Sosyal Medyada Etik, Bilgi Manipülasyonu ve Siber Güvenlik

Ethics, Information Manipulation and Cyber Security in Social Media

Aynur TEKKE

Yüksek Lisans, Kırıkkale Üniversitesi,
Sosyoloji Anabilim Dalı
aynurtekke61@gmail.com
https://orcid.org/0000-0002-5280-3169

Aybala LALE

Arş. Gör. Ankara Hacı Bayram Veli Üniversitesi,
Uluslararası İlişkiler Bölümü.
lalea933@gmail.com
https://orcid.org/0000-0003-3289-5403

Araştırma & Yayın Etiği

Bu makale en az iki hakem tarafından incelenmiş, iThenticate yazılımı ile taranmış, araştırma yayın ve etiğine aykırılık tespit edilmemiştir.

Research & Publication Ethics

This article was reviewed by at least two referees, a similarity report was obtained using iThenticate, and compliance with research/publication ethics was confirmed.

Atıf/Citation

Tekke, Aynur - Lale, Aybala . "Sosyal Medyada Etik, Bilgi Manipülasyonu ve Siber Güvenlik". Akademik İncelemeler Dergisi 16 / 2 (Ekim 2021): 44-62.
https://doi.org/10.17550/akademikincelemeler.958167

Makale Türü/Article Type: Araştırma Makalesi/Research Article
Geliş Tarihi/Date Received: 27.06.2021
Kabul Tarihi/Date Accepted: 24.09.2021
Yayın Tarihi/Date Published: 15.10.2021

ISSN: 1306-7885
E-ISSN: 2602-3016
Cilt/Volume: 16 | Sayı/Issue: 2 |
Yıl/Year: 2021 (Ekim/October

Akademik İncelemeler Dergisi

Sosyal Medyada Etik, Bilgi Manipülasyonu ve Siber Güvenlik

Öz

Bu çalışmanın amacı, kitle iletişim araçları ile sosyal medyada üretilen ve akışa dâhil edilen bilgileri dijital etik ve siber güvenlik stratejileri bağlamında analiz etmektir. Dijital etik ilkeleri, bireylerin yaşam mahremiyetini göz önünde bulunduran normları kapsamaktadır. Siber uzay, bilgisayar ve bilgisayar ağlarına ilişkin bir kavram olmanın yanı sıra insan eliyle üretilen faaliyetler bütününü de içerdiği için, siber uzayda manipülasyon teknikleri önemli bir siber tehdit olarak kullanıcıların karşısına çıkmaktadır. Siber tehditlerle mücadele etmek için ise dijital etik kurallarının geliştirilmesi önem arz etmektedir. Dijital etik kurallarının ihlal edilmesi sonucunda yanlış ve yalan bilginin oluşmasıyla birlikte bireylerin yanlış bilgilendirilmesi söz konusu olmaktadır. Çalışmada, öncelikle bireyleri "aynı olma" paydasında buluşturma amacı güden sosyal medya, Adorno ve Horkheimer'ın kültür endüstrisi kavramı kapsamında değerlendirilmiştir. Bu doğrultuda, manipülatif nitelik taşıyan içerikler, dijital etik ilkeleri bağlamında analiz edilmiştir. Daha sonra, genelde siber uzayda karşılaşılan sosyal medya tehditleri ve özelde ise bilgi manipülasyonu devletlerin uyguladığı siber güvenlik stratejileri bağlamında karşılaştırılmıştır. Netice olarak, bilginin dijital etik ilkelerinden uzaklaştıkça manipülatif niteliğinin arttığı görülmüştür. Bu nedenle siber uzayın tüm aktörlerinin siber etik kurallarının geliştirilmesi ve uygulanabilmesi için etkin olmaları gerektiği tespit edilmiştir.

Anahtar Kelimeler: Sosyal Medya, Siber Güvenlik, Siber Uzay, Dijital Etik, Bilgi Manipülasyonu

Ethics, Information Manipulation and Cyber Security in Social Media

Abstract

This study aims to analyze the information in social media which is produced and included in the stream by mass media in the context of digital ethics and cyber security. The principles of digital ethics include norms that consider individual privacy of life. In addition to being a concept related to cyberspace, computer, and computer networks, it also includes whole human-made activities, for this reason, manipulation techniques in cyberspace appear as an important cyber threat to users. As it comes to the purpose of coping with cyber threats the development of digital etic rules is essential. As a result of the violation of digital etic rules, wrong and false information is formed and individuals are misinformed. In the study, social media, which aims to bring individuals together on the basis of "being the same", has been evaluated within the scope of the culture industry concept of Adorno and Horkheimer. In this direction, content with a manipulative nature has been analyzed in the context of digital ethical principles. Then, social media threats encountered in cyberspace in general and information manipulation, in particular, are compared in the context of cybersecurity strategies implemented by states. As a result, it has been seen that the manipulative nature of information increases as it moves away from the principles of digital ethics. For this reason, it has been determined that all actors of cyberspace must be active to develop and apply cyber ethics rules.

Keywords: Social Media, Cyber Security, Cyberspace, Digital Ethics, Information Manipulation

Giriş

Toplumsal ve kültürel ölçekte ilişkilerin değişimi ve dönüşümü olarak ifade edilebilen küreselleşme olgusu, toplum ve birey özelinde farklı etkilere yol açmaktadır. Etkilerin, gündelik yaşamda farklı olgular bağlamında görünür hale geldiği bilinmektedir. Bu noktada kitle iletişim araçları, küreselleşmenin getirilerinin pekiştiricisi olarak karşımıza çıkmaktadır. Küreselleşmeyle başlayan toplumları ortak bir paydada toplama, bütün toplumları ve bireyleri tek bir perspektiften değerlendiren aynılaştırma süreci, kitle iletişim araçlarıyla sürdürülmektedir. Dolayısıyla kitle iletişim araçlarının içeriğini oluşturan bilgi akışı sayesinde küreselleşme amaçlarına ulaşabilmektedir. Benzerlik anlayışıyla hareket eden sosyal medyanın, kitle iletişim araçlarının üstlendiği rolü devam ettirdiğini söylemek mümkündür. Kitle iletişim araçları ve sosyal medya, bilginin üretilmesi, aktarılması ve yayılması süreçlerinde ortak bir şekilde hareket etmekte ve böylece etkileme güçlerini pekiştirdikleri görülmektedir.

Kitle iletişim araçlarıyla üretilen ve sosyal medya aracılığıyla yayılma süreci hızlandırılan içerikler, zamanla gerçekliğin önüne geçmektedir. Bu durum, beraberinde uyulması gereken dijital etik ilkelerini ihmal etmeyi getirmektedir. Bireyler ve toplumlar arasındaki sınırların ortadan kaldırıldığı, bireylerin benzerlik, bir arada olma, aynı olma paydasında buluştuğu sosyal medyada bireysel ve toplumsal mahremiyet kalmamakta, gizli kalma durumu söz konusu olmamaktadır. Kaynağın gerçek olgu ve olaylara dayandırılmaması gibi durumlarda içeriklerin yalan, yanlış, aldatıcı ve manipüle edici niteliklere sahip olması da görülen sonuçlar arasında yer almaktadır. Doğru veya yanlış nitelik taşıyan bilgi akışının çevrim içi platformlarda yer alması ve yine bu platformlar aracılığıyla paylaşılması, iletilmesi aynı zamanda saklanması eylemlerini kapsayan siber uzay, bireylerin yaşantısını şekillendiren bir kavramdır. Bu şekillendirici kavramın beraberinde getirdiği tehdit ve riskler gerek küresel gerek yerel ölçekte farklı önlemler almayı gerektirmektedir. Farklı önlemlerin kapsayıcısı ise siber güvenlik stratejileri olmaktadır. Dijital etik ilkelerini dikkate alarak hazırlanan siber güvenlik stratejilerinin önceliği, bilgi ve bilginin üretim, korunma, saklanma ve dağıtılma süreçleridir. Akış içinde bireylerin maruz kaldığı yanlış bilgi, yalan bilgi ve yanlış bilgilendirme süreçlerinden korunmaları için siber güvenlik stratejileri büyük önem taşımaktadır. COVID-19 ile başlayan pandemi sürecinde de yine sosyal medya içinde görünür hale gelen yanlış ve yalan nitelikler taşıyan asılsız, manipüle edici içerikler de bu noktada vurgulanması gerekmektedir. Dünya Sağlık Örgütü ("Munich Security Conference" (2020)) tarafından infodemi kapsamında değerlendirilen bu süreçteki içerikler, bilginin kitle iletişim araçları ve sosyal medyayla birlikte işlenmesi sonucunda manipüle edici bir özellik taşıdığını açıklar niteliktedir (WHO, 13 Eylül 2021).

Bu çalışma, kitle iletişim araçlarını ve siber uzay kapsamında yer alan sosyal medyayı, manipülatif içerikler ve dijital etik ilkeleri bağlamında değerlendirmektedir. Aynı zamanda siber uzayda bulunan tehditlere karşı yürütülen siber güvenlik stratejilerini ABD, Çin ve Rusya ülkeleri özelinde detaylandırmak da yine çalışmanın amaçları arasında yer almaktadır. Bu amaç doğrultusunda, manipülatif nitelik taşıyan içerikler çalışmanın odak noktasında yer almaktadır. Bu değerlendirme, kitle iletişim araçlarıyla sosyal medyada bulunan yanlış ve aldatıcı içerik türleri ve onlara karşı yürütülen siber güvenlik

stratejileriyle sınırlıdır. Bu anlamda, manipülatif içerikler, dijital etik ilkeleri, siber uzay tehditleri ve ülkelerin siber güvenlik stratejileri karşılaştırmalı bir yaklaşımla ele alınmaktadır.

