl çıktı?* <https://www.sabah.com.tr/kesfet/youtube-ne-zaman-kuruldu-youtube-turkiyeye-ne-zaman-geldi-ve-hangi-yil-cikti-tk1-6337827>

- Safranchuk, I. (2022). The conflict in Ukraine: Regional and global contexts. *Policy Perspectives*, 19(1), 11–24. <https://doi.org>
- Saka, E. (2017). Türkiye’de internet. K. Alemdar (Ed.), *Türkiye’de kitle iletişimi: Dün-bugün-yarın içinde* (ss. 958–981). Gazeteciler Cemiyeti.
- Sardini, N. H. (2018). Digital democracy and democracy in Indonesia: Opportunities and challenges. In UNESCO (Ed.), *Countering online hate speech* (pp. 7–8). <https://unesdoc.unesco.org/ark:/48223/pf0000233231>
- Sarioğlu, E. B. (2020). Sosyal medyada adalet kavramı: Kadına ve çocuğa yönelik şiddetin sosyal medyadaki yansımaları. *Karadeniz Uluslararası Bilimsel Dergi*, 45, 291–317. <https://doi.org/10.17498/kdeniz.664868>
- Sayar, K. (2021, Ağustos). *Felaket kaydırması (doomscrolling) nedir? Nasıl durdurabiliriz?* <https://kemalsayar.com/haftanin-yazisi/felaket-kaydirmasi-doomscrolling-nedir-nasil-durdurabiliriz>
- Schreier, F. (2015). *On cyberwarfare*. DCAF.
- Scott, D. M. (2008). *The new rules of marketing & PR: How to use social media, blogs, news releases, and podcasts to reach your buyers directly*. Wiley.
- Seçkin, O. (2001). *Devlet güvenliği ve haber alma*. Polis Akademisi Başkanlığı Yayınları.
- Sezgin, A. A. (2017). Çevrimiçi gazetelerin okur yorumlarında nefret söylemi: Reina saldırısı örneği. *AJIT-e: Academic Journal of Information Technology*, 8(30), 107–130.
- Shipley, T. G., & Bowker, A. (2014). Investigating social networking sites. In *Investigating internet crimes* (pp. 315–344). Elsevier.
- Silva, L., Mondal, M., Correa, D., Benevenuto, F., & Weber, I. (2016). Analyzing the targets of hate in online social media. In *Proceedings of the International AAAI Conference on Web and Social Media* (Vol. 10, No. 1, pp. 687–690).
- Statista. (2025, 5 Şubat). *Most popular social networks worldwide as of February 2025, by number of monthly active users* [Grafik]. <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>
- Suleyev, S. (2019). *Medya ve terör ilişkisi bağlamında medyada terörizm propagandası* [Yüksek lisans tezi, İstanbul Üniversitesi]. İstanbul Üniversitesi Akademik Arşiv. <https://nek.istanbul.edu.tr/ekos/TEZ/ET001532.pdf>
- Sütçü, C. (2022). Dijital çağda savaş ve propaganda: Ukrayna-Rusya örneği. *Uluslararası İletişim ve Medya Çalışmaları Dergisi*, 7(2), 45–60.
- Şahin, M. (2011). 1950-1960 Arap devrimleri ve 2011 Arap Baharı benzerlikler ve farklılıklar. *Mülkiye Dergisi*, 35, [sayfa aralığı].
- T.C. İletişim Başkanlığı Dezenformasyonla Mücadele Merkezi. (2025). “15 Temmuz Şehitler Köprüsü, Fatih Sultan Mehmet Köprüsü ve ülke genelinde otoyollar satılıyor” iddiası. <https://dbs.iletisim.gov.tr/hakikat/1457>
- T24. (2011, 9 Ağustos). *İngiltere’de isyan yağmaya dönüştü!* <https://t24.com.tr/haber/ingilterede-isyan-yagmaya-donustu,161322>

- Tamir, A. (2018). Sosyal medyanın gücü: Londra isyanları. *Yeni Medya*, 4, 1–16. <https://izlik.org/JA28HB62TT>
- Tarhan, N. (2018). *Değerler psikolojisi ve insan* (12. Baskı). Timaş Yayınları.