1.Manipülatif Kitle İletişim Araçları

Toplumsal bağlamda ele alındığında küreselleşme, temelde iki olguyla ilişkili olarak değerlendirilmektedir. Olgulardan ilki ekonomi, diğeri ise sosyal ve kültürel değişimdir. Bu iki olgu özelinde genel bir değerlendirme yapıldığında küreselleşme aracılığıyla toplumlar arasındaki etkileşimlere aracılık eden maddi unsurların yanında manevi unsurların da yer aldığı görülmektedir. Manevi unsur kapsamına giren bilgi ve kültür de etkileşimin odağında bulunmaktadır. Dolayısıyla toplumlar arasındaki etkileşimin artması bilgi ve kültür akışının da oluşmasını sağlamaktadır. Akışın ve değişimin sürdürülmesi hususunda büyük rol üstlenen kitle iletişim araçları, toplumların özel olarak ürettiği bilginin diğer toplumlara ulaştırılmasına aracılık ederek küreselleşmenin ilerleyişini şekillendirmektedir (Avcıoğlu, 2013, 22–23). Küreselleşmenin getirilerinden biri olan teknolojinin gelişmesiyle beraber, bireyler arasında iletişim kurulmasına aracılık eden araçlar da elektronik bir forma bürünmüştür. Sonuç olarak da iletişim hızlı ve kolay bir hal alırken, aynı zamanda kitleselleştiği de görülmektedir (Gönenç, 2014, 36). İletişimin değişen formu ve bu formun destekleyicisi olan araçlar, gündelik yaşamın pek çok noktasına temas etmekte, yaşamı değiştirip dönüştürmektedir.

Adorno ve Horkheimer, iletişim ile beraber oluşan kültürün, günümüz koşullarında bütün bireyleri, olguları ve olayları benzerlik paydasında buluşturduğunu ifade etmektedir. Genel görünüm itibariyle bakıldığında söz konusu yazarlar, bütün kültürlerin aslında aynı özelliklere sahip olduğunu, tek bir noktada ortaya çıkan ögelerin bütün toplumların yaşantısında kendisine bir yansıma bulabildiğini belirterek, bu durumu "kültür endüstrisi" kavramsallaştırmasıyla beraber açıklamaktadırlar. Yaşam içinde mevcut olan alanları, olguları ve olayları nesneleştirerek kitle bilinci paydasında yeniden düzenleyen kültür endüstrisi, bireysel ve toplumsal yaşam üzerinde şekillendirici bir etkiye sahiptir (Adorno ve Horkheimer, 2014, 162–163). Kültür endüstrisi, bireyler tarafından bilinen her şeye yeni bir form kazandırarak tüketime uygun bir hale getirmektedir. Tek bir noktada başlayan yeni form halleri zamanla kendine daha fazla alan bulmakta ve büyük bir sistem ağı oluşturmaktadır (Adorno, 2007, 109). Horkheimer ve Adorno'nun yaklaşımlarının temelinde yer alan belirli bir kültür algısının benzerlik odaklı olması ve bütün bireylere bu benzerliğin empoze edilmesi hali kitle iletişim araçları aracılığıyla sürdürülmektedir.

Kitle iletişim araçlarıyla başlayan benzer hale getirme eylemi, sosyal medya aracılığıyla sürdürülmektedir. Sosyal medyanın topluma karşı olan yaklaşımları da süreci şekillendirmektedir. Toplumların sahip olduğu özelliklerin, fark etmeksizin bütün toplum üyeleri nezdinde aynı şekilde var olduğu değerlendirilmektedir. Görsellikle beraber her bireyin aynı dile sahip olduğu algısının oluşmasına aracılık eden medya, paylaşımların da aynı doğrultuda olmasını sağlamaktadır (Öztürk, 2013, 238).

2.Sosyal Medya ve Dijital Etik İlkeleri

İletişim kurma eylemiyle birlikte şekillenen bireysel alışkanlıklar, medya araçlarının da form değiştirmesiyle beraber değişkenlik göstermekte ve çevrimiçi olarak kurulan iletişim önem kazanarak, her yerde görünür hale gelmektedir. Bu her yerde görünür olma halinin ve önem kazanmanın arka planına bakıldığında bireylere sunulan alternatiflerin çeşitli olması ana sebep olarak söylenebilmektedir. Çevrimiçi veya çevrimdışı iletişim

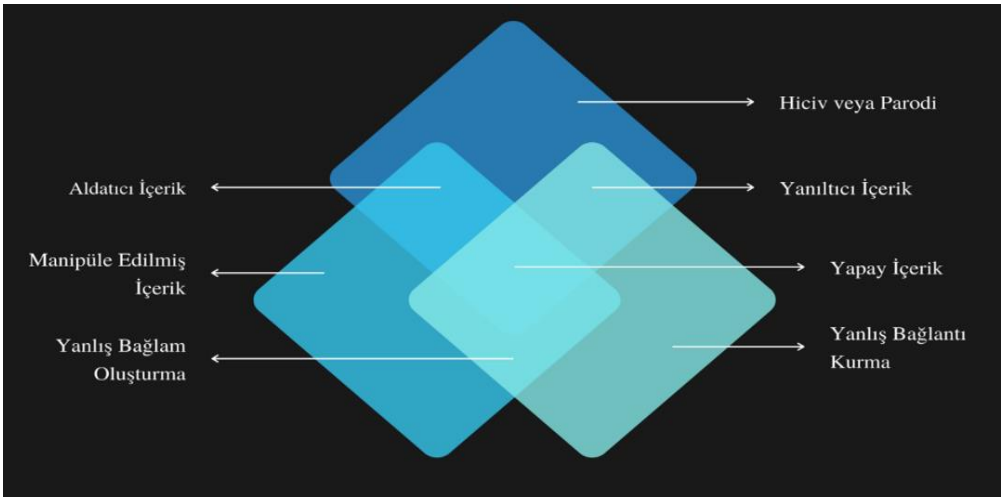
kurma, etkileşim halinde bulunma, sınırsız bir alanda bulunma gibi avantajlar sosyal medyanın sunduğu alternatifler arasında yer almaktadır (Tutgun Ünal, 2020, 1).

Sosyal medya içinde her birey, sınırsız bilgi akışının bir temsilcisi rolünü üstlenmektedir. Dolayısıyla, sosyal medyanın bireylerin düşüncelerini etkilediği ifade edilebilmektedir. Bireyler arasında görünür olan iletişim engellerinin ortadan kalkmasına yardımcı olan sosyal medya, kendi kabulleri çerçevesinde oluşturduğu, her bireyin eşit derecede söz hakkına sahip olduğu bir alan oluşturmaktadır. Bu alanda, kendiliğinden ortaya çıkan, resmî, gayrı resmî, bilimsel olan veya bilimsel olmayan içerikler bulunmaktadır. Fakat her ne kadar sosyal medyanın sunmakta olduğu avantajlar bireysel düzeyde çekici bir nitelik taşısa da olumsuz etkilerinin de vurgulanması gerekmektedir (Amedie, 2015, 3–4). Sosyal medya aracılığıyla oluşturulan etkileşimlerin bireylerin yaşamlarındaki gerçekliğin önüne geçmesi, Horkheimer ve Adorno tarafından kavramsal çerçevesi oluşturulan kültür endüstrisi ekseninde manipülatif kitle iletişim araçları bağlamında çözümlenmiştir. Bu perspektiften bakıldığında sosyal medyanın, bireyleri etkileme gücünü temsil eden manipülasyonun destekleyicisi rolü üstlendiği ve manipülasyona uygun bir ortam oluşturma görevini yerine getirdiği söylenebilmektedir.

Bilgiye erişimin kolaylaştığı bilgi çağındaki etik ilkeleri Mason (1986), dört temel kavram ile beraber çözümlemektedir. Bu kavramlar; gizlilik, doğruluk, erişilebilir olma ve fikri mülkiyettir. Çevrimiçi olarak edinilen bilgi içeriklerinin etik olarak sahip olması gereken ilkeleri analiz eden Mason, bilgi teknolojileri kapsamında ortaya konan bilgilerin, bireyler ve toplumların yararına oluşturulduğundan emin olmak için önemli olduğunu ifade etmektedir. Her bireyin, çevrimiçi platformlarda sahip olduğu potansiyeli ortaya koymak adına uyması gereken ilkeler olarak da bu dört temel kavram ifade edilebilmektedir. Gizlilik ilkesi, bireyin mahremiyeti olarak ifade edilebilecek bilgilerin saklanmasını kapsamaktadır. Doğruluk ilkesi, bilgi kirliliği, bilgi manipülasyonu olarak ifade edilebilecek yanlış bilgilerin önüne geçebilmek için gerçekleştirilmesi gereken stratejileri ifade etmektedir. Erişilebilir olma ilkesi, teknolojik imkanlar başta olmak üzere çevrimiçi platformlara erişim hakkının bütün bireyler arasında eşit olmasına dair belirlenen normları kapsamaktadır. Son olarak fikri mülkiyet ise, akışa dâhil olan bilgilerin ortaya çıkmasını sağlayan, aracılık eden bireylerin haklarını korumaktadır. Ozan Leymun'un (2020) belirttiği gibi Mason tarafından belirlenmiş olan dört ilke günümüzde de geçerli olarak kabul edilmekte ve uygulanmaktadır.

Sosyal medya platformları içinde bulunan yoğun bilgi akışının beraberinde gelen gerçek ve yalan dikotomisi bilgi kirliliği oluşturmaktadır. Wardle (2017), akış içinde yayılan içerik türlerinin doğruluk niteliği üzerinde bir sınıflandırma yapmıştır. Bu sınıflandırmaya göre genel görünüm olarak yanlış ve hatalı nitelendirmelerinin yapıldığı içerik türleri Şekil 1'de gösterildiği gibidir.

Şekil 1: Yanlış ve Hatalı Olarak Görülen İçerikler (1)



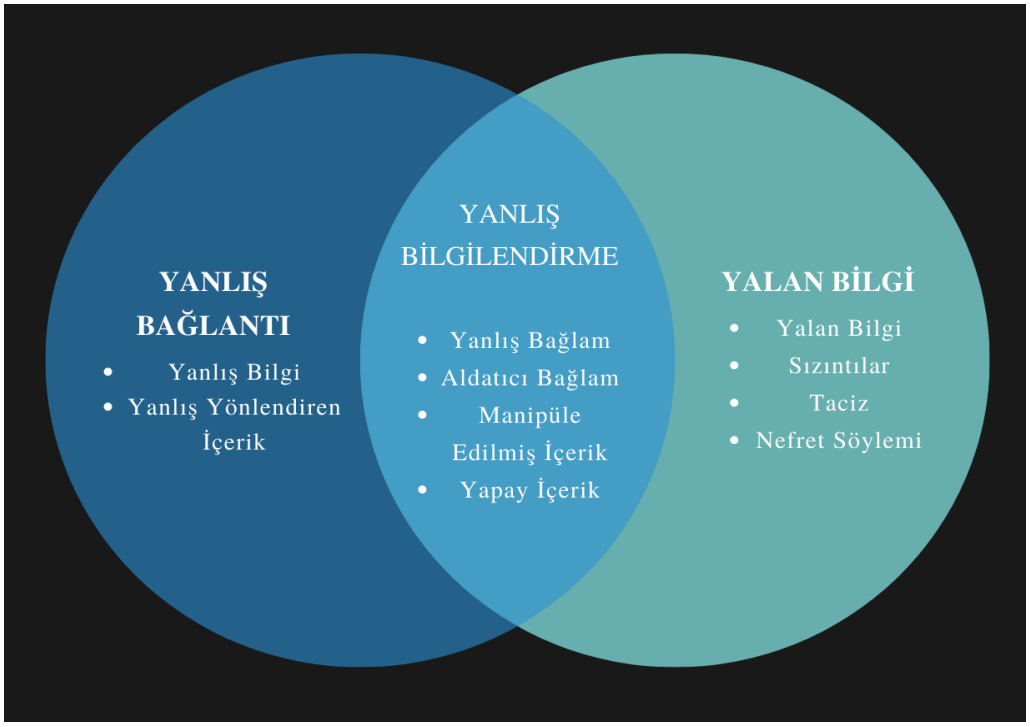
Kaynak: (Wardle, 2017)

"Hiciv veya parodi", zarar verme amacı taşımayan fakat aldatıcı niteliği bulunan içerikler bu türde yer almaktadır. "Yanıltıcı içerik ve aldatıcı içerik", bilginin odağında olan konunun, gerçek bilgilerin asılsız bir hale getirilmesi, başka bir ifadeyle çarpıtılmasıyla oluşturulmaktadır. "Yapay içerik", hiçbir şekilde gerçek bilgiye dayanmamakta, tamamen asılsız olarak kurgulanan içeriklerdir. "Manipüle edilmiş içerik", odak noktasına gerçek bilgiyi, konuyu, görüntüleri alarak üzerinde değişiklikler yapılmasını kapsamaktadır. "Yanlış bağlantı kurma ve yanlış bağlam oluşturma" ise, bilgileri aktarırken belirlenen başlıkların, bağlamların doğru olmayan şekillerde aktarılmasıyla oluşturulan içeriklerdir.

2.1.Sosyal Medya Aracılığıyla Yürütülen Manipülasyon

Gelişen ağı ve kullanıcı sayısıyla sosyal medya, çeşitli yönlendirmelere ve etkilemelere yani manipülasyon araçlarına sahiptir. Nitekim sosyal medya, milyarlarca bireyin fikirlerini sansürsüz paylaşmalarına imkân sağladığı için çeşitli siber güvenlik riskleri taşımayabilmektedir. Anonimliğin ve sahte kimliklerin var olabildiği bir platformda bu tehditler farklı şekillerde görünür hale gelebilmektedir. Görünür hale gelen tehditlerin yer aldığı ortak payda ise, yanlış ve yalan olgularıyla şekillendirilen manipülasyonlardır. Wardle ve Derakshan'ın (2017, 5) yanlış bilgi akışına ve bireyleri yönlendiren manipülasyon içeriklerine dair yapmış olduğu kategorileştirme (Şekil 2) bu noktada detaylı bilgi edinilmesini sağlamaktadır.

Şekil 2: Yanlış Bilgi Akışı Şeması (2)



Kaynak: (Wardle ve Derakshan, 2017)

Yanlış bağlantı/Misenformasyon (misinformation), doğru olmayan bilgi ve bireyleri manipüle edecek içerikleri kapsamaktadır. Yalan bilgi (malinformation), zarar verme amacı taşıyarak, bireylere ait olan mahremiyetin ve özel alanın yok sayıldığı, kamusal alanda görünür hale gelen ve dolaşıma dâhil edilen bilgi ve eylemleri içermektedir. İki kategorinin kesişim noktasında bulunan yanlış bilgilendirme (disinformation) ise, bağlamı doğru olmayan, aldatıcı bilgilerle donatılmış içeriklerle oluşturulmaktadır. COVID-19 sürecindeki yanlış bilgilendirmenin karşılığı ise infodemi kavramıyla ifade edilmektedir. Her ne kadar farklı şekillerde infodemi kavramının içeriği açıklanmaya çalışılsa da genel görünüm itibariyle yanlış olan bilginin dolaşıma girmesi, yayılması olarak açıklanması mümkündür (WHO, 13 Eylül 2021). Gölbaşı ve Metintaş'ın (2020, 127–128) belirttiği gibi teknolojik gelişmelerle beraber haber kaynağına ulaşmada, bilgi edinme süreçlerinde sosyal medya büyük önem taşımaktadır. Gerçeklik ve sosyal medyada kurulan ütopya arasında sağlanan bilgi akışı, bazı sonuçları da beraberinde getirmektedir.

Dünya Sağlık Örgütü (DSÖ) tarafından, COVID-19 salgın sürecinde asıl tehlikeli olanın "infodemi" olduğu belirtilmektedir. Bilginin aşırı bir boyuta ulaşması ve bu aşırılık içinde doğru, yanlış, iyi, kötü gibi nitelendirmelerin yapılmasının güç olması güvenilir kaynaklara ulaşma konusunda engel teşkil etmektedir. Şüpheli ve yanlış olarak nitelendirilebilecek bilgilerin, başka bir ifadeyle söylentilerin gündeme gelmesi çevrimiçi platformlar aracılığıyla hızla büyümekte, virüs gibi yayılım göstermektedir (Zarocostas, 2020, 636). Salgın sürecindeki öngörülemez artış, hızlı yayılma süreci beraberinde paralel bir ilerleyiş gösteren bilgi ve haber akışını da getirmiştir. Bu akış, bireyler açısından tehlikeli olmakta, manipülasyona, psikolojik olarak kötü etkilenmelere açık bir ortam hazırlanmasına yol açmaktadır (Sarıoğlu ve Turan, 2020, 823–824). İnfodemi kavramıyla özdeşleşmiş hale gelen sosyal medya, odak noktada yer alan bilginin

kaynağını oluşturmaktan ziyade yayılma sürecinin oluşması ve hızlanması sürecinde etkin rol üstlenmektedir.

2.2.Manipülasyonun Arka Planı: Senkronizasyon İstenci

Adorno ve Horkheimer'ın (2014), kültür endüstrisi olarak adlandırdıkları bireylere tek tip bir benzerliğin empoze edilme halinin Pettman odağındaki adlandırılması ise senkronizasyon istencidir. Pettman'ın kavramsallaştırması, sosyal medyada oluşturulan içeriklerden bireylerin uzak kalmak istememesi ve kendilerini sosyal medya akışı içine dâhil etmeleri sonucunda oluşmaktadır. Bireyler, ne kadar akış içinde olursa o kadar toplum tarafından kabul göreceği düşüncesiyle hareket etmektedir. Dolayısıyla bahsi geçen akış içeriğinin doğruluğu teyit edilmeksizin bireylerin hayatlarında görünür hale gelmesi mümkün olmaktadır.

Pettman, dijital tüketiciler olarak adlandırdığı sosyal medya kullanıcılarının, sosyal medyanın akışı içinde gezinirken popüler ve güncel olan olaylardan haberdar olabilmek için bir dijital sürü haline geldiğini hipermodülasyon kavramıyla belirtmektedir. Zamanla akış içinde yalnızca yanlış bilinçlenme sorunu var olmamakta aynı zamanda bireysel olarak bir sonsuz döngü içinde bölünme ve arzuların ortaya çıkması aracılığıyla bilincin fethedilmesi söz konusu olmaktadır. Dolayısıyla odağından çıkmış ve dikkati dağılmış bir bilinç sosyal medya tarafından kolay bir şekilde yönlendirilebilmektedir (Pettman, 2016, 29–30).