- Taşdemir, E. (2025). Sosyal medyada terör propagandası: DEAŞ örneği. *Uluslararası Güvenlik ve Terörizm Dergisi*, 5(1), 735–750. <https://doi.org>
- Teknoblog. (2020, 10 Mayıs). *Facebook yeni masaüstü web sitesi görünümü* [Ekran görüntüsü]. <https://www.teknoblog.com/facebook-yeni-masaustu-web-sitesini-simdi-deneyebilirsiniz/>
- Temelli, V. K. (2023). *Sosyal medya istihbaratında büyük verinin yeri ve önemi* [Yüksek lisans tezi, Jandarma ve Sahil Güvenlik Akademisi].
- Terörle Mücadele Kanunu*, No. 3713 (1991). *T.C. Resmî Gazete*, (20843 Mükerrer), 12 Nisan 1991. <https://mevzuat.gov.tr>
- Tirab, T. A. (2017). Küreselleşme çağında ulusal güvenlik perspektifinden medya-güvenlik ilişkisi ve topluma yansımaları. *Güvenlik Stratejileri Dergisi*, 13(24), 113–151. <https://doi.org/10.17752/guvenlikstrti.356952>
- Toker, Y., ve Dilmaç, S. (1992). *Psikolojik harekât ve propaganda*. Emniyet Genel Müdürlüğü İstihbarat Daire Başkanlığı Yayınları.
- Toruk, İ., ve Sine, R. (2016). Sosyal medyanın toplumsal etkileri bağlamında “Black Mirror” dizisinin alımlanması. *Selçuk Üniversitesi Türkiyat Araştırmaları Dergisi*, (37), 457–481.
- Tosun, L. P. (2019). Sosyal ağ sitelerinin kullanımı ve öznel iyi oluş. *Psikiyatride Güncel Yaklaşımlar*, 11(3), 304–317. <https://doi.org/10.18863/pgy.444304>
- Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., & Nyhan, B. (2018). *Social media, political polarization, and political disinformation: A review of the scientific literature*. William and Flora Hewlett Foundation. <https://doi.org>
- Tunç, A., ve Atılğan, A. (2017). Algı üzerine kurulu yönetsel bir anlayış: Algı’nın yönetimi. *International Journal of Disciplines Economics & Administrative Sciences Studies*, 3(3), 228–238.
- Tunçay, E., Bağcan, S., ve Savaş, S. (2023). Lider ve fanatizm açısından Amerika Birleşik Devletleri Kongre baskını sürecinde Donald Trump’ın tweetlerinin incelenmesi. *Journal of History School*, (LXV), 1724–1761. <https://doi.org>
- Tümerkan, S. (1987). *Dolandırıcılık suçu*. Kazancı Kitap Ticaret.
- Türk Dil Kurumu. (2026). Güncel Türkçe sözlük. <https://sozluk.gov.tr/>
- Türk, G. (2013). Sosyal medyanın gücü: Londra isyanları. *Yeni Medya*, (1), 114–130.
- Türk, G. D. (2013). Demokrasinin dördüncü kuvveti yeni medya teknolojileri. *XVIII. Türkiye’de İnternet Konferansı, İNETD* içinde (ss. 55–60).
- Türkdoğan, O. (2013). *Sosyal hareketlerin sosyolojisi*. Bilge Kültür Sanat.
- Türkiye Barolar Birliği. (2014). *Gezi Parkı olayları raporu*. <https://barobirlik.org.tr>

- Tüysüzoğlu, G. (2012). Myanmar: Bir “başarısız devlet” örneği mi?. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi*, 14(1), 1–22.
- Tzu, S. (2022). *Savaş sanatı* (P. Otkan ve G. Fidan, Çev.). Türkiye İş Bankası Kültür Yayınları.
- U.S. Department of Defense. (2010). Perception management. *Dictionary of military and associated terms* içinde. https://www.militaryfactory.com/dictionary/military-terms-defined.php?term_id=4039
- Uluç, G., ve Yarcı, A. (2017). Sosyal medya kültürü. *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, [cilt], 88–102.
- Ulukaya, C. (2020). *Sosyal medya yargılaması: Adaletin hem başladığı hem bittiği yer*. Journo. https://www.academia.edu/44027831/Sosyal_medya_yarg%C4%B1lamas%C4%B1_Adaletin_hem_bitti%C4%9Fi_hem_ba%C5%9Flad%C4%B1%C4%9F%C4%B1_yer
- Ulusal, D., ve Özdemir, H. B. (2024). Siyasal iletişim aracı olarak sosyal medya: “Haydi Türkiye” seçim videosu üzerine bir inceleme. *Uluslararası Kültürel ve Sosyal Araştırmalar Dergisi*, 10(2), 35–48. <https://doi.org/10.46442/intjcss.1580555>
- University of Plymouth. (t.y.). *What is energy security?* <https://www.plymouth.ac.uk/discover/what-is-energy-security>
- Utma, S. (2018). Dijital çağda medyanın psikolojik gücü: Algı yönetimi perspektifinden kuramsal bir değerlendirme. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 22(Özel Sayı 3), 2903–2913.