Sosyal medya ve çevrimiçi olarak kurgulanan alanların bireylerin yaşamını şekillendiren etkilerini ve bu etkiler sonucunda oluşan dikkat dağınıklığını farklı örnekler ekseninde çözümleyen Pettman, sosyal medyanın farklı dikkat sapmaları/dağınıklıkları bir araya getiren bir sapma/dağınıklık olduğunu ifade etmektedir. Sosyal medyanın üstlenmiş olduğu bu görevi ise meta-dikkat dağıtıcı olarak adlandırarak bireylerin yaşamının merkezine yerleşen oyalama eyleminin sonsuz bir döngü içine dâhil olma sürecini irdelemektedir. Dikkat dağınıklığının sonsuzluk ile nitelendirilmesinin arka planına ise birbirini takip eden, karşılıklı olarak etkileşim kuran süreçleri yerleştirmektedir. Sosyal medya içinde yer alan her eylemin birer adım olduğu düşünülürse her bir adımın sonucunda farklı bir adım atma gereksinimi bireyler tarafından hissedilmektedir. Bu da diyalektik niteliğe sahip bir üretim sürecini gerektirmektedir. Üretim sürecinin içine dâhil olan olgular, süreklilik arz eden bir davranış zincirinin halkası olmakta ve rolünü yerine getirmektedir. Sonu gelmeyen bir bağlılık zinciri, bireyleri oluşturduğu akışın içine dâhil etmekte ve bu duruma bireylerin kendini mecbur hissetmesini sağlamaktadır. Akış içindeyken gündemden haberdar olma, bilgi edinme, diğer bireylerle etkileşim halinde olma, beğenilme, merak edilme gibi eylemler akış içinde kalmanın mecburiyetini güdülemektedir.

Sosyal medyada her bireyin bir şekilde muhatap olduğu, ulaşabildiği bilgi akışı her zaman doğru bir nitelik taşımamaktadır. Dolayısıyla yanlış bilgi edinme, yanlış bilgilendirilme gibi süreçlerle karşılaşılması kolay bir şekilde mümkün hale gelmektedir. Toplumların genelini hedef alan aldatıcı içerikler, büyük çapta bir yankı uyandırmadan önce bireysel düzeyde bir etki bırakmayı tercih etmekte ve bu sebepten ötürü de manipülatif bağlamlar, içerikler akışa dâhil edilmektedir. Senkronizasyon istencine sahip olan, sürekli gündemden haberdar olmak isteyen bireyler tarafından da dijital etik ilkelerinden yoksun olan bu içerikler edinilmektedir.

2.Siber Uzayda Sosyal Medya Tehditleri

"Siber" kavramı, "sibernetik" kelimesinden türemiştir. İlk kez 1948 yılında Norbert Wiener adlı Amerikalı bir bilim adamı tarafından, "hayvanlarda ve makinelerde kontrol ve iletişim çalışmaları" anlamında kullanılmıştır (Wiener, 1948). Zamanla, bu ilk anlamından uzaklaşmıştır. Oxford sözlüğü siber kavramını, "elektronik iletişim ağlarına, özellikle internete bağlı olan" (Oxford Learner's Dictionaries) şeklinde tanımlamış ve bilgi teknolojileriyle ilintili olarak değerlendirmiştir. Siber uzay ise 21. yüzyılın teknolojik ve dijital gelişiminin ürettiği en temel kavramlardan biridir. Singer ve Friedman (2018, 29) siber uzayı; "içerisinde bilginin çevrim içi olarak saklandığı, paylaşıldığı ve iletildiği, bilgisayar ağları ve kullanıcıların alemi" olarak tanımlamaktadır. Siber uzay kavramına dair uzlaşılan husus, uzay son ekinin ilk akla geldiği gibi "sonsuz boşluk" anlamına gelmediğidir. Zira, siber uzayın muhtevası insan eliyle üretilmektedir. Siber uzayda üretilen, paylaşılan, toplanılan bilginin idamesini sağlayan yegane aktör insandır (Kurnaz, 2016, 60).

Bilgiyi, fiziki altyapıyı ve insanı içeren siber uzayda karşılaşılan sosyal medya tehditleri oldukça kapsamlıdır. Zira, sosyal ağ platformları, insanların birbirleriyle iletişime geçme ve etkileşim kurma yöntemlerini büyük ölçüde değiştirmektedir. Son zamanlarda sosyal medya platformlarının sayısı, amaçlarının ve kullanım alanlarının genişliğiyle birlikte giderek artmakta ve karmaşık hale gelmektedir. Böylece, bu platformlar insan hayatına sınırsız bir şekilde kapılarını aralarken, tespit edilmesi güç tehditleri ve riskleri de beraberinde getirmektedir.

Sosyal medyanın kullanımındaki bu hızlı büyümenin bir sonucu olarak artan siber tehditler ikiye ayrılmaktadır: klasik tehditler ve modern tehditler. Klasik tehditler, belirli bir ağdaki tüm kullanıcıları saldırıya açık hale getirmektedir. Modern tehditler ise yalnızca kullanıcı gizliliğini ve güvenliğini tehlikeye atabilecek çevrimiçi sosyal ağ altyapısını ve kullanıcılarını ilgilendirmektedir. İnternet ve sosyal medyanın gelişmesiyle birlikte siber uzayda ortaya çıkan klasik tehditler ve sorunların en bilinenleri; kötü amaçlı yazılımlar, kimlik avı saldırıları, hizmeti engelleme saldırıları, solucanlar, virüsler, gelişmiş kalıcı tehditler şeklindedir. Modern tehditler ise kullanıcıların kişisel bilgilerini elde etme, kişisel verilerin gizliliğini tehdit, sahte profiller ve anonimleştirme saldırıları, siber taciz, bilgi gizliliği sızıntısı, bilgi manipülasyonu, dolandırıcılık vb. şeklindedir (Almarabeh ve Sulieman, 2019, 2–3). Makalenin konusu itibarıyla yukarıda bahsedilen siber tehditler [3] ismen verilmiş olup, sosyal medyada karşılaşılan en temel siber tehditlerden biri olarak bilgi manipülasyonu derinlemesine incelenecektir.

Geleneksel medya araçlarıyla popülerliğini artıran manipülasyon kavramı, siber uzayda bir propaganda unsuru haline gelerek etkisini artırmaktadır. Manipülasyonun en etkin kullanıldığı alanlardan biri de sosyal medyadır. İçeriğin kaynağını veya kimlikleri gizlemek, içeriğin bağlamını değiştirmek, algoritmaları yanıltmak için spam gibi araçları kullanmak gibi yöntemler manipülasyon taktikleri arasındadır (Silverman, 2020, 18). Özellikle internet aracılığıyla sosyal medya kullanımı sayesinde algı oluşturulabilmekte, yanlış bilgilendirme ve manipülasyon gibi faaliyetlerle örtülü operasyonlar gerçekleştirilebilmektedir. Bu bağlamda yanlış bilgilendirme ve manipülasyon, siyasi saiklerle yanlış bilgiyi bilinçli olarak üretme ve yayma anlamına gelmektedir (Silverman, 2020, 18). Herkese açık bir kullanıcı profilinin oluşturulabildiği sosyal medya platformları kullanım amaçlarına ve tasarımlarına göre kategorilere ayrılmaktadır: sosyal ağ siteleri, bloglar ve içerik toplulukları, sanal dünyalar ve içeriğin oluşturulmasıyla ilgili herkesin katkıda bulunabildiği katılımcı projeler (Başıbüyük, 2014, 52). Sosyal medyanın bu hızlı

gelişimi manipülasyonun "bilgi manipülasyonu" şeklinde tezahür etmesine neden olmuştur. Nitekim sosyal medyada sık sık altı çizilen yalan haberler, propaganda, bilgi kirliliği, yanlış bilgi yayma gibi kavramlar bilginin manipüle edildiği anlamına gelmektedir. Kontrol ve yönlendirme kelimeleriyle anlam bulan manipülasyon, bilgi sistemleri kanalıyla yönlendirilmiş bilgi üreterek karşı tarafın imkan ve enerjisinin yanlış kullanılmasını sağlamayı amaçlar. Yönlendirmek maksatlı yapılan faaliyetler toplumda yanlış bilgilendirme yoluyla bir korku ve panik havasının yaratılmasını önceler (Başıbüyük, 2014, 46). Ancak, manipülasyon başlı başına yönlendirme anlamını taşımaz; ekleme, çıkarma, seçme yoluyla bilginin değiştirilmesini de kapsar (Sarı, 2020). Bu hususta, sosyal medyada bilgi manipülasyonunu engellemek maksadıyla çeşitli doğrulama platformları etkinliğini sürdürmektedir. Snopes.com, teyit.org, doğrula.org, dogrulukpayi.com, wardavar.org vb. bu doğrulama platformlarına verilebilecek örnekler arasında yer almaktadır. Brandtzaeg ve Folstad, doğrulama platformlarını üç kategoride inceler: (1) siyasi ve kamusal açıklamalar, (2) çevrimiçi söylentiler ve asılsız haberler, (3) belirli konularda tartışmalar veya çatışmalar (Brandtzaeg ve Folstad, 2017, 65). Doğrulama platformlarının ilk örneklerinden olan dogrulukpayi.org, Ortak Gelecek İçin Diyalog Derneği'nin girişimi olarak 20 Haziran 2014 tarihinde yayın hayatına başlamıştır. Türkiye siyasetine etki eden demeçleri kamuya açık verilerle analiz eden platform, doğruluk payını ölçmeyi ve kamuoyuyla paylaşmayı amaç edinmektedir (dogrulukpayi.com). Bu platform, Brandtzaef ve Folstad'ın kategorileştirmesi çerçevesinde ilk kategoride değerlendirilebilir. Bir diğer örnek Türkiye'de 2016 yılında kurulan teyit.org doğrulama platformudur. Bu platform medya gündeminde yer alan şüpheli bilgileri tespit etmek, araştırmalar yapmak ve kullanıcılara doğrulanmış bilgileri sunmak amacıyla kurulmuştur. 'Eleştirel düşünme alışkanlığını kazandırma ve yeni-medya okuryazarlığını artırma' gayesiyle yola çıkan bu platform bilginin güvenilirliğinin tespit edilmesini kolaylaştırmaktadır. 2018 yılında Facebook ile anlaşan platform, özellikle asılsız haberlere karşı tedbirleri önceleyen uygulamalara yer vermektedir (teyit.org). Bu platform ise ikinci kategori kapsamında yer almaktadır. Yalansavar.org ise 'akıl ve sağduyunun sesini dinlemek, mantıksal safsatalara düşmemek, asılsız iddiaları irdelemek' (yalansavar.org) iddiasıyla üçüncü kategoriye dâhildir. Örneklerini çeşitlendirebileceğimiz tüm aktif platformlara rağmen, kullanıcıların konu ile ilgili bilgi ve farkındalıklarının eksikliği doğrulama platformlarının performanslarını sınırlamaktadır. Zira, sosyal medya kullanıcılarının önemli bir kısmı edindikleri bilgilerin doğruluğunu gözetmeksizin paylaşma eğilimindedirler. Bu nedenle, siyasi ya da ekonomik saiklerle üretilen yalan haberlerin kamuoyunu etkileme potansiyeli giderek artmakta, bu da bireylerin 'sahte gerçekler' karşısında doğru haber alma hakkını önemli kılmaktadır.

Sosyal medya platformlarında içeriğin özelleştirilmesi, bu platformları özellikle yanlış bilgilendirme kampanyalarına açık hale getirir. Kullanıcılar, bilgileri çevrimiçi olarak kolayca ve hızlı bir şekilde paylaşabilir ve genellikle bunu paylaşılan bilgilerin doğruluğunu onaylamadan yaparlar. Sosyal medyanın bilgi manipüle eden aktörleri birbirinden farklı yöntemler benimseyebilirler. Örneğin; süreçlere, kişilere ya da kişi topluluklarına olumlu veya olumsuz etkide bulunabilmek için toplumda önyargı ve kavram yanılgıları yaratabilir ve yeni terimler üretebilirler. Siber alanda hâkim olan gündem konusunu değiştirebilir, anonim kaynaklara atıfta bulunabilir, verileri kötüye kullanabilirler. Özelleştirmek gerekirse, son yıllarda sosyal medyanın seçimleri manipüle ettiğine yönelik iddialar gündemdedir. Örneğin; Cambridge Analytica şirketinin bir uygulamayla Facebook kullanıcılarının verilerini çekerek seçimlere müdahale etmesi kamuoyunda geniş yankı uyandırmıştır. Dünyanın dört bir yanından seçmenlerin psikolojik profillerini siyasi kampanyalara dâhil etmek maksatlı bu veri sızıntısı

seçmenlerin davranışlarının tespitinde oldukça etkili olmuştur (Confessore, 2018). Bu yöntem, özellikle Donald Trump'ın Başkan seçildiği 2016 ABD seçiminde etkili bir şekilde kullanılmıştır. 2016 seçimlerini Trump'ın kazanmasının ardından ortaya çıkan seçimlerde hile iddialarının akabinde Facebook, Rusya'nın seçimlere nüfuz operasyonunda etkisi olduğunu kabul etmiştir (Dale, 2017). Seçim kampanyası boyunca Facebook, Twitter vb. sosyal medya platformlarında büyük ölçüde sahte hesaplar kullanılmıştır. Kamuoyunu şekillendirmede duyguların ve inançların objektif gerçeklere tercih edildiği durumları ifade eden post-truth (hakikat ötesi) kavramı, bu durumu özetlemektedir. Zira, günümüzde insanlar çoğunlukla hakikat arayışı yerine bilgi yığınlarını sorgusuz kabul etme eğilimi taşırlar. Steve Tesich tarafından 1992 yılında öne sürülen kavramın orijinal bağlamı, iktidarın konumuna yönelik eleştirel bir bakış açısı sunmaktadır. Teisch'e göre, söylem üzerinde gücü elinde tutan aktörler, yanlışları görmezden gelirken, aynı zamanda demokratik ve liberal değerleri ihmal etmişlerdir (Krasni, 2020, 2). Post-truth çağı, yalan haberleri ve dezenformasyon sürecini tetiklemekte ve hakikate dayanmayan fikirleri güçlendirmektedir. Dolayısıyla 'hakikat-ötesi' olarak Türkçe'ye çevrilen bu kavram, aslında hakikatlerin öneminin yitirildiği vurgusu yapmaktadır. Bu nedenle, Post-truth içeriklerin sosyal medyada yayılmasını önlemek oldukça güçtür. Kavramın popülarite kazanması Brexit referandumu ve ABD Başkanlık seçimleriyle mümkün olmuştur. Özellikle Trump'ın ''Meksika sınırına duvar örme'', ''Müslümanların ülkeye girişini yasaklama'' gibi söylemleriyle sosyal medyada aktif olması ''gerçekliğin anlamını yitirdiği'' yönündeki endişeleri doğurmuştur (Aydın, 2020, 78). Post-truth çağda en sık yüzleşilen ise 'fake news' (sahte haberler), yani kasıtlı ve doğrulanabilir şekilde yanıltıcı olabilecek içeriklerdir. Hızla yayılan sahte haberler, hakikatin çarpıtılarak 'post-truth' bir döneme girildiği iddiasını güçlendirmektedir. Zira post-truth çağ, algıların hakikatten önemli olduğu, her türlü manipülasyonun ve sahte içeriğin kolaylıkla geniş kitlelere yönlendirilebildiği bir çağdır (Yerlikaya ve Toker Aslan, 2020). Örneğin; 2018 yılında Twitter, Rusya ve İran destekli olduğu düşünülen trol hesapların milyonlarca tweet'ini, sosyal medya paylaşımlarının kamuoyunu ne ölçüde etkilediğini göstermek amacıyla paylaşmıştır. Paylaşımlar arasında ABD başkanlık seçimleri ve Brexit sürecine dair tweet'ler yer almaktadır. Aşağıdaki tweet'te ise Trump destekçilerinin medyanın gösterdiğinden çok daha fazla olduğu iddia edilmektedir (BBC, 2018).

Resim 1: Rusya İnternet Araştırma Ajansıyla Bağlantılı Bir Tweet

Kaynak: (BBC, 2018)

Siber uzayda bilgi manipülasyonu ve yanlış bilgilendirme, "sosyal mühendislik" kavramı altında değerlendirilebilir. Aslında sosyal mühendislik dolandırıcılık, bilgi toplama ya da sistemlere erişim sağlama gibi amaçlarla kullanılmaktadır. Örneğin; psikolojik bilgi manipülasyonu gerçekleştirilerek gizli bilgileri ifşa etmek oldukça etkili sosyal mühendislik yöntemlerinden biridir. Sosyal mühendisler iyi bir gözlemci olan ve insan ilişkilerinde başarılı kişilerden oluşmaktadır. Bilişim dünyasına ait bir kavram olmanın ötesinde en temel aktörü "insan" olduğu için sosyal bilimlerle de ilişkilidir. İnsanların karar verme yetilerini engellemek; güven, korku, endişe, panik vb. duygularını suistimal etmek gibi amaçlar taşır (Netsparker, 2017, 71). Sosyal mühendislik yöntemleri kişileri daha çok gizli bilgiler vermeye ve ikna etmeye dayansa da etkileme, yönlendirme, zorlama, aldatma gibi unsurlarıyla bilgi manipülasyonunu da bünyesinde barındırabilmektedir. Yakın bir örnek olarak COVID-19 pandemisi boyunca sosyal medyada dolaşıma giren sahte haberler ve oluşturulmaya çalışılan panik havası verilebilir. Bu süreçte, doğru ve güncel bilgiye ulaşmanın önemi ortaya çıkmıştır. Şekil 1'de görüldüğü üzere infodemi Wardle'ın içerik türleri ayrımında "manipüle edilmiş içerik" olarak varlık kazanmıştır. Öyle ki DSÖ bile bu bilgi kirliliğine atıfta bulunmuş, literatüre önceki başlıklarda değinilen "infodemi" kavramını dâhil etmiştir. İnfodemi, virüsten daha hızlı yayılarak geniş kitleleri manipüle etmiş ve panik havası oluşturmuştur.