- Ünal, R., ve Taylan, A. (2017). Sağlık iletişimde yalan haber yanlış enformasyon sorunu ve doğrulama platformları. *Atatürk İletişim Dergisi*, (14), 81–100.
- Van Dijk, J. (2006). *The network society* (2nd ed.). Sage Publications.
- Vegasis Medya. (2025, Mart). *Türkiye’nin yerli sosyal medya yolculuğu: Kendi dijital dünyanı inşa et!* <https://vegasismedya.com/turkiyenin-yerli-sosyal-medya-yolculugu/>
- Vergi Usul Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, Kanun No. 7338, Resmi Gazete (Sayı: 31640). (2021, 26 Ekim). <https://resmigazete.gov.tr>
- Wardle, C., ve Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making* (Report No. DGI(2017)09). Council of Europe.
- Weimann, G. (2014). *New terrorism and new media* (Vol. 2). Commons Lab of the Woodrow Wilson International Center for Scholars. <https://www.wilsoncenter.org/publication/new-terrorism-and-new-media>
- Wood, P., Nahorney, B., Chandrasekar, K., Wallace, S., & Haley, K. (2016). *Internet security threat report* (Vol. 21). Symantec.
- World Health Organization. (2020). *An ad hoc WHO technical consultation managing the COVID-19 infodemic: Call for action, 7-8 April 2020*. <https://who.int>

- Yağmurlu Dara, A. (2013). Kamu yönetiminde halkla ilişkiler ve sosyal medya. *Selçuk İletişim*, 7(1), 5–15.
- Yakın, M. (2004). *Reklamda algı yönetimi* (Yüksek lisans tezi, Ege Üniversitesi Sosyal Bilimler Enstitüsü).
- Yalınız, M. O. (2025). Dijital otoriterlik ve yeni medya: Azerbaycan, Çin ve Rusya örneğinde sansür politikaları ve internet özgürlüğü. *R&S: Research Studies Anatolia Journal*, 8(3), 426–454.
- Yayla, A. (2014). *Karşılaştırmalı siyasal sistemler*. Adres Yayınları.
- Yayla, A. (2020). Totaliterizm ve dezenformasyon. *Liberal Düşünce Dergisi*, 25(98), 125–146. <https://doi.org/10.36484/liberal.756869>
- Yegen, C. (2013). Demokratik ve yeni bir kamusal alan olarak sosyal medya. *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi*, 1(2), 119–135.
- Yenal, S. (2020). *Strateji ve güvenlik alanında temel ve güncel yaklaşımlar*. Nobel Akademik Yayıncılık.
- Yeni Asya. (2018, 3 Kasım). Trump'ın "yaptırım" paylaşımına cevap Kasım Süleymani'den geldi. https://www.yeniasya.com.tr/dunya/trump-in-yaptirim-paylasimina-cevap-kasim-suleymani-den-geldi_477335
- Yeni Şafak. (2013, 2 Haziran). Başbakan Erdoğan'dan sosyal medya eleştirisi! <https://www.yenisafak.com/gundem/basbakan-erdogandan-sosyal-medya-elestirisi-528936>
- Yeniçifti, N. T. (2014). İletişimsel eylem ve Facebook: Gezi Parkı olaylarında sosyal medyanın gücü. *Selçuk İletişim*, 8(2), 263–284.
- Yılmaz, S. (2008). *Akıllı güç*. Kum Saati Yayınları.
- Yılmaz, S. (2018). *Temel istihbarat*. Kripto Yayınları.
- Yılmaz, S., ve Salcan, O. (2008). *Siber uzayda güvenlik ve Türkiye*. Milenyum Yayınları.
- Zengin, Ü. N., Biçen Gören, K. B., ve Beşgül, B. (2023). *Medya ve güvenlik raporu*. Polis Akademisi Yayınları. <https://cdn2.pa.edu.tr/Upload/Rapor/Dosya/medya-ve-guvenlik-raporu.pdf>
- Zhao, H., Wang, Y., & Zhao, Y. (2021). Comparison between social media and social networks in marketing research: A bibliometric view. *Nankai Business Review International*, 12(4), 531–561. <https://doi.org/10.1108/NBRI-01-2021-0005>