3.1.Sosyal Medyada Bilgi Manipülasyonuna Karşı Siber Güvenlik Stratejileri

Bilişim ve enformasyon teknolojilerindeki ilerleme devam ederken, siber uzayda bilgi manipülasyonu ve yanlış bilgilendirme gibi tehditlere karşı siber güvenlik önemli bir kavram haline gelmiştir. Ticaretten kritik altyapılara ve iletişime kadar her şey küresel bir ağda işlemektedir. Bu durum çeşitli skandallara ve siber saldırılara neden olmakta, hatta halk hareketlerini ve devrimleri bile tetiklemektedir. Yani, siber uzayda bilginin manipüle edilmesi sanal alemin dışında gözle görülür neticelere sebebiyet verebilmektedir. Bu nedenle, kurumların, devletlerin hatta bireylerin emniyetlerini ve güvenliklerini sağlamak için siber güvenlik risk faktörlerini ciddiye alarak politikalar ve stratejiler üretmeleri gerekmektedir.

Siber güvenlik, siber uzayda yer alan her türlü verinin, bilginin korunması, üretilmesi, muhafaza edilmesi ve iletilmesi olarak tanımlanabilir. Uluslararası Telekomünikasyon Birliği'ne göre (ITU); siber güvenlik, siber uzayı oluşturan kullanıcıların bilgilerini ve siber organizasyonları muhafaza etmek amacıyla kullanılan politikaların, güvenlik tedbirlerinin, yönergelerin, uygulamaların, eylemlerin ve teknolojilerin birleşimidir.

Literatürde siber güvenliğin CIA üçlüsü olarak adlandırılan üç temel amacı vardır: gizlilik, bütünlük ve kullanılabilirlik (confidentially, integrity, availability). Gizlilik, veriyi muhafaza etmektir. Kişisel veriler, sırlar, bireyler ya da şirketler hakkındaki detaylar şifrelenmesi ve erişim kontrolü olması gereken mahrem konulardır. Bütünlük, sistem ve içerisindeki verinin, yetki olmadan değiştirilememesi ve işlem yapılamamasıdır. Kullanılabilirlik ise sistemi beklenilen şekilde kullanabilmektir. Ayrıca, siber uzayda güvenliğin ekonomik, sosyal, politik vb. bakış açıları da mevcuttur (Singer ve Friedman, 2018, 58). Görüldüğü gibi, siber güvenliğin üç temel amacı, yukarıda değinilen Mason'ın (1986) dört etik ilkesi (gizlilik, doğruluk, erişilebilirlik, fikri mülkiyet) ile örtüşmektedir. Bu kapsamda, teknoloji-insan ilişkisi ve dijital dünyanın etik boyutu, siber güvenliğin en temel aktörü olan "insan" bağlamında ön plana çıkmaktadır. Dolayısıyla, teknik anlamının ötesinde sosyal uyumsuzluk yaratmak, şiddeti tetiklemek, kutuplaşmayı artırmak vb. sosyal veya siyasi nedenlerle bilginin manipüle edilmesi siber güvenliğin insani boyutunu

gözler önüne sermektedir. Siber saldırıların bu insani boyutu, hedef bağlamında klasik siber güvenlik tehditlerinden ayrışmaktadır. Klasik siber saldırılar bilgisayar altyapısını hedeflerken; yanlış bilgilendirme, bilişsel önyargılardan ve yanılgılardan faydalanır.

Siber güvenlik konusunda sosyal medyanın rolü güncel bir meseledir. Yalnızca siyasi fikirlerin ve tutumların alışverişi için olmayan sosyal medya, aynı zamanda manipülatif yanlış bilgilendirme kampanyalarında da yeni bir alandır. Sosyal medya algoritmalarının; sosyal medya kullanıcıların beğenilerini, paylaşımlarını, yorumlarını ve diğer tüm faaliyetlerini kayıt altına alması internetin bir 'yankı odası'na dönüşeceğini düşündürmektedir. Yankı odası tabiri, tüm bu veriler çerçevesinde elde edilen bilgilerin tekrarlanması, sıklıkla kullanıcıların karşısına çıkarılması, böylece kutuplaşmanın ve tek tipleşmenin sağlanması olarak değerlendirilebilir. Bir diğer tabir olan 'filtre balonu' ise sosyal ağlardaki çeşitli kişiselleştirmeler vasıtasıyla profilimizle uyuşmayan içeriklerin mümkün mertebe engellenmesini ifade eder. Dijital platformlar 'kişiselleştirme' adı altında kullanıcıları yankı odalarına ve filtre balonuna hapsetmekte, doğru bir iletişimin önünde engel olmaktadır. Öte yandan, siyasi aktörler, kasıtlı olarak yanıltıcı bilgileri yaymak ve kamuoyunu şekillendirmek için bot ve trol hesapları kullanmaktadırlar (Metodieva, 2018, 4). Sosyal medyanın bilgi manipülasyonu karşısında aldığı tedbirlerin başında tartışmalı paylaşımların altına uyarı eklemek gelir. 2016 ABD seçimlerinden sonra Facebook bu uyarıları kullanmış, gönderilerin boyutlarını küçülterek dikkati azaltmak, doğrulayıcı paylaşımları listelemek, haber akışında alt sıralarda yer almasını sağlamak gibi önlemler geliştirmiştir (Kirchner ve Reuter, 2020, 4). Bizzat sosyal medya mecralarının aldığı tedbirlerin dışında uluslararası yasal düzenlemeler etkin olmadığı için sosyal medyada bilgi manipülasyonuna karşı önlemler daha çok ulusal düzeyde belirlenmektedir. Zira, sosyal medya şirketlerine kıyasla devlet kurumları yanlış bilgilendirmeyle mücadelede çok daha etkin ve güçlüdür.

Bilgi manipülasyonuna yönelik karşı tedbirler arasında yanlış bilgi, yalan haber yasası oluşturmak, yeni mevzuatlar ve kanunlarla yasal tedbirler sağlamak, uzmanlaşmış hükümet ofisleri kurmak, yanlış bilgilendirme veritabanı oluşturmak, sosyal medyada vergilendirme vb. yöntemler mevcuttur (Nagasako, 2020, 133). Hükümetler ekonomik yaptırımlar ve para cezaları uygulayabilir, tutuklayabilir ve kovuşturabilir, uluslararası seyahatleri sınırlayabilir, web sitelerine el koyabilir ve vergiden muaf statüsünü geri alabilir. Bununla birlikte, ifade özgürlüğünün anayasal ve diğer yasal garantileri, hükümetin çevrimiçi bilgilerin içeriğini düzenleme çabalarını kısıtlamaktadır (Hartke, 2016, 22). 2020 yılında Poynter Enstitüsü tarafından yayımlanan "A Guide to Anti-misinformation Actions Around the World" (Dünya Genelinde Yanlış Bilgilendirmeyi Önleme Eylemleri İçin Bir Rehber) başlıklı rapor, bu ve buna benzer tedbirleri ülkeler bazında değerlendirmiştir. Bu çalışmada, bu rapordan da faydalanarak siber uzayda faaliyetleriyle önem arz eden birkaç ülke örneğiyle devletlerin genel tutumları analiz edilmeye çalışılacaktır.

Medya ve internet üzerindeki katı düzenlemelerine rağmen, bilgi manipülasyonu Çin'de sosyal medyaya nüfuz etmektedir. Bu nedenle, Çin yasaları, ekonomik veya sosyal düzeni bozabilecek her türlü çevrimiçi yayını ve yanlış bilgilerin aktarılmasını yasaklar. Yasa ayrıca ulusal güvenliği ve sosyalist sistemi tehlikeye atabilecek veya başkalarının itibarını ihlal edebilecek içerikleri de yasaklamaktadır. Çin'de sosyal medyada kamu düzenini ciddi şekilde bozan yanlış bilgilerin yayılması, yedi yıla kadar hapisle cezalandırılabilecek bir suçtur (Zhang, 2019, 43). 2016 yılında Çin hükümeti "ekonomik ve sosyal düzeni baltalayan" söylentiler oluşturmayı ve yaymayı suç saymıştır (Funke ve Flamini, 2018).

2016 yılında Çin'in ilk Siber Güvenlik Yasası, Ulusal Halk Kongresi Daimi Komitesi tarafından kabul edilmiştir. İlgili yasa sosyal medya da dâhil olmak üzere çevrimiçi ekonomik veya sosyal düzeni bozabilecek yanlış bilgilerin yayınlanmasını ve iletilmesini, ağ kullanıcılarının bir dizi çevrimiçi faaliyet yürütmesini yasaklamaktadır. Yasa çerçevesinde yasaklanan faaliyetler şunlardır:

- Ulusal güvenliği, egemenliği, çıkarları ve sosyalist sistemi tehlikeye atmak
- Etnik nefreti veya ayrımcılığı savunmak
- Ekonomik veya sosyal düzeni bozmak için yanlış bilgi üretmek
- Başkalarının itibarını, mahremiyetini, fikri mülkiyetini veya diğer yasal haklarını ihlal etmek (Zhang, 2019, 44–45).

Çin'in dijital etik anlayışı, hâkim Batı-merkezli yaklaşımın aksine Konfüçyüs felsefesinden izler taşımaktadır. Çin etiği, sosyal adaleti ve toplumdaki insan ilişkilerinin uyumunu vurgular. Çok kültürlü toplum yapısıyla Çin, özellikle sosyal uyumla ilgili endişeler taşımaktadır. Dolayısıyla yukarıda bahsi geçen yasak faaliyetler etik kavramının siber uzayda da önemli olduğunu göstermektedir (Hsieh vd., 2011, 282–283). Bu kapsamda, Çin internetin güvenilir ve etik bir şekilde kullanımını hedefleyen "dijital vatandaşlık" kavramına önem atfetmektedir. Bu nedenle, Çin etik kurallarının dijital ortamda da uygulanması için çeşitli tedbirler alınmakta ve yaptırımlar uygulanmaktadır. Bu husus, uluslararası medyada Çin'in "dijital diktatörlük" olarak nitelendirilmesine sebep olmaktadır. Çin'de vatandaşlara puan verecek bir sosyal kredi sisteminin hayata geçirilmesiyle sosyal huzuru bozduğu düşünülen davranışlara sahip kişiler tespit edilecektir. Hükümet aleyhine konuşmalar, Çin Komünist Partisi'nin kurallarına uymayanlar ya da internette zararlı sitelerde vakit geçirenler düşük puan alması; tüm ülkeye yerleştirilen kameralarla uyumlu bir toplum oluşturulmaya çalışılması planlanmıştır (DW, 2018).

Tüm bunların yanı sıra, sosyal medya platformları, Çin'de faaliyet gösterebilmek için bir lisans bulundurmak zorundadır. Danıştay tarafından 2000 yılında yayımlanan İnternet Bilgi Hizmetlerine İlişkin İdari Tedbirlere göre, internet üzerinden çevrimiçi kullanıcılara bilgi sağlayan her türlü hizmet yönetmeliğe tabidir. Sosyal medya kullanıcılarının da yasalar gereği kimlik bilgilerini hizmet sağlayıcılara kaydettirmeleri gerekmektedir. Siber Güvenlik Yasası uyarınca, bilgi yayınlama veya anlık mesajlaşma hizmetleri sağlarken, hizmet sağlayıcılar, kullanıcılardan gerçek kimlik bilgilerini kaydetmelerini istemelidir. Hizmet sağlayıcıların, kimlik doğrulama adımlarını gerçekleştirmeyen kullanıcılara ilgili hizmetleri sağlamaları yasaktır (Zhang, 2019, 46). Siber uzayda iki rakip güç olan Çin ve ABD arasındaki siber mücadeleye bakıldığında da Çin'in ulusal ağlarını mümkün olduğunca küresel ağlardan izole etmek, ulusal endüstrilerin yerli teknolojiler üretmesi ve hükümet kontrollü haber ve bilgi içeren medyayı hâkim kılmak yönünde bir eğiliminin olduğu açıktır. Çin, sosyal medyayı rejime uygun ve ABD'ye zarar verecek şekilde kullanmak için sansür, yanlış haber ve trol hesapları kullanmaktadır (CSIS, 2018, 72).

2016 ABD seçimlerinin sosyal medya aracılığıyla Rusya tarafından manipüle edilmesi iddiaları ABD'yi de harekete geçirmiştir. Kongre Ekim 2017'de Facebook ve Google gibi çevrimiçi platformların reklamların kopyalarını tutmasını, bunları herkese açık hale getirmesini gerektiren bir tasarıyı ilan etmiştir. Kasım ayında ise Facebook, Twitter ve Google temsilcileri, seçim sırasında yanlış bilgilendirmeyi yaymadaki rolleri konusunda Senato yargı komitesine ifade vermiştir. Bu esnada, California eyalet hükümeti Eylül 2018'de devlet okullarında medya okuryazarlığını destekleyen bir yasayı kabul ederek

güvenilir medyanın nasıl değerlendirileceğine ilişkin öğretim materyallerini sağlamayı hedeflemiştir (Funke ve Flamini, 2018). 2018 yılında ABD'nin Ulusal Siber Güvenlik Strateji Belgesi yayımlanmış, siber uzayın güvenliği ABD'nin ulusal güvenliğinin olmazsa olmazı olarak değerlendirilmiştir. Belgede, Amerika Birleşik Devletleri'nin, çevrimiçi olumsuz etki ve bilgi üretme kampanyalarıyla devlet dışı propaganda ve yanlış bilgilendirmeyi ortaya çıkarmak ve bunlara karşı koymak için tüm uygun ulusal güç araçlarını kullanacağı ifade edilmiştir. Bu araçlar, kötü niyetli siber faaliyetlere karşı dijital platformların kullanımını önlemek için yabancı hükümet ortakları, özel sektör, akademi ve sivil toplumla birlikte çalışmayı içermektedir (The White House, 2018).

Rusya da siber uzayda aktif bir aktör olarak bilgi manipülasyonu konusunda çeşitli yasa tasarıları kabul etmiştir. Söz konusu yasa tasarıları "kişilerin hayatını ve halk sağlığını tehlikeye atabilecek, kamu güvenliği ve düzeninin büyük ölçüde ihlal edilmesi tehdidini artırabilecek veya ulaşım ve sosyal altyapı, enerji ve iletişim tesisleri ve bankaların işleyişini engelleyebilecek bilgilerin" yayılmasını yasaklamaktadır. İhlalde bulunduğu tespit edilen çevrimiçi haber kaynakları, 5.000 dolara kadar para cezası ve 15 gün hapis cezasına mahkum olacaktır. Ayrıca, her gün 100.000'den fazla ziyaretçi toplayan web sitelerinin yanlış olduğu düşünülen yorumları 24 saat içinde kaldırması veya 50 milyon rubleye kadar para cezasına çarptırılması gerekecektir. 2019'da Rus medya düzenleme kurumu, hükümetin "sahte" olarak belirlediği haber kaynaklarından oluşan bir veri tabanı oluşturmayı planladığını bildirmiştir (Funke ve Flamini, 2018). Eş zamanlı olarak, bilgi manipülasyonunu bir siber araç olarak kullanan konumuyla Rusya, ABD seçimlerinin yanı sıra Brexit sürecine müdahale, Emmanuel Macron'un kampanya ekibinin verilerini sızdırma gibi girişimlerde de bulunmuştur. Dolayısıyla, bilişim ve sosyalleşmenin temsil edildiği siber uzayda, özelde kullanıcıların genelde devletlerin maruz kaldığı manipülasyon taktiklerine karşı alınan tedbirler "dijital vatandaşlık" kurallarını mümkün kılmıştır. Bu doğrultuda devletlerin benimsemiş olduğu etik ilkeler ve siber güvenlik stratejileri bilgi güvenliğinin sağlanmasını mümkün kılmaktadır.

Sonuç

Adorno ve Horkheimer'ın kitle iletişim araçları özelinde yapmış olduğu kültürel analiz olan kültür endüstrisi kavramı, günümüzde sosyal medyanın üstlendiği rolü açıklamaktadır. Genelde toplumların özelde ise bireylerin barındırdığı farklılıkların göz ardı edildiği sosyal medyada birçok dijital etik ilkesinin geçerli olmadığı görülmektedir. Dolayısıyla akışa dâhil edilen bilgi içeriklerinin yanlış ve yalan kurgular üzerinde konumlandırılması sonucunda da hatalı içerik türleri oluşmaktadır. Bunun güncel örneği ise COVID-19 süreciyle de görünürlüğü artan manipüle edilmiş bilgi anlamına gelen infodemidir. Senkronizasyon istenciyle hareket eden ve sosyal medya akışı içinde kendini konumlandıran bireyler, gündemden uzak kalmak istememektedir. "Ana sayfa" olarak isimlendirilen ve bireylerin "paylaş" butonuna basarak oluşturduğu akışıyla bireyler bir şekilde muhatap olmaktadır. Yanlış ve doğru olan içeriklerin birlikte yer aldığı bu platformlarda bilgi kirliliği oluşurken, doğrunun yanlıştan ayrılması gittikçe güç bir hal almaktadır. Bu bağlamda sosyal ağ olarak nitelendirilen bütün oluşumlarda geçerli olması gereken dijital etik ilkelerin ihmal edildiği görülmektedir. Sosyal medya platformlarındaki üyelik sözleşmeleri, birçok etik ihlali barındırmaktadır. Bireylerin mahremiyetinin saklanmasını kapsayan gizlilik ilkesi bu noktada ilk olarak karşılaşılan olgudur. Yine oluşturulan ve paylaşılan bilgilerin manipüle edilmiş, yapay, aldatıcı şekilde oluşturulması da doğruluk ilkesiyle çelişmektedir.

Bu değerlendirmeler çerçevesinde dijital etik ve siber güvenlik stratejilerinin ortak bir paydada buluştuğu görülmektedir. Birbirini kapsayan kitle iletişim araçları, sosyal medya ve siber uzay da bireyler arasındaki etkileşimi ve bağımlılığı pekiştiren oluşumlardır. Bireyler, farkına varamadıkları kadar bilgiye maruz kalmakta ve doğruluk, yanlışlık, yalan, gerçek gibi nitelendirmelerinin yapılmasının da gün geçtikçe zorlaştığı görülmektedir. Bilginin siber uzayda, manipüle edilmiş bir kimlik kazanması, kitle iletişim araçlarıyla başlayan yönlendirici etkinin daha da arttığını göstermektedir.

Bilgisayar ve bilgisayar ağlarına ilişkin bir kavram olarak "siber", teknolojinin gelişimiyle birlikte insanı da bünyesinde barındıran bir olgu haline gelmiştir. Bilişim teknolojilerinin icadından sonra kötü yazılımların ve virüslerin üretilmesi, siber uzayın da insan eliyle güvenliksizleştirilebilecek bir alan olduğunu ispat etmiştir. Bununla mücadelede bireylerin çabaları yeterli olmamaktadır. Bu nedenle, siber uzayda dijital etik kavramı çerçevesinde devletler birtakım kurallar belirlemektedirler. Siber uzayda bir güç mücadelesi içerisinde olan ABD, Rusya ve Çin gibi büyük devletler kendilerine has siber stratejiler geliştirmektedir. Sosyal medyada bilgi manipülasyonunun etik arka planı ise devletleri "dijital vatandaşlık" kavramıyla tanıştırmaktadır. Dijital ortamda üretimde bulunan, iletişim kuran ve bilgi teknolojilerini kullanma yetisine sahip olması beklenen dijital vatandaşlar da teknolojik sorunlarla yüzleştiğinden siber davranışların, değerlerin, etik kuralların oluşması gerekmektedir. Bu kapsamda üretilen stratejiler çoğunlukla devlet-merkezli olmaktadır. Siber uzayı yönlendiren büyük devletlerin stratejileriyse birbirinden önemli farklılıklar içermektedir. Sosyal medyada manipülasyon türlerini, etik olmayan davranışları ve siber güvensizliği önleyebilmek için bireylerden uluslararası örgütlere kadar sistemin tüm aktörlerinin aktif katılımda olması, yaptırım gücü olan siber etik ve siber hukuk kurallarının geliştirilmesi elzemdir. Böylece kısmen de olsa sosyal medya siber tehditleriyle mücadele edebilecek ortak bir rejim geliştirilmesi muhtemeldir.

Notlar

1. Şeklin orijinali göz önünde bulundurularak Türkçe'ye çevrilmiştir.

2. Şeklin orijinali göz önünde bulundurularak Türkçe'ye çevrilmiştir.

3. Ayrıntılı bilgi için bknz;
https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial2.pdf;
Singer, P. W. & Friedman, A. (2018). Siber Güvenlik ve Siber Savaş. Ankara: Buzdağı Yayınları.

Kaynakça

Adorno, Theodor W. Kültür Endüstrisi Kültür Yönetimi. İstanbul: İletişim Yayınları, 2007.

Adorno, Theodor W. - Horkheimer, Max. Aydınlanmanın Diyalektiği. İstanbul: Kabalcı Yayıncılık, 2014.

Almarabeh, Hilal - Sulieman, Amjad. "The Impact of Cyber Threats on Social Networking Sites." International Journal of Advanced Research in Computer Science 10/2 (2019), 1–9. https://doi.org/http://dx.doi.org/10.26483/ijarcs.v10i2.6384

Amedie, Jacop. "Impact of Social Media on Society." Advanced Writing: Pop Culture Intersections 2/ (2015). https://doi.org/10.18311/gjeis/2016/15773

Avcıoğlu, Gürcan Şevket. "Bilginin Küreselleşmesinde Kitle İletişim Araçlarının Manipülatif Rolü." Selçuk Üniversitesi Edebiyat Fakültesi Dergisi 29/ (2013), 21–34.

Aydın, Ali Fikret. ''Post-Truth Dönemde Sosyal Medyada Dezenformasyon: COVİD-19 (Yeni Koronavirüs) Pandemi Süreci.'' Asya Studies 4/12 (2020), 76-90.

BBC. "Twitter, Rusya ve İran Bağlantılı Troll Hesapların Attığı 10 Milyondan Fazla Tweeti Paylaştı." 2018. https://www.bbc.com/turkce/haberler-dunya-45897313

Brandtzaeg, Petter Bae - Folstad, Asbjorn. ''Trust and Distrust in Online Fact-Checking Services.'' Communication of the ACM, 60/9 (2017), 65-71. doi: 10.1145/3122803

Confessore, Nicholas. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." The New York Times. 2018. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

CSIS. "Who Said What? The Security Challenges of Modern Disinformation." 2018. https://www.canada.ca/content/dam/csis-scrs/documents/publications/disinformation_post-report_eng.pdf

Dale, Helle C. "Russia Used Facebook Ads to Wield Influence in America. We Need Greater Transparency." 2017. https://www.heritage.org/government-regulation/commentary/russia-used-facebook-ads-wield-influence-america-we-need-greater

Doğruluk Payı. ''Hakkımızda''. https://www.dogrulukpayi.com/~Hakkimizda

DW. "Çin 'Dijital Diktatörlüğe' İlk Adımı Attı." 2018. https://www.dw.com/tr/çin-dijital-diktatörlüğe-ilk-adımı-attı/av-44525408

Funke, Daniel - Flamini, Daniela. "A Guide to Anti-Misinformation Actions Around the World." Poynter. 2018. https://www.poynter.org/ifcn/anti-misinformation-actions/#china

Gölbaşı, Selva Dilan - Metintaş, Selma. "Covid-19 Pandemisi ve İnfodemi." ESTÜDAM Halk Sağlığı Dergisi 5/ (2020), 126–137. https://doi.org/https://doi.org/10.35232/estudamhsd.797508

Gönenç, Özgür. İletişim Dünyası. İstanbul: Yılmaz Basım Yayıncılık, 2014.

Hartke, Raul. "The Oedipus Complex: A Confrontation at the Central Cross-Roads of Psychoanalysis." International Journal of Psychoanalysis 97/3 (2016), 893–913. https://doi.org/10.1111/1745-8315.12561

House, White. “National Cyber Strategy of the United States of America.” 2018

Hsieh, Ying-chun et al. “Chinese Ethics in Communication, Collaboration, and Digitalization in the Digital Age.” Journal of Mass Media Ethics: Exploring Questions of Media Morality 18/3–4 (2011), 268–285. https://doi.org/http://dx.doi.org/10.1080/08900523.2003.9679668

Kirchner, Jan - Reuter, Christian. “Countering Fake News: A Comparison of Possible Solutions Regarding User Acceptance and Effectiveness.” Proceedings of the ACM on Human-Computer Interaction 4/CSCW2 (2020). https://doi.org/https://doi.org/10.1145/3415211

Krasni, Jan. ''How to hijack a discourse? Reflections on the concepts of post-truth and fake news''. Palgrave Communications 7/1, (2020), 1-10.

Kurnaz, İbrahim. “Siber Güvenlik ve İlintili Kavramsal Çerçeve.” Cyber Politik Journal 1/1 (2016), 62–83.

Mason, Richard O. “Four Ethical Issues of Information Age.” MIS Quarterly 10/1 (1986), 5–11.

Metodieva, Asya. “Disinformation as a Cyber Threat in the V4: Capabilities and Reactions to Russian Campaigns.” Strategic Policy Institue. 2018. https://stratpol.sk/wp-content/uploads/2018/08/Cyber-Security-Threats_V4_final_version-FINAL.pdf

Nagasako, Tomoko. “Global Disinformation Campaigns and Legal Challenges Tomoko Nagasako.” International Cybersecurity Law Review 1/ (2020), 125–136. https://doi.org/https://doi.org/10.1365/s43439-020-00010-7

Netsparker. “İstihbaratın Sınıflandırılması.” Siber Güvenlik (1), 2017.

Ozan Leymun, Şenay. “Dijital Etik.” Pandemi Döneminde Sınanan Dijital Vatandaşlık. ed. Adile Aşkım Kurt - H. Ferhan Odabaşı. 173–203. Ankara: Anı Yayıncılık, 2020.

Öztürk, Ali. İmajoloji. Ankara: Elis Yayınları, 2013.

Pettman, Dominic. Infinite Distraction: Paying Attention to Social Media. Chichester: UK and Malden MA: Politiy Press, 2016.

Sarı, Mehmet Şafak. ''Dezenformasyon nedir? Sosyal medya, savaş meydanı oldu''. 2020. https://journo.com.tr/dezenformasyon-nedir

Sarıoğlu, Elif Başak - Turan, Erkan. “COVID-19 Ile İlgili Haberlerde Bilginin Yeniden Üretilmesi Sürecinin İnfodemik Açıdan Analizi.” Turkish Studies 15/6 (2020), 819–837. https://dx.doi.org/10.7827/TurkishStudies.44109

Silverman, Craig. Dezenformasyon ve Medya Manipülasyonu Üzerine Doğrulama El Kitabı. ed. Çevirmen Var. Teyit, 2020.

Teyit.org. ''Nedir?''. https://teyit.org/nedir

Tutgun Ünal, Aylin. Sosyal Medya Etkileri - Bağımlılığı - Ölçülmesi. İstanbul: Der Kitabevi Yayınevi, 2020.

Wardle, Claire. “Fake News. It’s Complicated.” 2017. https://medium.com/1st-draft/fake-news-its-complicated-d0f773766c79

Wardle, Claire - Derakshan, Hossein. “Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking.” Council of Europe Report 9/2017 (2017).

Wiener, Norbert. Cybernetics: Or the Control and Communication in the Animal and the Machine. Massachusetts: MIT Press, 1948.

Yalansavar. ''Yalansavar-Sık Sorulan Sorular''. https://yalansavar.org/yalansavar-sik-sorulan-sorular/

Yerlikaya, Turgay - Toker Aslan, Seca. '' Social Media and Fake News in the Post-Truth Era: The Manipulation of Politics in the Election Process''. Insight Turkey 22/2 (2020), 177-196.

Zarocostas, John. "How to Fight an İnfodemic." The Lancet 395/10225 (2020), 676.

Zhang, Laney. "Government Responses to Disinformation on Social Media Platforms." The Law Library of Congress, 2019.

World Heath Organization. "Munich Security Conference." 2020. https://www.who.int/director-general/speeches/detail/munich-security-conference.